MTN CS Security Baseline Implementation & Rollout

MTN Irancell

BTEB-18:001445 Uen Rev PA8

Contents

1 Introduction

MTN Irancell should implement security measures on their Charging System (CS) nodes, to reach the desired security level, set by MTN Group and ensure full compliance to the baseline requirements.

Desired security level will be achieved through configuration of the charging and mediation nodes with adequate security controls, to resolve and remedy each potential finding identified by the security audit.

1.1 Charging System Security

The implementation of MTN CS security baseline in Charging System for MTN Irancell will focus on the following security concepts and mechanisms.

Current MTN Group CS Security Baseline has been re-structured in way to achieve industry best practices in modular layout as depicted in the table below.

Table 1 Baseline with a Modular Layout

Security Area	Security Baseline Tag	Short Description
Functional Requirements (FR)[1]		
Access Control (ACC)		Users will be granted access and certain privileges to system: Authentication and Authorization**.**
1.1 User Access Management	IN_ACC_xxx	Regular user accounts as well as system accounts on all layers (OS, DB, APP).
1.2 Password [2]Management	IN_ACC_xxx	Password Management requirements cover password policy including change of default passwords on all layers (OS, DB, APP

[1] *FR describes what the system should do*
[2] *A password is a convenient and easy method of authentication for users entering a computer system*

1.3 System Access Control	IN_ACC_xxx	System Access Control requirements cover prevention of unauthorized access to OS, Network Services, and applications.
2. Hardening (HARD)		Hardening requirements cover non-access control related system hardening.
2.1 OS Hardening	IN_HARD_xxx	OS Hardening requirements cover reducing the vulnerability surface of the OS including disabling of unsecure or unused services.
2.2 DB Hardening	IN_HARD_xxx	Database Hardening requirements cover reducing the vulnerability surface of the Database.
2.3 Web Server Hardening	IN_HARD_xxx	Web Server Hardening requirements cover reducing the vulnerability surface of the Web Server.
3. Logging (LOG)		System log collection is critical to understand the nature of security incidents/events during an active investigation and post analysis. Logs are also useful for establishing baselines, identifying operational trends, and supporting the customer's security team internal investigations, including audit and forensic analysis.
3.1 Audit Log	IN_LOG_xxx	
3.2 Archive Log	IN_LOG_xxx	
4. Encryption (ENCRYPT)		
4.1 Secure Protocols (TLS)	IN_ENCRYPT_xxx	
4.2 SSL/TLS Cipher	IN_ENCRYPT_xxx	

4.3 SSH Cipher	IN_ENCRYPT_xxx	Encryption requirements cover SSL/TLS based communication for web servers, network, and system services as well as encryption of data at rest.
5. Privacy[3i] (PRIV) - PRE_FEASIBILITY STUDY		In Charging System, at least the follwing shall be considered: • Privacy for the subscribers, mobile users Privacy for the administrative staff is not considered necessary in the Charging System, since the Charging System is not to be used for any private action.
6. •Additional Security Features (ADD_SECFEAT)		Security enhancement features and functionalities that may improve the charging system security posture to minimize further the level of risks
6.1 IP Filtering, IPSec, EVS, RSYSLOG	IN_ADD_SECFEAT_xxx	
Non-Functional Requirements (NFR)[4],		
7. Upgrade (UPG)	IN_UPG_xxx	
7.1 Patching (PATCH)	IN_PATCH_xxx	
8. Relevant Artifact (AF)	IN_AF_xxx	
8.1 Security Implementation Validation	IN_VAL_xxx	

[3] *Privacy Policy sets out the approach which Customer will take in relation to the treatment of Personal Information. It includes information on how Customer collects, uses, discloses, and keeps secure, individuals' Personal Information. It also covers how Customer makes the Personal Information it holds available for access to and correction by the individual*

[4] *NFR describe how the system works*

9. Compliance Monitoring (CPL)	IN_CPL_xxx	A non-functional requirement is that it essentially specifies how the system should behave and that it is a constraint upon the systems behaviour. One could also think of non-functional requirements as quality attributes for of a system. The following Operational security standards policy can be considered as a NFR: • Security Controls impl. Logs & screenshots • Vulnerability scanning after baseline deployment (Evidence impl. security controls meet the baseline compliance) • Audit logs review • Password recovery procedure Etc…
10. Audit Logs Review (REV)	IN_REV_xxx	
11. Password Recovery (RECOV)	IN_RECOV_xxx	
12. Pre-defined System Accounts &	IN_PREDSA_xxx	Predefined system accounts properties per node type & per level (OS, DB, and APP)
13.		

1.2 Scope

The scope of the requirement analysis activity is to evaluate the Charging System (CS) and Multi Mediation (MM) nodes capabilities against MTN CS baseline identified requirements for security and define the appropriate controls to meet MTN standards (CS security baseline mandatory requirements).

The scope of this document includes the following topics:

- Requirement Analysis, which encompasses short description to each requirement.
- Charging System 17.0 or higher, as indicated below
- Requirements are considered on Operating system, Database, and Application levels as per MTN CS security Baseline scope

1.2.1 Nodes in Scope

The table below illustrates the list of nodes and their characteristics in MTN Irancell scope.

Table 2 Charging System and Mediation nodes characteristics - MTN Irancell

Node	Current Patch Level (ICP)	Comment
Charging System		
SDP	CS18 SDP 5 R24A	Live Native (Physical)
AIR	CS 18 AIR 4.0	Live Native (Physical)
ngCRS	CS 18 ngCRS 8.1	Live Native (Physical)
ngVS	CS 18 ngVS 5.0	Live Native (Physical)
CCN	CS 18 CCN 6.1.0	Live Native (Physical)
ECMS	CS 18 ECMS 5.0	Live Native (Physical)
CS-NMT	CS 18 CS-NMT 3.0	Live Native (Physical)
Multi Meditation		

EDA	EDA 1	Live Native (Physical)
EMM	EMM 18	Live Native (Physical)

1.2.2 3PP Component Details

3PP components for the Charging System and the Mediation details per node type, are illustrated in the table below.

Table 3 Charging and Mediation Nodes 3PP Component Details

Node Type	Hardware	Operating System (OS)	3PP Details
Charging System			
SDP (Native)	HP DL360 Gen 8 HP DL360 Gen 9	RHEL 6.x	• Database (DB): TimesTen[5] Release 11.2.2 • Apache 2.2.34 • SDP application (APP) is built on the Flexible Distributed Systems (FDS) platform
AIR (Native)	HP DL360 Gen 9	RHEL 6.x	• Apache Web Server 2.2.34 • Java 1.8.0_131 • AVIM application(APP)

[5] *The TimesTen database embedded in SDP is an in-memory SQL database for storage of subscribers and service classes. The database is synchronized between the different SDP servers in the cluster.*

CCN	BSP8100	TSP7 SUSE Linux SLES 11 SP4 based on CBA (Component Based Architecture)	• Apache v2.0
ngCRS	HP DL380 Gen9	RHEL 7.3	• Java jdk1.8.0_131 • Apache HTTP Server 2.4.6 • PostgreSQL 9.4.9-1 • Apache Tomcat 8.5.12 • Oracle 11.2.0.4
ngVS	HP DL360 Gen9	RHEL 7.3	• Java 1.8.0_144 • Cassandra 2.1.16 • Jetty webserver is 9.3.9 (Embedded Mode)
CS-NMT	HP DL360 Gen9	RHEL 7.3	• Java JRE 1.6.31
ECMS	HP DL360 Gen9	RHEL 7.3	• Oracle 11.2.0.4 • Apache Tomcat 9.0.0
Multi Mediation			
EDA	HP BL460cGen9	RHEL 7.3	• Apache Tomcat 8.0.47 • Cassandra 2.2.5/2.1.13 • Zookeeper 3.4.9.1
EMM	HP BL460cGen10	RHEL 7.3	• Database (DB): PostgreSQL 9.6.2 • Veritas 7.2 • Apache Tomcat 8.0.41

1.2.3 Security Related Documentation for Charging and Mediation Nodes

Following documents, described in table below, per node are used as references for MBSS implementation procedure development.

Table 4 Charging System and Mediation Documentation

Node	Document	Source	Comment
SDP (LINUX)	• SDP System Administrator's Guide, RHEL, 4/1543-FAM 901 107/5 Uen BH • SDP Hardening Guideline and Instruction, RHEL, 15/1531-FAM 901 107/5 Uen K	CPI library documentation for SDP 5 [1]	
	• CIS Red Hat Enterprise Linux 6 Benchmark v1.4.0	CIS library documentation [10]	Additional (3pp library)
AIR (LINUX)	• AIR System Administrator's Guide, Linux, 3/1543-FAM 901 108/5 Uen AT • AIR Hardening Guideline and Instruction, RHEL, 12/1531-FAM 901 108/5 Uen U	CPI library for AIR 4.0, [1]	
	• CIS Red Hat Enterprise Linux 7 Benchmark v2.1.0	CIS library documentation, [11]	Additional (3pp library)
CCN (TSP)	• CCN System Administrator's Guide, 1/1543-FAM 901 098/5 Uen AZ • CCN Hardening Guidelines and Checklist, 19/1553-FAM 901 098/5 Uen T • TSP Node Hardening Guideline and Instruction, 2/1531-ANA 901 06 Uen AA • TSP Node Hardening Checklist, 1/153 11-ANA 901 06 Uen J • Logging User Guide, 1/1553-CRA 119 645/4 Uen G	CPI library for CCN 6.1.0, [1]	

EDA (LINUX)	• System Administrators Guide for Native Deployment Ericsson Dynamic Activation 1 1/1543-CSH 109 628 Uen D • Hardening Guideline for Native Deployment Ericsson Dynamic Activation 1 1/154 43-CSH 109 628 Uen A	CPI library for Ericsson Dynamic Activation 1 Sep-17 [5]	
EMM (LINUX)	• System Administrator's Guide for Linux, 1/1543-FAM 901540 Uen D • Security Policy and Guideline, 1/0400-FAM 901 540 Uen A	CPI Store for EMM 18, [4]	
	• CIS Red Hat Enterprise Linux 7 Benchmark v2.1	CIS library documentation [11]	Additional (3pp library)
ngCRS	• CRS System Administrator's Guide 1/1543-FAM 901 483/1 Uen AA • CRS Hardening Guidelines and Instructions 2/1543-FAM 901 483/1 Uen K	Charging data Reporting System (CRS) 8.1, CPI [1]	
ngVS	• System Administrator Guide 1/1543-FAM 901 478 Uen AC • VS Hardening Guideline and Instructions, RHEL Voucher Server 5.0 11/1531-FAM 901 478 Uen A	• CPI library for Voucher Server (VS) 5.0, [1] • CAL library for Voucher Server (VS) 5.0, [3]	
CS-NMT	• CS-NMT System Administrator's Guide 1/1543-FAM 901 441/2 Uen A	• CPI library for Charging System-Network Management Toolkit 2.0, [1]	

	• CS-NMT Hardening Guide 2/1553-FAM 901 441/3 Uen A	• CAL library for Charging System-Network Management Toolkit 2.0, [3]	
ECMS	• Ericsson CMS Linux System Administrators Guide 2/1543-FAM 901 485 Uen N	• CPI library for Ericsson Customer Management System (ECMS) 5.0 [1]	

1.3 Delivery Phase

The Security Baseline Design & Implementation for MTN Irancell is scoped into separate phases, depending on the Network Migration and Modernization activity readiness.

Security Baseline Implementation and the Compliance check for the completed set of installed and integrated nodes would be automated using the Ericsson Security Manager(ESM) remotely, as a tool.

1.4 Excluded

Following is excluded from the scope of the document:

- Any other requirements other than the ones explicitly identified in this document and mapped to CS Security Baseline [1]
- MINSAT and VXML-IVR nodes
- IN_REQ045_v4, IN_REQ140_v4 and IN_REQ141_v4 marked as “Additional Validation Requirements”: Only a check will be performed to see whether
    - IP Filtering is required to be enabled,
    - Predefined System Account Properties is to be compiled,

  - Compliance Checklist will be taken up by ESM Compliance Manager

- Security for Charging System in virtualized deployment
- Integration with Ericsson Network Access Management (ENAM) or Ericsson Centralized Audit Logging (ECAL) solutions
- Integration with other 3PP/Local Security Information and Event Management (SIEM) or Identity Access Management (IAM) systems solutions, e.g. OpenLDAP, Windows AD, Centrify, ArcSight, Imperva, etc
- Qualys Vulnerability scanning

2 Requirement Analysis (HLD) Structure

2.1 Overview

Each of the requirements has been given a unique ID. The defined slogan (title) of each requirement will be corresponding to the name of the security control (MBSSv3 Work Package, WP), intended to be selected per node to meet the baseline requirements.

The requirement structure and its definition shall include the following items:

- Requirement ID: IN_REQxxx_v4 (v4 stands for MBSSv4)
  - Example: IN_REQ001_v4
- Requirement Slogan (Title)
- Mapping of created requirement(s) to:
  - MTN CS security baseline requirement(s) tag, Essential
  - Internal/External auditor report (finding number), Optional.
- Impacted node(s) list
- Level (OS, DB, APP)
- High Level Description
- Solution proposed
  - Operating System
  - Database

- Application

- References

  This item shows the impacted nodes security documentation for each defined security control (REQ).

  The Chapter 4 lists the corresponding reference documents and their URL links (CPI/3PP Library).

3 Functional Requirement (FR)

3.1 Access Control (ACC): User Access Management

3.1.1 IN_REQ001_v4: Prevent Sharing of Privileged Accounts

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_001, OS_ACC_006, OS_ACC_007, OS_ACC_008, DB_ACC_001, DB_ACC_002, DB_ACC_003, DB_ACC_004, APP_ACC_001, APP_ACC_002

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- Charging System (including Mediation) has the concept of application users which is separated from the DB users and OS users. The login credentials for the application users cannot be used to access the database or OS system. In this way the concept of application users separates the DB users and OS users from the users of Charging System.

Sharing of privileged accounts should be restricted. Direct access to these accounts should not be allowed. A user can be assigned a privileged role to handle part of total set of administrative tasks. This can be done locally as well as remotely, using LDAP server (limited to supported node only) for authentication and authorization of the user access.

Solution Proposed- By taking the role-based access into use the “privileged” accounts and a system-specific shared account are changed into roles which can be assigned to appropriate users. Each user can be assigned one or more roles, so no shared user accounts are required.

Once more than one person knows the privileged accounts passwords, plausible deniability becomes a factor: who performed the task and when that task was performed does not mean much when 15 administrators have the same password and level of access.

Operating System

1. *User Privilege and Role*

a) *Locally*

- For RHEL/SUSE

This can be taken care by `SELinux` and `sudo` configuration

- For CCN (TSP/SUSE)

The practice of sharing the privileged system accounts e.g. `root`, `telorb` and `jambala` passwords among two or more admins is unacceptable. The prevention of sharing CCN privileged accounts (`root`, `telorb` and `jambala`) can be achieved by creating individual users and JIM administrator; and assigning suitable roles to those users/administrators.

b) *Using LDAP*

All charging system does not support LDAP external interface nodes; consequently, external user authentication won't be possible for all accesses.

The table below demonstrates the list of charging nodes, which support the LDAP interface (users can be authenticated against a variety of external identity store)

Table 5 LDAP Interface Support by Charging and Mediation Nodes

Node	LDAP Interface Support	Reference Doc.
SDP	YES	Lightweight Directory Access Protocol (LDAP) is used between two SDPs or between an SDP and an external database for fetching community data for a subscriber who has not been charged if the Community Charging function is used. Reference: SDP Network Element Description, 1/1551-FAM 901 107/5 Uen BB
AIR	NO	
CCN	YES	Telecom Server Platform (TSP) supports Lightweight Directory Access Protocol (LDAP) interface and its compliance to LDAP v3 standard.

		Reference: LDAP Interface Description, 2/155 19-CRA 119 638/5 Uen A
EDA	YES	Dynamic Activation is shipped with a set of common southbound interface adapters, for example HTTP, Telnet and LDAP Reference: Customization - Architectural Overview Ericsson Dynamic Activation 1 20/1553-CSH 109 628 Uen E
EMM (Linux)	YES	Multi Mediation as Lightweight Directory Access Protocol (LDAP) client supports v2 and v3 for authentication of Multi Mediation users from external central user repository starting in MM 8.1. MM18 supports LDAP Authentication Mode: In this case, all Multi Mediation users get authenticated from the external LDAP system which is integrated with Multi Mediation Reference: Network Impact Report, 1/109 48-FAM 901 469 Uen CN User Management Guide Ericsson Multi Mediation 18, 2/1553-FAM901540 Uen A
ngCRS	NO	
ECMS	NO	
CS-NMT	NO	
ngVS	NO	

LDAP[6] can be used as a central directory accessible from anywhere on the network. For those nodes supporting LDAP interface and are already integrated with LDAP server, user will be created on LDAP server and assigned authorization level based upon role and input from MTN Irancell.

LDAP characteristics, including which node, interface, level currently have been integrated need to be provided by MTN Irancell.

Database

1. *User Privilege[7] and Role[8]*

[6] *LDAP supports Secure Sockets Layer (SSL) and Transport Layer Security (TLS), sensitive data can be protected from prying eyes.*

[7] *A **user privilege** is the right to run a SQL statement, or the right to access an object that belongs to another user, run a PL/SQL package, and so on. Oracle Database define the types of privileges*

[8] ***Roles** are created by users (usually administrators, to group together privileges or other roles. They are a way to facilitate the granting of multiple privileges or roles to users*

Administrative privileges can be granted only to trusted users. System privileges[9] can be granted to other users or revoke from them

a) TimesTen

Users can access TimesTen database objects, authorization can be controlled to these objects with privileges in similar way as for Oracle database.

In SDP node, the database is protected by standard Linux user privileges, which means that no individual users have permissions to access the database. Only `root` *and* `sdpuser` *must have, access to the database application.*

When hardening is applied, there can be some consequences that must be

- The `sdpuser` can no longer be used directly, but only as a role.
- The `root` user can no longer be used directly, but only as a role.

The following link gives more information on it:

https://docs.oracle.com/cd/E11882_01/timesten.112/e21642/privileges.htm#TTSQL343

b) Oracle

Administrative privileges can be granted only to trusted users. System[10] privileges can be granted to other users or revoke from them.

c) PostgreSQL (9.1, & or 9.6.2)

Users must be granted privileges to use database objects created by other users (By default, only the owner of an object can do anything with the object)

The following link provides all the information you may need about the subject:

https://www.postgresql.org/docs/9.1/static/ddl-priv.html

https://www.postgresql.org/docs/9.4/static/ddl-priv.html

d) Cassandra (2.2)

[9] *A **system privilege** is the right to perform an action or to perform an action on any schema objects of a type. For example, the privileges to create tablespaces and to delete the rows of any table in a database are system privileges*

[10] *A **system privilege** is the right to perform an action or to perform an action on any schema objects of a type. For example, the privileges to create tablespaces and to delete the rows of any table in a database are system privileges.*

Cassandra 2.2 introduces an improvement of replacing the simplistic approach of managing permissions on an individual user basis, with something much more powerful and flexible, through role-based access control (RBAC). Under this new scheme, permissions are granted to a role just as they were previously granted to a user, the key difference is that roles can also be granted to each other.

So, in this context we can think of them as Groups, rather than Individuals.
This greatly simplifies permissions management for administrators by allowing related privileges to be bundled together by granting them to roles, which can in turn then be assigned to database users.

The following link gives more information

https://www.datastax.com/dev/blog/role-based-access-control-in-cassandra

e) MySQL

MySQL is an open source database management software that helps users store, organize, and later retrieve data. It has a variety of options to grant users nuanced permissions within the tables and databases.

In CCN MySQL database is running and used for storing the different type database and application logs and being accessed by Logging query tools, it's not accessible from outside node. Only MySQL user can access the MySQL

MySQL database is removed in TSP 7 for details please see the reference section, TSP Node Hardening Guideline, and Instruction Chapter 3.3.7

More details about MySQL Access Privilege System are here:

https://dev.mysql.com/doc/refman/5.5/en/privilege-system.html

NOTE:

All nodes should be already integrated with OpenLDAP/Windows AD

Only user authentication and authorization configuration support will be provided based upon MTN Irancell input

Privilege to `superuser` account (`root`) would be granted to 3-4 Individual Unix/Linux accounts only

Application

Prevention of sharing privileged account at application level is performed per node type and depending on type of Java GUI applications used and administration tools.

The table below demonstrates the list of predefined users at the Operating System, Database, and Application layer with high privilege for Charging & Mediation nodes.

Table 6: Predefined system accounts with high privilege

Node Type	OS Super user	OS Users hosting Application	OS Users hosting Database	Application Users at the GUI	Database Users
Charging Nodes					
SDP	root	sdpuser	root	fdsuser, SysAdm	sdpuser, root
AIR	root	fdsuser	Not Applicable	fdsuser, SysAdm	Not Applicable
CCN	root	telorb, jambala	Not Applicable	jambala	Not Applicable
ngCRS	root	crsadmin	oracle postgres	admin	BI, OAM, mmsuper
ECMS	root	ecms	oracle	jmxRead, licenseRead, AD	SYS, SYSTEM
CS NMT	root	csnmt	Not Applicable	nmtroot	Not Applicable
ngVS	root	zookeeper	vsuser	vsuser	vs
Mediation Nodes					
EMM	root	mmsuper	postgres	mmsuper	postgres, mmsuper
EDA	root	actadm, dvecli, casadm, zooadm, sysnuser	casadm	admin, cai3guser	cassandra

References-

Reference Document	Chapter
CPI Library	
SDP User Guide System Administration Tool	4 Authority
AIR Hardening Guideline and Instruction, Sun Solaris	4.2 Roles

AIR User Guide System Administration Tool	4 Authority Handling
LE OS Hardening Guidelines, and Instructions	4.2.1.2 Authentication
CCN Hardening Guidelines and Checklist	3.3.2 Creation of user account
	3.3.3 Assigning role-based access to users
CCN User Administration User Guide	2.4 Accounts
	4.2 Access Group
System Administrators Guide for Virtual Deployment Ericsson Multi Activation 16.1	2.6 Users
User Guide for Subscriber Activation Ericsson Multi Activation 16.1	7.5 Access Control
EMM: User's Guide	4.8 User Management
EMM: Procedure Manual	3.11 User Management
3PP Library	
Openscg.com, Security Hardening PostgreSQL	Role base access control

- More details here: http://docs.oracle.com/cd/E25054_01/network.1111/e16543/authentication.htm
- More details here: http://www.postgresql.org/docs/9.1/static/sql-createrole.html
- More details here: http://www.postgresql.org/docs/9.1/static/sql-alterrole.html
- More details here: http://docs.oracle.com/cd/E11882_01/server.112/e41084/statements_6010.htm#SQLRF01310

3.1.2 IN_REQ002_v4: Minimize the Use of Generic User Accounts

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_OS_ACC_001

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description - Generic accounts are a security risk. This risk can be reduced if generic account holders follow some basic safe working practices.

Solution Proposed – The consequences of granting access to the generic user account across the organization should be weighed carefully.

A generic user account is one that is not derived using a standard naming convention. For example, instead of logging into a workstation with your first name/last name, you log in as Admin; meaning there is no corresponding real user associated with the account.

It's tempting to set up accounts this especially when duties are shared among multiple users. In the **short term**, it seems beneficial to have an account set up that multiple people can use. However, in the **long term**, the lack of accountability such an account could be problematic. Data Protection laws may require audits of who has access to your business data.

To minimize the use generic accounts following should be considered:

- Individuals should login with their own username, password provided
- It is the responsibility of the individual to take ownership and accountability of activities performed by the username assigned to him
- Login to the hosts using pre-defined system accounts should be disabled. This can be achieved by assigning `/bin/false` or `/sbin/nologin` shell to those accounts (wherever applicable)
- Direct login via system accounts with high privileges (as per Table 6) should be restricted. Sudo privileges for these accounts should be assigned to approved individual users.

Ericsson and industry best practice recommendations:

- MTN Group Information Security Policy (GISP) for user IDs shall be enforced during the creation of new user account (avoid/reduce the use of generic user accounts).
- It is a commonly enforced best practice, to attach each identity & account to an individual, with privileged access.

References-

N/A

3.1.3 IN_REQ003_v4: Remove or Disable Inactive Users

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_004, DB_ACC_008, APP_ACC_006

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- The users which are inactive for at least a certain number of days must be identified and removed.

Solution Proposed-

Operating System

a) RHEL/SUSE

Disabling inactive accounts ensures that accounts which may not have been responsibly removed are not available to attackers who may have compromised their credentials. Inactive users on the OS layer will be deleted by the following methods:

Option 1: EHardening or MM_Utility Tool

EHardening Tool

Hardening procedures are performed on Hardware, OS, and the Application.

To achieve this, a file `/root/defaultconf.ini` with below entries must be updated before running the EHardening tool

```
AccountListDisableUsers = <list of user accounts that are disabled>
```

MM_Utility Tool

Multi Mediation Utility Manager accepts the user inputs in the form of template, which will be opened for User alteration and confirmation during Hardening progression.

The following parameters must be updated

```
AccountListDisableUsers = <list of user accounts that are disabled>
```

Option 2: Standard Linux Command(CLI)

Use the `userdel` command to delete a user account and related files from user account. The `userdel` command must be run as `root` user. The syntax is as follows:

```
userdel <username>

userdel [options] <username>

userdel -r[11] <username>
```

Database

Inactive users will be deleted from the database. This is Not applicable for AIR and CS-NMT since there is no database installed on the same.

a) TimesTen

IMPORTANT NOTE:

Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions[12]. Only `root` and `sdpuser` are to have, and must have, access to the database application.

The `sdpuser` and `root` can no longer be used directly, but only as a role.

While human interaction is prohibited, TimesTen support human interaction using system account i.e. `sdpuser, root`, or internal/external identified individual users.

[11] *The -r option is used to recursively Delete the User's Home directory and the files stored inside it*

[12] *The database is protected by standard Linux user privileges, which means that no individual users have permissions to access the database. Only root and sdpuser are to have, and must have, access to the database application.*

However, in a non-embedded configuration, TimesTen is a high performance relational in-memory database. The `DROP USER` statement drops the user "`<username>`" from the database: The `drop user` command must be run as an `admin` user

```
Command> drop user <username>;
User dropped.
```

b) PostgreSQL

Command `DROPUSER` removes an existing PostgreSQL user. Only superuser and users with the `CREATEROLE` privilege can remove PostgreSQL users.
To remove a `superuser`, you must yourself be a `superuser`.

The identified inactive user can be deleted by executing the below SQL statement

```
DROP USER <username>;
```

c) Cassandra

`DROP USER` removes an existing user. In Apache Cassandra 2.2.0 and later, you can test whether the user exists or not. Attempting to drop a user that does not exist results in an invalid query condition unless the IF EXISTS option is used. If the option is used, the statement will be a no-op if the user does not exist. You must be logged in as a `superuser` to issue a `DROP USER` statement. Users cannot drop themselves.

Delete the identified inactive user

```
cqlsh> DROP USER <user_name>;
```

The following link provides all the information you may need about the subject:

https://docs.datastax.com/en/cql/3.1/cql/cql_reference/drop_user_r.html

d) MySQL

The DROP USER statement removes one or more MySQL accounts and their privileges. It removes privilege rows for the account from all grant tables. To use DROP USER, you must have the global CREATE USER privilege, or the DELETE privilege for the mysql database.

Drop user with below command:

```
DROP USER <user_name>;
```

e) Oracle

The following default accounts created by Oracle have a well-known password and can be potentially used to alter the database to launch exploits against production to gain unauthorized access to user data:

- `BI` account owns the Business Intelligence (BI) sample schema
- `HR` account is used to manage the HR (Human Resources) sample schema
- `IX` account is used to manage the Information eXchange (IX) sample schema
- `OE` account is used to manage the Order Entry (OE) sample schema
- `PM` account is used to manage the product media (PM) sample schema for Business-to-Business
- `SCOTT` account is used in examples throughout the Oracle database
- `SH` account is used to manage the SH sales history schema, which stores business data

1. Execute the following SQL to drop the <USERx> user and all objects in the user's schema:

   ```
   SQL> DROP USER USERx CASCADE;
   ```

2. After removing the default account, ensure the user <USERx> does not exist by executing the following query:

   ```
   SQL> SELECT username FROM ALL_USERS WHERE
   USERNAME='USERx';
   ```

IMPORTANT NOTE: In case MTN Irancell decide not removing a specific default account, then this account shall be **renamed**.

There is no direct method to perform the schema or username renaming. Oracle does not provide any single command to perform this. There are two indirect ways to perform this. Out of these 2 methods one is not recommended by the Oracle

Renaming a schema is not an easy thing in Oracle. For reasons, unknown Oracle does not allow you to rename a schema by a keyword such as

- `rename old_schema to new_schema;`

  or

  `alter user old_schema rename to new_schema;`

- This facility does not exist in Oracle. There might be some utilities or some undocumented features which might leverage the renaming a schema.

- But if you really want one way to rename the schema go for the traditional way of **exporting** the existing schema and **import** into a new schema. Use clause from user to user while importing.

- But this too is not fully renaming schema as the privileges will not be imported.

Check the follwing link to use the indirect ways (methods) top perform the schema or username renaming:

http://www.acehints.com/2011/06/oracle-9i-10g-11g-methods-to-rename.html

Application

Removal or Disabling of inactive users' procedure at application level is performed per node type and depending on type of Java GUI applications used and administration tools.

References-

Reference Document	Chapter
CPI Library	
AIR User Guide System Administration Tool	4.3.2 Deleting an Existing User
LE OS Hardening Guidelines and Instructions	3 EHardening tool
	7 Operating System Hardening Checklist: - "Unnecessary user accounts disabled" - list
	8 Appendix: Sample Configuration File for EHardening - parameter `AccountListDisableUsers`
SDP User Guide System Administration Tool	4.2 Users
CCN User Administration User Guide	4.3.7 Deleting an Administrator
EMM: User Management Guide	3.1 User Details
	3.1.6 Deleting User

3.1.4 IN_REQ004_v4: Prevent Excessive Privileges on DB Public Roles

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- DB_ACC_010

Internal/External Audit Finding Reference-

Nodes- SDP, ngCRS, ngVS, ECMS, EDA, EMM

Level- Database

High Level Description- Only appropriate privileges must be granted to DB public roles. Excessive granting of unnecessary privileges can compromise security. For example, `SYSDBA` or `SYSOPER` privilege should never be granted to users who do not perform administrative tasks.

Solution Proposed – The `PUBLIC` role is a special role that every database user account automatically has when the account is created. By default, it has no privileges granted to it, but it does have numerous grants, mostly to Java objects.

Database.

a) TimesTen

IMPORTANT NOTE:

Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions[13]. Only `root` and `sdpuser` are to have, and must have, access to the database application.

The `sdpuser` and `root` can no longer be used directly, but only as a role.

While human interaction is prohibited, TimesTen support human interaction using system account i.e. `sdpuser, root`, or internal/external identified individual users.

b) PostgreSQL

Under `GRANT`, the default privileges for any object type normally grant all grantable permissions to the object owner and may grant some privileges to `PUBLIC` as well. However, this behavior can be changed by altering the global default privileges with `ALTER DEFAULT PRIVILEGES`

Example how to remove the public EXECUTE permission that is normally granted on functions, for all functions subsequently created by role admin:

```
ALTER DEFAULT PRIVILEGES FOR ROLE admin REVOKE EXECUTE ON
FUNCTIONS FROM PUBLIC;
```

IMPORTANT NOTE:

PostgreSQL grants default privileges on some types of objects to PUBLIC.

[13] *The database is protected by standard Linux user privileges, which means that no individual users have permissions to access the database. Only root and sdpuser are to have, and must have, access to the database application.*

No privileges are granted to PUBLIC by default on tables, table columns, sequences, foreign data wrappers, foreign servers, large objects, schemas, or tablespaces.

For other types of objects, the default privileges granted to `PUBLIC` are as follows: `CONNECT` and `TEMPORARY` (create temporary tables) privileges for databases; `EXECUTE` privilege for functions; and `USAGE` privilege for languages and data types (including domains).

If the “Access privileges” column is empty for a given object, it means the object has default privileges (that is, its privileges column is null).

Default privileges always include **all privileges for the owner**, and can include some privileges for PUBLIC depending on the object type

The system tables are present in the `pg_catalog` database.

c) Cassandra

Public Roles are not available in Cassandra

Permissions can be verified by using the following command:

```
cqlsh> LIST ALL PERMISSIONS OF cassandra;
```

The creator of a role (the role the database user who issues the `CREATE ROLE` statement is logged in as), is automatically granted permissions on it. This enables users with role-creation privileges to also manage the roles they create, allowing them to `ALTER, DROP, GRANT` and `REVOKE` them. This automatic granting of 'ownership' permissions isn't limited to roles either, it also applies to database objects such as `keyspaces, tables` (and soon to user defined functions). This largely removes the requirement to have any active `superuser` roles, which reduces the risk of privilege escalation.

`REVOKE` command is used to revoke any excessive privilege on the DB tables.

NOTE: Customer approval should be taken in case of revoking permissions

References-

Reference Document	Chapter
3PP Library	
Cassandra Query Language v3.2.1	Data Control - Permissions
PostgreSQL 9.0.22 Documentation	5.6. Privileges.

More details are described here:

- http://cassandra.apache.org/doc/old/CQL-2.1.html

d) Oracle

The Privileges granted to public role shall be reviewed and updated accordingly.

3.2 Access Control (ACC): Password Management

3.2.1 IN_REQ015_v4: Assign or Change Password to Default System Account

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_024, DB_ACC_019, DB_ACC_023, APP_ACC_016

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- All default system accounts shall have passwords assigned.

Solution Proposed – The default system accounts at the Operating System, Application and Database Layers shall have passwords assigned where ever applicable.

Check the details of predefined system accounts for each node as depicted in the Table 6 i.e., is the password changeable or not.

The `passwd` command changes passwords for user and group accounts. A normal user can only change the password for his/her own account, the `superuser` (or `root`) can change the password for any account.
The administrator of a group can change the password for the group

NOTE: Using a null password, while convenient, is a highly unsecure practice, as any third party can log in first an access the system using the unsecure username. Always make sure that the user is ready to log in before unlocking an account with a null password**.**

References-

Reference Document	Chapter
CPI Library	
AIR User Guide System Administration Tool	3.2.3 Change Password
CCN Hardening Guidelines and Checklist	3.4.1 First Login Password Change
SDP User Guide System Administration Tool	4 Authority

3.2.2 IN_REQ016_v4: Change Default Passwords after Node Installation/Upgrade

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_024**,** DB_ACC_019, DB_ACC_020, DB_ACC_023, APP_ACC_016

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- Default password for Individual user accounts must be changed at first login. Persistent system accounts, created during installation, hardware swap or upgrade, must be changed after the operation(s) completion Post ICP upgrade the password of the System Accounts would revert to the default values.

Solution Proposed – The procedures for changing default password for persistent system accounts, are the same as in Chapter 3.2.1.
Default password for non-system accounts (existing or new added users) must be changed after Installation or Upgrade

Changing passwords for individual users at first login must be enforced.

Operating System

Accounts which have been created during/after installation or upgrade are required to change/reset their default password. Password will be changed by following command:

```
passwd <username>
```

Individual users shall be enforced to change their password at the next login using `password -f` option.

Database:

a) Oracle

In Oracle Database, database user accounts, including administrative accounts are installed without default passwords.

During installation, either a password of the account (always an administrative account) is created, or Oracle Database installs the default accounts, with their passwords expired.

b) TimesTen

IMPORTANT NOTE:

Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions[14]. Only `root` and `sdpuser` are to have, and must have, access to the database application.

The `sdpuser` and `root` can no longer be used directly, but only as a role.

While human interaction is prohibited, TimesTen support human interaction using system account i.e. `sdpuser, root`, or internal/external identified individual users.

However, in a non-embedded configuration, the `ALTER USER` statement allows a user to change the user's own password. A user with the `ADMIN` privilege can change another user's password.

Database users can be internal or external. Internal users are defined for a TimesTen database.

An external authority defines external users, such as the OS. External users cannot be assigned a TimesTen password.

```
ALTER USER <username> IDENTIFIED BY {password | "password"}
```

c) PostgreSQL

[14] The database is protected by standard Linux user privileges, which means that no individual users have permissions to access the database. Only root and sdpuser are to have, and must have, access to the database application.

The default PostgreSQL user neither requires nor uses a password for authentication. Instead, depending how PostgreSQL was originally installed and what version you are using, the default authentication method will either be `ident`[15] or `md5`[16]

From the `psql` prompt, issue the `ALTER USER` command to change the password for the PostgreSQL user

```
alter user <user_name> with password '<password>';
```

Another command for changing the password is

```
password <user_name>.
```

d) Cassandra

Superusers can change a user's password or `superuser` status. To prevent disabling of superusers, superusers cannot change their own `superuser` status. Ordinary users can change only their own password.

The following link provides more information about the subject:

https://docs.datastax.com/en/cql/3.1/cql/cql_reference/alter_user_r.html

d) MySQL

The SET PASSWORD statement assigns a password to a MySQL user account, specified as either a cleartext (unencrypted) or encrypted value:

'auth_string' represents a cleartext password.

'hash_string' represents an encrypted password

Application:

The password for the accounts can be changed at application level, performed per node type, and depending on type of Java GUI applications used and administration tools.

NOTE:

[15] *By using this option, the PostgreSQL Database obtains the operating system user name of the client by contacting the ident server on the client and checks if it matches the requested database user name. Ident authentication can only be used on TCP/IP connections*.

[16] *This option requires the client to supply an MD5-encrypted password for authentication*.

Using a null password, while convenient, is a highly unsecure practice, as any third party can log in first an access the system using the unsecure username. Always make sure that the user is ready to log in before unlocking an account with a null password**.**

References-

Reference Document	Chapter
CPI Library	
CCN Hardening Guidelines and Checklist	3.4.1 First Login Password Change
AIR User Guide System Administration Tool	3.2.3 Change Password
SDP User Guide System Administration Tool	4 Authority
3PP Library	
CIS Oracle Database 11g R2 Benchmark V2.0.0	1.2 Ensure All Default Passwords Are Changed

3.2.3 IN_REQ017_v4: Change default ILOM password

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_024

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- The HP ProLiant Server comes preconfigured with default ILOM user account and password. Default password must be changed.

Solution Proposed –. Default password must be changed via login to the HP ProLiant Server ILOM with the default user name `administrator` and the password `hpinvent`. If the default password isn't changed, any attacker or curious individual can access the server.

The following link gives more information on it:

https://support.hpe.com/hpsc/doc/public/display?docId=c03334051

References-

Reference Document	Chapter
3PP Library	
HPE iLO 4 User Guide	Editing local user accounts

3.2.4 IN_REQ018_v4: Set Password Aging

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag-: OS_ACC_019, OS_ACC_020, OS_ACC_022, DB_ACC_013, DB_ACC_015, DB_ACC_016, DB_ACC_018, APP_ACC_007, APP_ACC_008, APP_ACC_015

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- While changing the existing password, the new password shall comply to the MTN baseline password ageing policy (requirements) as stated above in Requirement Tag.

The password ageing i.e. restrictions and expiry shall be applied at Operating System, Database, and Application level wherever applicable.

Solution Proposed - The maximum period, that a user's password can be in effect before it must be changed should be set in days

The number of previous passwords that are stored and which a user is prevented from using should be set. For example, if this is set to 10, then the system prevents a user from reusing any of their previous 10 passwords.

Operating System

a) RHEL/SUSE

1. Default password expiry period for new accounts

Option 1: EHardening or MM_Utility Tool

EHardening Tool

The following parameters can be set by running ConfigEngine with EHardeningSetup module:

- The maximum number of earlier used passwords which cannot be reused

- The maximum number of weeks until a password change is requested
- The maximum number of weeks until a password change is mandated

MM_Utility Tool

The following parameters can be set by running Multi Mediation Utility Manager i.e. `/MM_UTILITY`

- `PasswordAgingMaxDays`

This variable contains a value specifying the maximum number of days' passwords remain valid before users change them.

- `PasswordAgingMinDays`

This variable contains a value specifying the minimum number of weeks' passwords remain valid before users change them.

- `PasswordAgingWarnDays`

This variable contains a value specifying the number of days before passwords expire and users are warned.

Option 2: CLI

The following parameter can be updated in the file `/etc/login.defs` file:

- `PASS_MIN_DAYS`

The minimum time before the password can be changed.

- `PASS_MAX_DAYS`

The maximum number of weeks until a password change is mandated.

- `PASS_WARN_AGE`

The WARN_AGE option is the number of days prior to the password expiring that a user will be warned his/her password is about to expire.

Option 3: Using PAM configuration files

The following parameter must be updated in the file `/etc/pam.d/system-auth-ac` and `/etc/pam.d/password-auth-ac`:

```
password sufficient pam_unix.so sha512 shadow nullok
try_first_pass use_authtok remember=<numeric_value>
```

The details of the above-mentioned parameters are described in Table 7

2. Password expiry period and password history for existing non-system user accounts

Password expiry parameters for existing non-system users can be set by the `chage` command.

The `chage` command is restricted to the root user, except for the `-l` option, which may be used by an unprivileged user to determine when his/her password or account is due to expire.

MTN CS security baseline provides values for password restriction settings that shall be used

Database

a) Oracle

As per the standard security policy, users should not use the same password, each time they are required to change it. To ensure that users don't reuse passwords there are two parameters:

```
PASSWORD_REUSE_TIME <value>
PASSWORD_REUSE_MAX <value>
```

Password restriction should not be applied on `DEFAULT or ECMD_DEFAULT` profile, as it would impact the functionality.

b) TimesTen

IMPORTANT NOTE:

Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions[17]. Only `root` and `sdpuser` are to have, and must have, access to the database application.

The `sdpuser` and `root` can no longer be used directly, but only as a role.

While human interaction is prohibited, TimesTen support human interaction using system account i.e. `sdpuser`, `root`, or internal/external identified individual users.

There are no password restrictions to be set for TimesTen accounts (`root`,`sdpuser`).

c) PostgreSQL

[17] *The database is protected by standard Linux user privileges, which means that no individual users have permissions to access the database. Only root and sdpuser are to have, and must have, access to the database application.*

Password expiry is supported in Postgres 9.x. Password expiration date can be changed by using `ALTER ROLE` with. `VALID UNTIL` option. ALTER ROLE changes the attributes of a PostgreSQL role.

Database `superuser` can rename any role. Roles having CREATEROLE privilege can rename non-`superuser` roles. The current session user cannot be altered.
There is No Generic file which can be updated to set the Password Expiry or Restriction Policy parameters for Database Users.

The following link provides all the information you may need about the subject:

https://www.postgresql.org/docs/9.2/static/sql-alterrole.html

d) Cassandra

Password Ageing cannot be set in Cassandra due to the product limitation

d) MySQL

MySQL 5.5 does not support password expiry.

MySQL 5.6 introduces password-expiration capability, to enable database administrators to expire account passwords and require users to reset their password.

Application:

Password ageing at application level is performed per node type and depending on type of Java GUI applications used and administration tools.

References-

Reference Document	Chapter
CPI Library	
AIR Hardening Guideline and Instruction, RHEL	5 Appendix: Hardening Instructions
LE OS Hardening Guidelines and Instructions Common Foundation 2	7 Operating System Hardening Checklist
CCN Hardening Guidelines and Checklist	3.4.4 Enabling Password History
	4 CCN Hardening Checklist
EMM: Hardening Guidelines	2.1.2 Hardening Template
3PP Library	
CIS Oracle Database 11g R2 Benchmark V2.0.0	3.4 Ensure 'PASSWORD_REUSE_MAX' Is Greater than or Equal to '20'

More details are described here:

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Identity_Management_Guide/user-pwdpolicy.html
- http://www.postgresql.org/docs/9.1/static/sql-createrole.html
- http://www.postgresql.org/docs/9.1/static/sql-alterrole.html

3.2.5 IN_REQ019_v4: Set Password Complexity

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_016, OS_ACC_017, OS_ACC_018, OS_ACC_025, OS_ACC_021, OS_ACC_023, APP_ACC_009, APP_ACC_014, DB_ACC_014, DB_ACC_024, DB_ACC_012

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- Set password complexity parameters for all users

Solution Proposed – Password complexity must be applied for the users at Operating System, Application, and Database layers. A password policy minimizes the inherent risk of using simple passwords by ensuring that they meet adequate complexity standards to thwart brute force attacks. They should also be changed frequently enough to mitigate the risk of someone revealing or discovering a password.

Operating System

Option 1: Ehardening or MM_Utility Tool

Ehardening Tool

Password complexity parameters can be set by running `ConfigEngine` with `EHardeningSetup` module and by configuring the `/etc/default/passwd` file via `SystemHardeningSetup.sh` file.

MM_Utility Tool

The following parameters can be set by running Multi Mediation Utility Manager i.e../`MM_UTILITY`.

- `PasswordMinLength`

This variable contains a numeric value specifying the minimum length of a user password.

- `PasswordMinClass`

This variable contains a numeric value specifying the minimum number of classes (numeric, uppercase, lowercase, and others) of characters required for a password.

- `PasswordMaxRepeat`

This variable contains a numeric value specifying the maximum number same characters allowed in the new password.

- `PasswordMaxSequence`

This variable contains a numeric value specifying the maximum number sequential characters allowed in the new password

Option 2: Using PAM

Pluggable authentication module is used on most Linux System to enforce password complexity. Certain parameters must be updated. This module can be plugged into the password stack of a given service to provide some plug-in strength-checking for passwords.

The parameters which must be updated:

- `minlen`

The minimum acceptable size for the new password

- `minclass`

The minimum number of required classes of characters for the new password.

- `difok`

Sets the number of characters that must be different from those in the previous password

- `maxsequence`

Reject passwords which contain monotonic character sequences longer than N (where the specified value is N)

- `maxrepeat`

Reject passwords which contain more than N (where the specified value is N) same consecutive characters.

- `dcredit`

Sets the minimum number of required digits

- `lcredit`

Sets the minimum number of required lowercase letters

- `ucredit`

Sets the minimum number of required uppercase letters

- `ocredit`

Sets the minimum number of required other characters

In RHEL 6 this can be achieved with the `pam_cracklib` module and updating the `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` file to incorporate the below parameters

```
password requisite pam_cracklib.so try_first_pass
retry=<value> difok=<value> ocredit=<value> dcredit=<value>
ucredit=<value> lcredit=<value> minlen=<value>
reject_username maxrepeat=<value>
```

In RHEL 7 this can be achieved with the `pam_pwquality.so` module and updating the `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` file as below:

```
password requisite pam_pwquality.so retry=<value>
```

Additionally, the following parameter must be updated in `/etc/security/pwquality.conf` file with the values as per MTN CS Security Baseline Standards

- `minlen`
- `minclass.`
- `maxsequence`
- `maxrepeat.`
- `dcredit`
- `lcredit`
- `ucredit`
- `ocredit`

The table below demonstrates a brief description of the parameters/options used in the PAM configurations

Table 7:Parameters Used in PAM Configurations

Parameter	Description
`try_first_pass`	This option requests authentication by using the user's initial password.

	Using the initial password means that the user is **not prompted for another password, even if multiple mechanisms are listed** No numeric values are expected for this option.
`retry`	Refer, to the number of chances a user gets to pick a good password before the passwd program aborts. Users can always re-run the passwd program and start over again.
`difok`	Refers to the minimum number of characters that must be different from the previous password.
`ocredit`	Refers to number of Special Characters to be used while setting password
`dcredit`	Refers to number of Numerical Characters to be used while setting password
`ucredit`	Refers to number of Uppercase Alphabetic Characters to be used while setting password
`lcredit`	Refers to number of Lowercase Alphabetic Characters to be used while setting password
`minlen`	Refers to minimum number of characters to be used while setting password
`reject_username`	This option checks whether the name of the user in straight or reversed form is contained in the new password. If it is found the new password is rejected.
`maxrepeat`	This parameter rejects passwords which contain more than N same consecutive characters. The default is 0 which means that this check is disabled.

use_authtok	This option tells pam_unix to not bother doing any of its own internal password checks, which duplicate many of the checks in pam_cracklib, but instead accept the password that the user inputs after it's been thoroughly checked by pam_cracklib
remember	Module pam_cracklib is capable of consulting a user's password "history" and not allowing them to re-use old passwords. However, the functionality for storing the user's old passwords is enabled via the pam_unix module. The value of the "remember" parameter is the number of old passwords being stored for a user & cannot be reused while changing the users' password.

Database

Password complexity is enforced using appropriate configuration settings during or after installation.

a) Oracle

Default password complexity verification routine requires that each password:

- Is a minimum of four characters in length?
- Does not equal the UserID
- Includes at least one alphabet character, one numeric character, and one punctuation mark
- Does not match any word on an internal list of simple words like welcome, account, database, user, and so on.
- Differs from the previous password by at least three characters

Password restriction should not be applied on DEFAULT or ECMD_DEFAULT profile, as it would impact the functionality

b) TimesTen

IMPORTANT NOTE:

Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions[18]. Only `root` and `sdpuser` are to have, and must have, access to the database application.

The `sdpuser` and `root` can no longer be used directly, but only as a role.

While human interaction is prohibited, TimesTen support human interaction using system account i.e. `sdpuser`, `root`, or internal/external identified individual users.

Password complexity cannot be set on TimesTen database.

c) PostgreSQL

Password Complexity can be set in PostgreSQL ONLY if `passwordcheck` module is installed.

The `passwordcheck` module checks users' passwords whenever they are set with `CREATE ROLE` or `ALTER ROLE`. If a password is considered too weak, it will be rejected, and the command will terminate with an error

d) Cassandra

Password Complexity cannot be set in Cassandra due to the product limitation

d) MySQL

Password complexity is introduced in MySQL 5.6 For this plugin must be installed, loaded, and registered in MySQL. Plugins.

NOTE:

The password handling parameter values, are required to be provided by the Customer in compliance with the Information Security Policy (InfoSec)

Application

Password complexity at application level is performed per node type and depending on type of Java GUI applications used and administration tools.

References-

Reference Document	Chapter
CPI Library	

[18] *The database is protected by standard Linux user privileges, which means that no individual users have permissions to access the database. Only root and sdpuser are to have, and must have, access to the database application.*

AIR Hardening Guideline and Instruction, RHEL	5 Appendix: Hardening Instructions
LE OS Hardening Guidelines and Instructions Common Foundation 2	7 Operating System Hardening Checklist
CCN Hardening Guidelines, and Checklist	3.5 Configuring the Password Syntax
	4 CCN Hardening Checklist
OCC Hardening Guideline and Instruction	4.3.3 Password and login Control
EMM: Hardening Guidelines	2.1.2 Hardening Template
3PP Library	
CIS Oracle Database 11g R2 Benchmark V2.0.0	3.8 Ensure 'PASSWORD_VERIFY_FUNCTION' Is Set for All Profiles

More details are described here:

- http://www.postgresql.org/docs/9.1/static/passwordcheck.html

3.2.6 IN_REQ020_v4: Set Password Complexity Verification Function

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_016, OS_ACC_017, OS_ACC_023, OS_ACC_025, OS_ACC_030, DB_ACC_024, APP_ACC_009, APP_ACC_014

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- Setting the password complexity verification functions to enforce the password complexity configured for the different layers.

After setting the password complexity parameters on all three layers, Operating System, Application, and Database, the same must be enabled with password complexity verification function to protect the network from intrusion.

It is recommended for system administrators to verify that the passwords used within an organization are strong ones. Establishing a good password policy from the start is just as critical to security as testing the strength of passwords already in use.

Complexity verification checks that each password is complex and strong enough to provide reasonable protection against intruders who try to break into the system.

Solution Proposed –

Operating System

The PAM (Pluggable Authentication Module) framework enables the admin to configure the use of system entry services (such as, `ftp, login, telnet`, or `rsh`) for user authentication.

For more information, refer to 3.2.5 Set Password Complexity.

Database

a) Oracle

For Oracle database, as per the standard security policy, users should not choose simple dictionary words that are easy to remember, and easy for a hacker to guess.

In Oracle, a PL/SQL script must be set to check the complexity of a user's password.

Password restriction should not be applied on `DEFAULT or ECMD_DEFAULT` profile, as it would impact the functionality

b) TimesTen

IMPORTANT NOTE:

Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions. Only `root` and `sdpuser` are to have, and must have, access to the database application.

The `sdpuser` and `root` can no longer be used directly, but only as a role.

While human interaction is prohibited, TimesTen support human interaction using system account i.e. `sdpuser`, `root`, or internal/external identified individual users.

TimesTen allows connection to the database of these 2 users without a password (i.e. TimesTen is not configured to do the authentication by itself)

c) PostgreSQL

The `passwordcheck` function, supported in PostgreSQL 9.0, checks users' passwords whenever they are set with `CREATE ROLE` or `ALTER ROLE`. If a password is considered too weak, it will be rejected, and the command will terminate with an error.

The following link provides all the information you may need about the subject:

https://www.postgresql.org/docs/9.0/static/passwordcheck.html

d) MySQL

The `validate_password` plugin (available as of MySQL 5.6.6) serves to test passwords and improve security. The plugin exposes a set of system variables that enable you to define password policy.

The following link provides all the information you may need about the subject:

https://dev.mysql.com/doc/refman/5.6/en/validate-password-plugin.html

Application

Password complexity verification at application level is performed per node type and depending on type of Java GUI applications used and administration tools.

References-

Reference Document	Chapter
3PP Library	
CIS Oracle Database 11g R2 Benchmark V2.0.0	3.8 Ensure 'PASSWORD_VERIFY_FUNCTION' Is Set for All Profiles
CCN Hardening Guidelines and Checklist, 19/1553-FAM 901 098/5 Uen J	3.5.5 Check Common Words

More details are described here:

- http://www.postgresql.org/docs/current/static/passwordcheck.html
- http://www.postgresql.org/docs/current/static/runtime-config-client.html#GUC-SHARED-PRELOAD-LIBRARIES
- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Managing_Smart_Cards/Pluggable_Authentication_Modules.html

3.3 Access Control (ACC): System Access Control

3.3.1 IN_REQ026_v4: Disable Direct Root Login in LINUX

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- - OS_ACC_007

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- Direct access to root must be disabled and the user (who have the root role) must obtain root privileges by using the su – command.

Solution Proposed- In Linux the root user has full unrestricted access to the system, for security reason it's not a good idea to have ssh root access enabled for unauthorized users. Because any hacker can try to brute force your password and gain access to your system.

The following are four different ways that an administrator can further ensure that `root` logins are disallowed. These are applicable both for RHEL and SUSE.

Operating System

a) Changing the root shell

To prevent users from logging in directly as root, the system administrator can set the root account's shell to `/sbin/nologin` in the `/etc/passwd` file. This prevents access to the root account through commands that require a shell, such as the `su` and the `ssh` commands.

Disabling the root shell will prevent root access through the GUI, SSH, SCP, SFTP and with `su`., as indicated in above. Table 8 it will not disable sudo or console access however.

b) Disabling root access via any console device (tty)

To further limit access to the root account, administrators can disable root logins at the console by editing the `/etc/securetty` file. This file lists all devices the `root` user can log into.

If the file does not exist at all, the `root` user can log in through any communication device on the system, whether via the console or a raw network interface. This is dangerous, because a user can log in to their machine as root via Telnet, which transmits the password in plain text over the network.

By default, Red Hat Enterprise Linux's `/etc/securetty` file only allows the root user to log in at the console physically attached to the machine.

To prevent the `root` user from logging in, remove the contents of this file by typing the following command at a shell prompt as root:

```
echo > /etc/securetty
```

NOTE: Once this file is emptied, login via root user to the console fails with error "Login incorrect". However, login via normal user to the console succeeds.

IMPORTANT NOTE:

A blank `/etc/securetty` file does not prevent the root user from logging in remotely using the `OpenSSH` suite of tools because the console is not opened until after authentication.

However if the session to the console is closed and re-opened, the `tty` entry for console (i.e: `ttyS1`) is automatically updated in the `/etc/securetty` file

This is because the `init` respawns the `tty-getty` service as per configuartions in `/etc/init/tty.conf` & `/etc/init/serial.conf`

The following message is noticed in the `/var/log/messages` file when the process respawns:

```
m init: serial (ttyS1) main process ended, respawning
```

c) Disabling root SSH logins

To prevent root logins via the SSH protocol, edit the SSH daemon's configuration file, `/etc/ssh/sshd_config`, and change the value of the parameter `"PermitRootLogin"` to `"no"`

Restart of `sshd` service is required when changes are performed in the SSH Configurations.

d) Using PAM to limit root access to services

PAM, through the `/lib/security/pam_listfile.so` module, allows great flexibility in denying accounts. The administrator can use this module to reference a list of users who are not allowed to log in. To limit root access to a system service, edit the file for the target service in the `/etc/pam.d/` directory and make sure the `pam_listfile.so` module is required for authentication.

Table 8 describes ways that an administrator can further ensure that root logins are disallowed:

Table 8:Methods of Disallowing the Root Access

Method	Description	Effects	Does Not Affect

Changing the root shell	Edit the `/etc/passwd` file and change the shell from `/bin/bash` to `/sbin/nologin`	Prevents access to the root shell and logs any such attempts. The following programs are prevented from accessing the root account: `login, gdm, kdm, xdm, su, ssh, scp, sftp`	Programs that do not require a shell, such as FTP clients, mail clients, and many setuid programs. The following programs are not prevented from accessing the root account: `sudo, FTP` clients, `Email` clients
Disabling root access via any console device (tty)	An empty `/etc/securetty` file prevents root login on any devices attached to the computer	Prevents access to the root account via the console or the network. The following programs are prevented from accessing the root account: `login, gdm, kdm, xdm`, another network service that open a tty	Programs that do not log in as root but perform administrative tasks through setuid or other mechanisms. The following programs are *not* prevented from accessing the root account: `su, sudo, ssh, scp, sftp`
Disabling root SSH logins	Edit the `/etc/ssh/sshd_config` file and set the `PermitRootLogn` parameter to `no`	Prevents root access via the OpenSSH suite of tools. The following programs are prevented from accessing the root account: `ssh, scp, sftp`	This only prevents root access to the `OpenSSH` suite of tools
Use PAM to limit root access to services	Edit the file for the target service in the `/etc/pam.d/` directory. Make sure the `pam_listfile.o` is required for authentication	Prevents root access to network services that are PAM aware. The following services are prevented from accessing the root account: FTP clients, Email clients, `login, gdm kdm, xdm, ssh, scp, sftp,`	Programs and services that are not PAM aware

		Any PAM aware services	

NOTE: While you have disabled for example directly using SSH to log in to the server as root, this of course does not mean that you want to disable root-level functions entirely. A new user (s) must be created just for SSH purposes and be allowed to switch to root once logged in.

Root privileges can be delegated out to other user accounts as required. As a best practice you do not want to provide the root password to multiple users as it makes auditing and tracking who is doing what with the account more difficult. To provide root access to other users, the user account can be added to the `sudoers` file which will grant them root privileges.

See details in below link:

https://www.rootusers.com/23-hardening-tips-to-secure-your-linux-server/

References-

Reference Document	Chapter
CPI Library	
AIR Hardening Guideline and Instruction, RHEL	5 Appendix: Hardening Instructions
TSP Node Hardening Guideline, and Instruction	3.3.4 IO Login Restriction
3PP Library	
CIS Red Hat Enterprise Linux 6 Benchmark, V1.4.0	6.2.8 Disable SSH Root Login
	6.4 Restrict root Login to System Console
CIS Red Hat Enterprise Linux 7 Benchmark, V1.1.0	6.2.8 Disable SSH Root Login
Red Hat Enterprise Linux 6.8 Security Guide	2.1.9.2. Disallowing Root Access
Red Hat Enterprise Linux 7: Security Guide	4.2 Controlling Root Access
CIS SUSE Linux Enterprise Server 12 Benchmark v1.0.0	9.2.8 Disable SSH Root Login (Scored)
	9.4 Restrict root Login to System Console

3.3.2 IN_REQ027_v4: Disallow Root Access via FTP

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- - OS_ACC_009

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- FTP access for root user should be disabled. Any critical files on the node can be transferred if root user has access to FTP.

Solution Proposed –

Any user name added to `/etc/vsftpd/user_list` or `/etc/vsftpd/ftpusers` file will prevent them from logging via FTP protocol

The `/etc/vsftpd/ftpusers` file lists names of users who are not allowed to log in to the FTP server. When login is attempted, the FTP server checks the `/etc/vsftpd/ftpusers` file to determine whether the user should be denied access. If the user's name is not found in that file, the server then searches the `/etc/vsftpd/user_list` file.

Operating System.

a) RHEL

Configuration files `/etc/pam.d/vsftpd`,`/etc/vsftpd/vsftpd.conf` and `/etc/vsftpd/ftpusers` must be updated and the `vsftpd` service should be restarted.

b) SUSE

Configuration files `/etc/pam.d/vsftpd`, `/etc/vsftpd.conf` and `/etc/ftpusers` must be updated and the `vsftpd` service should be restarted.

NOTE:

VSFTPD package is required for FTP Server. If it is missing, it must be installed

References-

Reference Document	Chapter
3PP Library	
Red Hat Enterprise Linux 6.8 Deployment Guide	21.2.2.5 Files Installed with vsftpd

3.3.3 IN_REQ028_v4: Disable Anonymous FTP Login

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_HARD_011

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- Anonymous FTP logins should be disabled.

Solution Proposed- By default anonymous FTP is enabled on the OS layer. This will be disabled by updating the `/etc/vsftpd/vsftpd.conf` files. It is not recommended to use anonymous FTP since it allows unauthorized users to access FTP without identifying themselves. This is a security risk.

Operating System.

a) RHEL/SUSE

By enabling anonymous access in Linux FTP Server (`vsftpd`) anyone can access the ftp server by using the username "Anonymous". If anonymous user is enabled anyone can log in without password. It´s not secure in publicly accessible ftp servers. Disabling anonymous access is recommended.

Disable anonymous access in FTP Server by setting `anonymous_enable=NO` in the `/etc/vsftpd/vsftpd.conf` file.

If desired to access ftp server as a local user, local user must be enabled before that by setting `local_enable=YES`.

Save the `vsftpd.conf` file and restart the `vsftpd` daemon.

References-

Reference Document	Chapter
3PP Library	
System Administration Guide: Network Services	28 Administering the FTP Server (Tasks) - Controlling FTP Server Access
Red Hat Enterprise Linux 6.8: Deployment Guide	21.2.2.6.2. Log in Options and Access Controls
Red Hat Enterprise Linux 6.8 Security Guide	2.1.9.2. Disallowing Root Access
	2.2.6.3. User Accounts

	2.2.6.3.1. Restricting User Accounts

3.3.4 IN_REQ029_v4: Use of SSH Key Based Authentication

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_010, OS_ACC_011

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- SSH keys provide an easy, yet extremely secure way of logging into servers. SSH encryption keys must be generated for UNIX/Linux users', which will be used for users' authentication. Password less ssh connection shall be made from the local system to the concerned node.

Solution Proposed- SSH key pairs are two cryptographically secure keys that can be used to authenticate a client to an SSH server. Each key pair consists of a public key and a private key.

The private key is retained by the client and should be kept secret. Any compromise of the private key will allow the attacker to log into servers that are configured with the associated public key without additional authentication. As an additional precaution, the key can be encrypted on disk with a passphrase.

The public key is uploaded to a remote server that you want to be able to log into with SSH. The key is added to a special file within the user account you will be logging into called `~/.ssh/authorized_keys`.

When a client attempts to authenticate using SSH keys, the server can test the client on whether they are in possession of the private key. If the client can prove that it owns the private key, a shell session is spawned, or the requested command is executed.

NOTE: MTN Irancell must provide details of the UNIX/Linux server, individual UNIX /Linux user (client) from where `ssh` key based authentication to the concerned node must be initiated.

References-

Reference Document	Chapter
CPI Library	

RHEL6 Deployment Guide	14.2.4. USING KEY-BASED AUTHENTICATION

More details are described here:

- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/s2-ssh-configuration-keypairs

3.3.5 IN_REQ030_v4: Configure the SSH Session Timeout

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_027

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- Setting a distinct timeout period for SSH connections on your server is an important and simple step for maintaining both server stability and security.

Solution Proposed – When a client remotely connects via SSH to your (properly configured) Linux-based server, the server will execute a series of KeepAlive requests to connected clients at designated intervals. Upon each execution, the server sends a packet to the client to verify that the client connection is still valid and functional. Should this KeepAlive packet exchange ever fail the server can automatically sever that connection. To ensure your server terminates any SSH clients that do not respond properly you must edit your `/etc/ssh/sshd_config` file.

Operating System

a) RHEL/SUSE

The following parameters must be updated in `/etc/ssh/sshd_config` file.

- `ClientAliveInterval`

Sets a timeout interval in seconds after which if no data has been received from the client, `sshd` will send a message through the encrypted channel to request a response from the client. The default value is 0, indicating that these messages will not be sent to the client.

- `ClientAliveCountMax`

Sets the number of client alive messages which may be sent without sshd receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, `sshd` will disconnect the client, terminating the session. The default value is 3.

NOTE:

The timeout interval is given in seconds. To have a timeout of 5 minutes, set interval to 300. SSH Service must be restarted to have this configuration into effect.

References-

Reference Document	Chapter
CPI Library	
TSP Node Hardening Guideline and Instruction	3.3.14 Configuring SSH session Timeout
3PP Library	
CIS Red Hat Enterprise Linux 7 Benchmark, V1.1.0	6.2.12 Set Idle Timeout Interval for User Login
CIS SUSE Linux Enterprise Server 12 Benchmark v1.0.0	9.2.12 Set Idle Timeout Interval for User Login (Scored)

3.3.6 IN_REQ031_v4: Disable/Configure Weak SNMP Community String

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_HARD_004

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- SNMPv1 and SNMPv2c use a weak community string that provides a weak form of access control. SNMPv3 provides much improved access control using strong authentication and should be preferred over SNMPv1 and SNMPv2c wherever it is supported.

Solution Proposed- SNMP community string is used in SNMPv1 and SNMPv2. If SNMPv1 or SNMPv2 is used, weak community string (public, private) should be replaced with stronger community string.

It is recommended to use either: SNMPv3 OR SNMPv3 with ESA (Ericsson SNMP Agent) as SNMPv3 uses username/password authentication, along with an encryption key**.**

It is recommended to use either:

SNMPv3 without ESA

OR

SNMPv3 with ESA (Ericsson SNMP Agent*)*

NOTE:

The following should be considered during MBSS development, Detailed Security Design chapter:

- Ericsson SNMP Agent (ESA) not in use
- Ericsson SNMP Agent (ESA) in use – SNMPv3 configuration (`unique string`)

References-

Reference Document	Chapter
CPI Library	
SDP Network Configuration	4.3 ESA
SDP Network Configuration, RHEL	4.3 ESA
AIR Network Configuration, Linux	5.4 ESA
AIR Network Configuration, Solaris	5.4 ESA
TSP Node Hardening Guideline and Instruction	3.3.12 Restricting SNMPv2 Access
	3.3.13 Configuring SNMPv3 Access
EMM8, System Administrator's Guide for Linux	13 Alarm Configuration[19]
EMM8, System Administrator's Guide for Solaris	13 Alarm Configuration
EMM7 – F&E, Network Element Description	3.9 Alarm Handling
EMM 7 – Online Mediation, Network Element Description	3.8 Alarm Management
EMM 7 – Online Mediation, User's Guide, Online Mediation	7.6 Alarm Distribution Settings
Ericsson SNMP Agent 4.0, ESA Setup, and Configuration	4.4 Community Strings

[19] *Support for hardware alarms are introduced in EMM8 using Ericsson SNMP Agent (ESA). ESA replaces Emanate/Adventnet for sending alarms over SNMP.*

3.3.7 IN_REQ032_v4: Set Account Lockout Threshold for Invalid Logon Attempts

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- - OS_ACC_005, DB_ACC_011, APP_ACC_003, DB_ACC_017

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- User account gets locked out automatically after 3 invalid or failed logon attempts

Solution Proposed- Brute force is a method to find a user's password by trying to login with various password combinations. By having a password lockout policy such users can be locked out of their account if a certain number of incorrect passwords are entered

Operating System

a) RHEL

Option 1: Ehardening or MM_Utility Tool

Ehardening Tool

Account lockout parameters can be set by running `ConfigEngine` with `EHardeningSetup` module.

MM_Utility Tool

The below parameter can be set by running Multi Mediation Utility Manager i.e. `/MM_UTILITY`

- `LoginMaxRetries`

This variable contains a numeric value specifying the number of consecutive failed login attempts. If the login fails after maximum retries, the account will be locked.

Option 2: CLI

Linux uses a configuration file to control login attributes of its users. This file is `/etc/login.defs`. Variables that control how the login process works include `FAIL_DELAY, LOGIN_RETRIES, LOGIN_TIMEOUT` and `FAILLOG_ENAB`.

- The `FAIL_DELAY` variable acts the same as the `SLEEPTIME` above.
- The `LOGIN_RETRIES` works the same way as the `RETRIES` variable above.
- The `LOGIN_TIMEOUT` works the same way as the `DISABLETIME` variable above.
- The `FAIL_DELAY` variable instructs the `syslog daemon` to log failure of attempts to log in.

Option 3: Using PAM configuration files

Linux password lockout policy can be configured using PAM (Pluggable Authentication Modules) to lock a user's account temporarily if they attempt to brute force into an account by trying various password combinations. This configuration uses the `pam_faillock`.so module.

The below line should be updated in `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` files

```
auth        required      pam_faillock.so preauth silent
audit deny=<value> unlock_time=<value>
```

The details of the parameters are described in Table 7

Database

a) *Oracle*

The maximum times a user login can fail before locking the account can be set by configuring the `FAILED_LOGIN_ATTEMPTS` parameter.

a) TimesTen

IMPORTANT NOTE:

Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions[20]. Only `root` and `sdpuser` are to have, and must have, access to the database application.

The `sdpuser` and `root` can no longer be used directly, but only as a role.

While human interaction is prohibited, TimesTen support human interaction using system account i.e. `sdpuser`, `root`, or internal/external identified individual users.

[20] *The database is protected by standard Linux user privileges, which means that no individual users have permissions to access the database. Only root and sdpuser are to have, and must have, access to the database application.*

However, in a non-embedded configuration External user accessing the database (if `root` and `sdpuser` privileges were assigned to those users) are authenticated through an external service. This external service can be the operating system or a network service, such as Oracle Net. If operating system or network service permits, then it can authenticate users before they can log in to the database.

Since external user authentication is performed at the Operating System (OS) level, a failure login attempt that exceed the threshold will result in a locked account.

b) *PostgreSQL*

Account lockout threshold cannot be set on PostgreSQL due to product limitation

c) Cassandra

Account Lockout Threshold cannot be set in Cassandra due to the product limitation.

d) MySQL

It is also possibly to configure the *"locking out a user after several failed login attempts"* through the following script (example) using `fail2ban` for this goal. In this case you just install it on you Linux OS, then enable the section for `[mysqld-iptables]` in the `/etc/fail2ban/jail.local.`

```
[mysqld-iptables]
enabled = true
filter   = mysqld-auth
action   = iptables [name=mysql, port=3306, protocol=tcp]
sendmail-whois [name=MySQL, dest=root,
sender=fail2ban@example.com]
logpath = /var/log/mysqld.log

maxretry = 5
```

This program checks the mysql logs by its own given pattern and then blocks the IP addresses which they try to login more than 5 times, in iptables

Application

Account Lockout Threshold at application level can be set per node type and depending on type of Java GUI applications used and administration tools.

NOTE:

Regarding Database configuration, this is not applicable for AIR since there is no database in AIR, also not for SDP since TimesTen[21] Database is running in embedded mode.

References-

Reference Document	Chapter
CPI Library	
AIR User Guide System Administration Tool	4.6 Authority Window – General
CCN Hardening Guidelines and Checklist	3.4.6 Locking User for failed password
LE OS Hardening Guidelines and Instructions Common Foundation 2	8 Appendix: Sample Configuration File for Ehardening
SDP Hardening Guideline and Instruction, Sun Solaris	4.3 System Configuration
CCN Hardening Guidelines and Checklist	4 CCN Hardening Checklist
3PP Library	
CIS Red Hat Enterprise Linux 6 Benchmark v1.4.0	6.3.3 Set Lockout for Failed Password Attempts
CIS SUSE Linux Enterprise Server 12 Benchmark v1.0.0	9.3.2 Set Lockout for Failed Password Attempts
CIS Oracle Database 11g R2 Benchmark V2.0.0	3.1 Ensure 'FAILED_LOGIN_ATTEMPTS' Is Less than or Equal to '5'

3.3.8 IN_REQ033_v4: Force System to Prompt for Password in Single User Mode

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_OS_ACC_002, OS_ACC_029

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

[21] *The TimesTen database embedded in SDP is an in-memory SQL database for storage of subscribers and service classes. The database is synchronized between the different SDP servers in the cluster.*

High Level Description- Linux provides so-called "single user mode" or "rescue mode" in which a multi-user Linux system boots into a single user environment with `superuser` privilege. Single user mode mainly used for doing administrative task such as cleaning the file system, Managing the quotas, Recovering the file system, and recover the lost `root` password. In this mode services won't start. None of the users can login except `root` and the system won't ask for password to login

For example, it is used for running `fsck` (which is used to check and repair filesystems) on a `/usr` partition because this requires that the partition be unmounted (i.e., not logically attached to the system). A partition is a logically independent section of a Hard Disk Drive (HDD).

Solution Proposed- Access to Single User Mode must be prevented because if attackers can boot the system into single user mode, they are logged in automatically as root without being prompted for the root password.

Due to security reasons, one may want to force system to prompt for root password even in Single User mode.

In RHEL6, edit `/etc/inittab` and add `"su:S:wait:/sbin/sulogin"` before `'initdefault'` line.

Additionally, edit the `/etc/sysconfig/init` file and replace `SINGLE=/sbin/sushell` with `SINGLE=/sbin/sulogin.`

In RHEL7, by default, Single User mode is password protected by the root password.

The following link (Chapter 24 .9.4. Changing and Resetting the Root Password) provides more information you may need about the subject:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/pdf/system_administrators_guide/Red_Hat_Enterprise_Linux-7-System_Administrators_Guide-en-US.pdf

In SUSE it includes the following entry in the`/etc/inittab` file to ensure that a root password is required for Single User Mode logins:
`~~:S:respam:/sbin/sulogin.`

IMPORTANT NOTE: Secure the boot loader (Grub menu) with password in RHEL 6. It is also possible to use GRUB menu where to put the password so that no one logs in to single user mode without permission.

References-

Reference Document	Chapter

3PP Library	
SUSE Documentation: Security and Hardening Guide	Single User Mode Password for root

More details are described here:

- https://www.suse.com/documentation/sles11/book_hardening/data/sec_sec_prot_general_single_user.html

3.3.9 IN_REQ034_v4: Enable Database Authentication

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- DB_ACC_019, DB_ACC_023, DB_ACC_020

Internal/External Audit Finding Reference-

Nodes- SDP, ngCRS, ngVS, ECMS, EDA, EMM

Level- Database

High Level Description- Database authentication is the process or act of confirming that a user who is attempting to log in to a database is authorized to do so and is only accorded the rights to perform activities that he or she has been authorized to do.

Solution Proposed – Authentication acquires one more dimension because it may happen at different levels. The database may perform it itself, or the setup may be changed to allow either the operating system, or some other external method, to authenticate users**.**

Database

a) Oracle

Oracle provides a more secure authentication scheme for database administrator usernames. It's possible to choose between operating system authentication and password files to authenticate database administrators.

b) *TimesTen*

IMPORTANT NOTE:

Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions[22]. Only `root` and `sdpuser` are to have, and must have, access to the database application.

The `sdpuser` and `root` can no longer be used directly, but only as a role.

While human interaction is prohibited, TimesTen support human interaction using system account i.e. `sdpuser, root`, or internal/external identified individual users.

However, in a non-embedded configuration "**Authenticate**" attribute can't be set

c) *PostgreSQL*

In PostgreSQL the following authentication methods are supported:

- Trust Authentication

When trust authentication is specified, PostgreSQL assumes that anyone who can connect to the server is authorized to access the database with whatever database user name they specify (even `superuser` names). Of course, restrictions made in the database and user columns still apply. This method should only be used when there is adequate operating-system-level protection on connections to the server.

- Password Authentication

There are several password-based authentication methods. These methods operate similarly but differ in how the users' passwords are stored on the server and how the password provided by a client is sent across the connection.

`scram-sha-256`

The method `scram-sha-256` performs SCRAM-SHA-256 authentication. It is a challenge-response scheme that prevents password sniffing on untrusted connections and supports storing passwords on the server in a cryptographically hashed form that is thought to be secure.

This is the most secure of the currently provided methods, but it is not supported by older client libraries.

`md5`

[22] *The database is protected by standard Linux user privileges, which means that no individual users have permissions to access the database. Only root and sdpuser are to have, and must have, access to the database application.*

The method `md5` uses a custom less secure challenge-response mechanism. It prevents password sniffing and avoids storing passwords on the server in plain text but provides no protection if an attacker manages to steal the password hash from the server. Also, the `MD5` hash algorithm is nowadays no longer considered secure against determined attacks.

The `md5` method cannot be used with the `db_user_namespace` feature.

To ease transition from the md5 method to the newer SCRAM method, if md5 is specified as a method in `pg_hba.conf` but the user's password on the server is encrypted for SCRAM (see below), then SCRAM-based authentication will automatically be chosen instead.

`password`

The method password sends the password in clear-text and is therefore vulnerable to password “sniffing” attacks. It should always be avoided if possible. If the connection is protected by SSL encryption then password can be used safely, though. (Though SSL certificate authentication might be a better choice if one is depending on using SSL).

- GSSAPI Authentication

GSSAPI is an industry-standard protocol for secure authentication defined in RFC 2743. PostgreSQL supports GSSAPI with Kerberos authentication per RFC 1964.

- SSPI Authentication

SSPI is a Windows technology for secure authentication with single sign-on. PostgreSQL will use SSPI in negotiate mode, which will use Kerberos when possible and automatically fall back to NTLM in other cases.

- Ident Authentication

The ident authentication method works by obtaining the client's operating system user name from an ident server and using it as the allowed database user name (with an optional user name mapping). This is only supported on TCP/IP connections.

- Peer Authentication

The peer authentication method works by obtaining the client's operating system user name from the kernel and using it as the allowed database user name (with optional user name mapping). This method is only supported on local connections.

- LDAP Authentication

This authentication method operates similarly to password except that it uses LDAP as the password verification method. LDAP is used only to validate the user name/password pairs. Therefore, the user must already exist in the database before LDAP can be used for authentication.

- RADIUS Authentication

This authentication method operates similarly to password except that it uses RADIUS as the password verification method. RADIUS is used only to validate the user name/password pairs. Therefore, the user must already exist in the database before RADIUS can be used for authentication.

- Certificate Authentication

This authentication method uses SSL client certificates to perform authentication. It is therefore only available for SSL connections. When using this authentication method, the server will require that the client provide a valid, trusted certificate. No password prompt will be sent to the client.

- PAM Authentication

This authentication method operates similarly to password except that it uses PAM (Pluggable Authentication Modules) as the authentication mechanism. The default PAM service name is `PostgreSQL`. PAM is used only to validate user name/password pairs and optionally the connected remote host name or IP address. Therefore, the user must already exist in the database before PAM can be used for authentication.

- BSD Authentication

This authentication method operates similarly to password except that it uses BSD Authentication to verify the password. BSD Authentication is used only to validate user name/password pairs. Therefore, the user's role must already exist in the database before BSD Authentication can be used for authentication.

d) Cassandra

To configure Cassandra to use internal authentication, first make a change to the `cassandra.yaml` file and increase the replication factor of the `system_auth keyspace`, Then, startup Cassandra using the default user name and password (cassandra/cassandra), and start cqlsh using the same credentials.

Change the authenticator option in the `cassandra.yaml` file to `PasswordAuthenticator.`

By default, the authenticator option is set to `AllowAllAuthenticator`

e) MySQL

There are several different situations where a user or dba may require identifying how a user is connecting to the server and what authentication method was used. Depending whether the user has connected directly with an account that is specified in the `mysql.user` table or whether the user is via proxy user will vary how to determine these details.

To identify the authentication method for their existing connection the following query can be used:

```
mysql> SELECT USER (), CURRENT_USER (), @@PROXY_USER;
```

More details are here:

https://dev.mysql.com/doc/refman/5.5/en/pluggable-authentication.html

3.3.10 IN_REQ035_v4: Prevent Direct Login to the Database

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- DB_ACC_001, DB_ACC_002

Internal/External Audit Finding Reference-

Nodes- SDP, ngCRS, ngVS, CCN, EDA, EMM

Level- Database

High Level Description – The Database should listen for TCP/IP connections only on the approved addresses and not all (0.0.0.0/0)

Solution Proposed – Connection attempts made to the Database using TCP/IP should be allowed only from authorized hosts

Database

a) Oracle

If the user specifies a host name for the HOST parameter in the ADDRESS line of the `listener.ora` file, the listener listens on IN_ADDRANY in case the host name is default host name.

If the user wants the listener to listen on the first IP to which the specified host name resolves, the address must further be qualified with `(IP=FIRST)`.

This feature is disabled by default.

CAUTION:

Current configuration in the `listener.ora` should be considered before modifying the same to maintain product functionality.

b) TimesTen

By default, a server process is spawned at the time a client requests a connection. By setting the `-serverPool` option in the `ttendaemon.options` file on the server system, a reserve pool of server processes can be pre-spawned.

The following Table describe the communication protocols that the TimesTen Client can use with the TimesTen Server:

Table 9 Communication Protocols-TimesTen

Communication Type	Description
TCP/IP Communication	The TimesTen Client communicates with the TimesTen Server using TCP/IP sockets. This is the only form of communication available when the TimesTen Client and Server are installed on different systems.
Shared memory communication	If both the TimesTen Client and Server are installed on the same system, applications using the TimesTen Client ODBC driver may use a shared memory segment for inter-process communication (IPC). Using a shared memory segment provides better performance than TCP/IP communication. To use this, set the Network Address of the logical server as `ttShmHost`.
UNIX domain socket communication	If both the TimesTen Client and Server are installed on the same system, the UNIX domain sockets can be used for communication. To use this, set the Network Address of the logical server as `ttLocalHost`.

IMPORTANT NOTE:

Human interactions with TimesTen database are not allowed as per node Hardening Guideline & Instructions[23]. Only `root` and `sdpuser` are to have, and must have, access to the database application locally.

The `sdpuser` and `root` can no longer be used directly, but only as a role.

c) PostgreSQL

The parameter "`host`" in `pg_hba.conf` file defines the connection attempts made using TCP/IP in PostgreSQL.

The "`address`" field of the "`host`" parameter specifies the IP address range using standard numeric notation for the range's starting address, then a slash (/) and a CIDR mask length.

Typical examples of an IPv4 address range specified this way are `172.20.143.89/32` for a single host, or `172.20.143.0/24` for a small network, or `10.6.0.0/16` for a larger one.

d) Cassandra

The following parameters should be updated in `cassandra.yaml` file

- `listen_address`

The IP address or hostname that Cassandra binds to for connecting this node to other nodes. Default value is `localhost`

- `rpc_address`

The listen address for client connections. Default value is `localhost`
Valid values:

`unset`: Resolves the address using the configured hostname configuration of the node. If left unset, the hostname resolves to the IP address of this node using /etc/hostname, /etc/hosts, or DNS

`0.0.0.0`: Listens on all configured interfaces. The `broadcast_rpc_address` must be set to a value other than 0.0.0.0

`IP Address`

`Hostname`

[23] *The database is protected by standard Linux user privileges, which means that no individual users have permissions to access the database. Only root and sdpuser are to have, and must have, access to the database application.*

Both the parameter values (`listen_address` and `rpc_address`) should be set to `host1_priv` and the `host1_priv` should be defined in `/etc/hosts` file

References-

Reference Document	Chapter
3PP Library	
Oracle Database Net Services Reference	Address
Oracle TimesTen In-Memory Database Operations Guide	Communication protocols for Client/Server communication
Security Hardening PostgreSQL	Password Authentication

3.3.11 IN_REQ036_v4: Restrict Mounting of NFS Shares

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_013, OS_ACC_014

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level- Operating System

High Level Description- Possibility to access the remote NFS shares without having root privileges, can lead to a disclosure of sensitive information, or in some conditions the compromise of the host itself.

This could allow, for example, the analyst to mount the home directory of a user and peruse its contents. This could lead to the compromise of information relating to additional remote systems to which the user has valid account on.

Solution Proposed – With NFS we can export directories within a file system over the network to other clients allowing us to share various files over the network. It is important to configure this properly and secure it as much as possible so that only the required clients have access to the NFS share, otherwise it may be possible for anyone to mount it and access the data.

To do this we are going to use the `/etc/exports` file on the NFS server and lock down shares to only be accessible by specific IP addresses**.**

Operating System

a) RHEL/SUSE

The NFS server mount points are configured with the `/etc/exports` file, this file lists the directories that are available to be accessed over NFS. Alternatively, configuration files can also be created within the `/etc/exports.d/` directory if they have the .exports extension.

Below is an example NFS configuration within the `/etc/exports` file.

```
[root@server ~]# cat /etc/exports

/root/nfs       <IP>(rw,async)
```

The `/root/nfs` directory is available only to the IP address<IP>, so only the system at this IP address will be able to successfully access and mount the directory. Hostnames can also be used instead of IP addresses.

After any changes to the `/etc/exports` file we should use the `exportfs` command to update the table of exported NFS file systems. The client systems will also need the `nfs-utils` package installed to be able to mount NFS.

NOTE: There should be no space between the IP address and the options (`rw, sync`), if there was a space here, then the IP address would have default options and the (`rw, sync`) would instead apply to any other client that attempts to access the NFS share, which would essentially give read/write access to anyone.

For CCN, both Linux and Dicos TPs are acting is a NFS clients to access FS and IO files system (system storage, NFS servers) – Using NFSv3

- Check The `/etc/exports` list of entries. It indicates “director (ies)” that is/are shared and how they are shared.

```
Proc_m0_s9# cat /etc/exports
#
# /etc/exports: nfs configuration
#

/opt/mirror 172.16.0.0/21(rw,sync,no_subtree_check,root_squash,insecure,anonuid=101,anongid=501)
/opt/mirror 172.16.8.0/21(rw,sync,no_subtree_check,root_squash,insecure,anonuid=101,anongid=501)
/opt/mirror 172.16.32.0/21(rw,sync,no_subtree_check,root_squash,insecure,anonuid=101,anongid=501)
```

References-

Reference Document	Chapter
CPI Library	
RHEL 6 Security Guide	2.2.4 Securing NFS

More details are described here:

- RHEL6
  http://computernetworkingnotes.com/network-administration/how-to-configure-nfs-server-in-rhel-6.html

- SUSE10
  https://www.suse.com/communities/blog/configuring-nfsv4-server-and-client-suse-linux-enterprise-server-10/

- SUSE11
  https://www.server-world.info/en/note?os=SUSE_Linux_Enterprise_Server_11&p=nfs

- CPI store, File System, Chapter 2 (Function)
  http://cpistore.internal.ericsson.com/alexserv?ac=LINKEXT&li=EN/LZN7410076R13D&FN=52_15517-ANA90105_1Uen.C.html&ORPA=file+system&SL=EN/LZN7410241R3B

3.3.12 IN_REQ038_v4: SDP Dump Tool Configuration and File Transfer Permission

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_OS_AF_002, MTNG_CSBL_NEW_APP_AF_002

Internal/External Audit Finding Reference-

Nodes- SDP

Level- Operating System
High Level Description: The tools that are used to take snapshots/dump of the system are:

- Snapshot

The runscript `dumpSubscribers.ksh`, normally located in

`/opt/sdp/SnapShot/bin` is a shell script which contains all necessary information to create a snapshot of the SDP (SOLARIS/RHEL) database.

- Subscriber Dump Tool

The purpose of Subscriber Dump Tool is to support dump and load of subscriber data from and to an SDP (SOLARIS/RHEL). The tool is available via the command line as `/opt/sdp/DataTool/bin/subscriberDumpTool`.

The tools should be launched as `superuser` who has full authority for all actions in FDS or OS.

Solution Proposed- These tools are executed only by `sdpuser` or `root`. So, the appropriate roles of `sdpuser` or `root` should only be provided to pre-defined users.

Reference-

Reference Document	Chapter
CPI Library	
SDP System Administrator's Guide	7.6.2 Exporting and Importing Service Data
SDP System Administrator's Guide, RHEL	7.5.2 Exporting and Importing Service Data
SDP Data Collection Guideline	3.4.2 Data to Be Collected
SDP User Guide Reports Administration	8.3 Generating a Snapshot
CAL Library	
SDP Implementation Instruction - Subscriber Balancing and Blackbox Migration	3 Description of Subscriber Dump Tool

3.3.13 IN_REQ040_v4: Set Permission for Cron Job File

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_OS_ACC_003

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level- Operating System

High Level Description- The cron service is required by almost all UNIX / Linux OS to schedule necessary tasks. Cron uses specific configuration files and directories. Regular users can modify and install their own cron configuration or jobs.

Solution Proposed- CRON jobs allow system administrators to schedule tasks. The ownership of the configuration files used by the Cron daemon is set to the user running the scheduled job.

The permission of these cron configuration files should have appropriate privilege ONLY to the owner of the job. It is a Security Risk if these files are world writable which allows unauthorized users to add/delete/modify the cron jobs and manipulate the tasks.

Additionally, access to the cron daemon can be controlled by configuring the `/etc/cron.deny` & `/etc/cron.allow` files.

Operating System

a) RHEL

The following list of files and directories are used within cron*:*

- `/etc/crontab` file
- `/etc/cron.hourly` directory
- `/etc/cron.daily` directory
- `/etc/cron.weekly` directory
- `/etc/cron.monthly` directory
- `/etc/cron.d` *directory*

In the `/etc/crontab` file, the run-parts script executes the scripts in the `/etc/cron.hourly/`, `/etc/cron.daily/`, `/etc/cron.weekly/`, and `/etc/cron.monthly/` directories on an hourly, daily, weekly, or monthly basis respectively. The files in these directories should be shell scripts.

If a `cron` task is required to be executed on a schedule other than hourly, daily, weekly, or monthly, it can be added to the `/etc/cron.d/` directory. All files in this directory use the same syntax as `/etc/crontab`.

The `cron` daemon checks the `/etc/crontab` file, the `/etc/cron.d/` directory, and the `/var/spool/cron/` directory every minute for any changes. If any changes are found, they are loaded into memory. Thus, the daemon does not need to be restarted if a `crontab` file is changed.

It’s recommended to restrict read/write and search access to user and group root, preventing regular users from accessing these files/directories.

3.3.14 IN_REQ041_v4: Remove SUID Bit for the Keys Files

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag-: MTNG_CSBL_NEW_OS_ACC_004

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level- Operating System

High Level Description- SUID (set user id) and SGID[24] (set group id) binaries pose a risk of exploitation due to them running as user 'root' or as group 'root' (or some other group or user).

The SUID bit should be set only on files that were installed via authorized means. A straightforward means of identifying unauthorized SGID files is determine if any were not installed as part of an RPM package, which is cryptographically verified. Investigate the origin of any unpackaged SUID files.

Executable files with the SUID permission run with the privileges of the owner of the file. SUID files of uncertain provenance could allow for unprivileged users to elevate privileges. The presence of these files should be strictly controlled on the system.

Solution Proposed- SUID/SGID bits can be misused when the SUID/SGID executable has a security hole. Therefore, you should search the entire system for SUID/SGID executables and document it. For example, ensure that code developers do not set SUID/SGID bits on their programs if it is not an absolute requirement.

In RHEL 6, To search the entire system for SUID or SGID files, you can run the following command:

```
find / -path /proc -prune -o -type f -perm +6000 -ls

find / -path /proc -prune -o -type f -perm +4000 -ls

find / -path /proc -prune -o -type f -perm +2000 -ls
```

The `-prune` option in this example is used to skip the `/proc` filesystem.

In RHEL 7, To search the entire system for SUID or SGID files, you can run the following command:

```
find / -path /proc -prune -o -type f -perm /6000 -ls;
```

[24] SGID (Set Group ID up on execution) is a special type of file permissions given to a file/folder. Normally in Linux/Unix when a program runs, it inherit's access permissions from the logged in user. SGID is defined as giving temporary permissions to a user to run a program/file with the permissions of the file group permissions to become member of that group to execute the file. In simple words users will get file Group's permissions when executing a Folder/file/program/command.

SGID is like SUID. The difference between both is that SUID assumes owner of the file permissions and SGID assumes group's permissions when executing a file instead of logged in user inherit permissions.

```
find / -path /proc -prune -o -type f -perm /4000 -ls;

find / -path /proc -prune -o -type f -perm /2000 -ls;
```

IMPORTANT NOTE:

Very often you can use workarounds like removing the executable bit for world/others. However, a better approach is to change the design of the software if possible.

References-

Reference Document	Chapter
3PP Library	
CIS Red Hat Enterprise Linux 6 Benchmark: 1.1 Filesystem Configuration	9.1.13 Find SUID System Executables (Not Scored), and 9.1.14 Find SGID System Executables (Not Scored)
How to Set and View StickyBit, SUID & SGID in Linux with Examples	What is SUID Bit and How to set it How SGID Bit work on file and directory
Security and Hardening Guide: SUSE Linux Enterprise Server 11-12 SP2	UID/SGID Files

More details are described here:

- https://linoxide.com/how-tos/stickbit-suid-guid/
- https://www.suse.com/documentation/sles-12/pdfdoc/book_hardening/book_hardening.pdf

3.3.15 IN_REQ042_v4: Set Default Shell for User/Service Accounts to Null

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag-: MTNG_CSBL_NEW_OS_ACC_005

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level- Operating System

High Level Description- Default shell for user and service accounts should be set to null. Negligence of this will lead to malicious file substitution and service user can find a way to login and continue to elevate their privilege

Solution Proposed- Most Linux systems use either `/sbin/nologin` or `/bin/false` as the **default shell** for service accounts. Many hardening guides, such as CIS benchmarks, recommend changing the default shell for these accounts to `/dev/null`).

a) How to prevent non-root users from login into the system using nologin shell

The `/sbin/nologin` command refuse a login. It displays a message that an account is not available and exits non-zero. This is preferred method these days to deny login access to account.

```
# usermod -s /sbin/nologin <user_name>
```

The `/bin/false` is **old** method which does nothing and always return unsuccessful code. It can be used to deny login access to existing user:

```
# usermod -s /bin/false <user_name>
```

The /`etc/passwd` file can be updated where shell for the user can be changed:

From
`/bin/bash`

To
`/sbin/nologin`

Following program will not affected by this shell (`/sbin/nologin`):

- FTP clients
- Mail clients
- Sudo
- SetUID programs

Please note that it prevents access to the shell and logs the attempt. All the following programs are prevented from accessing the user account:
`telnet/login, gdm/kdm/xdm (graphical login), su, ssh/scp/sftp, etc`

b) How to disable user shell for security reasons

User accounts created for automated tasks may require fine-grained permissions, such as file transfer across systems, monitoring, etc.

Changing the login shell does not necessarily prevent users from **authenticating** (except in some services that check if the user's shell is mentioned in `/etc/shells`).

Changing the shell to `/bin/false` or `/usr/sbin/nologin` will ONLY prevent them from running commands on those services that can be used to run commands (`console login, ssh, telnet, rlogin, rexec`...), so affect authorization for some services only.

References-

Reference Document	Chapter
3PP Library	
Linuxtopia: Red Hat Enterprise Linux 6 Essentials eBook	15.3. Standard Users
pam_listfile - deny or allow services based on an arbitrary file Chapter 6. A reference guide for available modules	6.16. pam_listfile - deny or allow services based on an arbitrary file
Linux PAM configuration that allows or deny login via the sshd server	How do I configure pam_listfile.so module to deny access?

More details are described here:

- http://www.linuxtopia.org/online_books/rhel6/rhel_6_deployment/rhel_6_deployment_s1-users-groups-standard-users.html
- http://www.linux-pam.org/Linux-PAM-html/sag-pam_listfile.html
- https://www.cyberciti.biz/tips/linux-pam-configuration-that-allows-or-deny-login-via-the-sshd-server.html

3.3.16 IN_REQ043_v4: Set Appropriate Umask Default Value

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_OS_ACC_006

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level- Operating System

High Level Description- The user file-creation mode mask (Umask) is used to determine the file permission for newly created files. It can be used to control the default file permission for new files. It is a four-digit octal number.

Solution Proposed- Default Umask value can be set temporarily or permanently as per requirements for SOLARIS, RHEL and SUSE.

Operating System

To temporarily set the umask value, run the below command on your terminal:

```
# umask new_umask_value

# umask 0077
```

To permanently set the umask value for files/directory creation

Add the umask value to be set inside `~/.bashrc` or `~/.bash_profile` as every time login operation is performed, the above files are executed updating the new umask value.

- A umask of 022 allows only you to write data, but anyone can read data.
- A umask of 077 is good for a completely private system. No other user can read or write your data if umask is set to 077.
- A umask of 002 is good when you share data with other users in the same group. Members of your group can create and modify data files; those outside your group can read data file but cannot modify it. Set your umask to 007 to completely exclude users who are not group members

To understand the difference between. `bashrc` and `.bash_profile` file, refer the below link:

http://www.golinuxhub.com/2013/12/how-to-set-environment-path-variable.html

IMPORTANT NOTE:

If `useradd` command is executed, the home directory created has 700 as default permission which means it does not take the Umask value defined locally. For `useradd` command `umask` value is set differently inside `/etc/login.defs`.

```
# less /etc/login.defs

# The permission mask is initialized to this value. If not
specified,

# the permission mask will be initialized to 022.

UMASK 077
```

References-

Reference Document	Chapter
3PP Library	
CIS Red Hat Enterprise Linux 6 Benchmark v1.4.0	7.4 Set Default umask for Users
CIS SUSE Linux Enterprise Server 12 Benchmark v1.0.0	10.4 Set Default umask for Users

3.3.17 IN_REQ044_v4: Create and Enable Warning Banners

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_HARD_007

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level- Operating System

High Level Description- Warning banners message shall be configured at operating system level.

Solution Proposed- SSH warning banners and welcome messages are necessary when organization wishes to prosecute an unauthorized user or just give out some information or announcement.

There are two ways to display messages one is using `issue.net` file and second one is using `MOTD` file

- `issue.net`: Display a banner message before the password login prompt.
- `motd`: Display a banner message after the user has logged in.

Warning banners can be configured, by updating the related configuration files.

Operating System

a) RHEL

- Terminal access: `/etc/issue, (/etc/issue.net)` and `/etc/motd` files to be updated with proprietary information and legal warning text

- GNOME Users:
  Set `/apps/gdm/simple-greeter/banner_message_enable true`
  `/apps/gdm/simple-greeter/banner_message_text` file to be updated with proprietary information and legal warning text

- VSFTPD: `/etc/vsftpd/vsftpd.conf` file should include
  Option 1
  `ftpd_banner=<insert_greeting_here>`
  if banner is short one or
  Option 2
  `banner_file=/etc/banners/ftp.msg`
  if banner is long one and is saved in `ftp.msg` file in `/etc/banners` directory

- SSH: `/etc/ssh/sshd_config` file should include
  `banner /etc/issue` or
  `banner /etc/issue.net`

b) SUSE

- Terminal access: `/etc/issue`, (`/etc/issue.net`) and `/etc/motd` files to be updated with proprietary information and legal warning text

- Graphical GNOME Users:
  Set `/apps/gdm/simple-greeter/banner_message_enable 1` (true)
  `/apps/gdm/simple-greeter/banner_message_text` file to be updated with proprietary information and legal warning text

- Graphical (KDM) Users: `/usr/share/kde4/config/kdm/kdmrc` file to include `GreetString` parameter under the `[X-*-Greeter]` section. Parameter shall include proprietary information and legal warning text.

- VSFTPD: `/etc/vsftpd.conf` file should include
  `ftpd_banner=<insert_greeting_here>`

- SSH: `/etc/ssh/sshd_config` file should include
  `banner /etc/issue` or
  `banner /etc/issue.net`

References-

Reference Document	Chapter
CPI Library	
AIR Hardening Guideline, and Instruction, RHEL	4.1 System Access
SDP Hardening Guideline and Instruction, RHEL	4.1.1 System Access Messages

CCN Hardening Guidelines and Checklist	3.3.10 Banner Message Before Login
	3.3.11 Banner Message After Login
EMM7 F&E: System Administrator's Guide for Linux	7.6.2 Parameters Section
3PP Library	
CIS Red Hat Enterprise Linux 6 Benchmark v1.4.0	6 Set SSH Banner
	8 Warning Banners
Red Hat Enterprise Linux 6.8 Security Guide	2.2.6.1. FTP Greeting Banner
CIS SUSE Linux Enterprise Server 11 Benchmark v1.1.0	9.2.14 Set SSH Banner
	11 Warning Banners

3.3.18 IN_REQ045_v4: Configure Host Based Firewall

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MR-036-NW002

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level- Operating System

High Level Description- Activate and configure `iptables/firewalld`.

IP Filter provides state full packet filtering capabilities and can filter packets by IP address or network, port, protocol, network interface, and traffic direction. In addition, it also can perform network address translation (NAT) and port address translation (PAT).

IP Filter supports both IPv4 and IPv6 and is configured using a simple firewall rules policy language.

Solution Proposed- Host-based firewalls fill the gap in network security. Host-based firewalls allow us to tailor the types of connections we will accept from all hosts (regardless of their location). For host-based firewalls, we often have a simplified subset of requirements; traffic is allowed or denied based on its source host or network and destination port and protocol.

Operating System

a) RHEL

Host based firewall is taken care by `iptables` configuration in RHEL6 and by `firewalld` configuration in RHEL7.

b) SUSE

Host based firewall is taken care by `iptables` generated by `SuSEfirewall2` script in SUSE.

References-

Reference Document	Chapter
CPI Library – iptables (RHEL & SUSE)	
LE OS Hardening Guidelines and Instructions	8 Appendix: Sample Configuration File for EHardening
SDP Hardening Guideline and Instruction, RHEL	5 Appendix: Hardening Instructions
AIR Hardening Guideline and Instruction, RHEL	5 Appendix: Hardening Instructions
EMM: System Administrator's Guide	There is not a specific chapter, but iptables are supported
3PP Library – iptables (RHEL & SUSE)	
CIS Red Hat Enterprise Linux 6 Benchmark, v1.4.0	4.7 Enable IPtables
	4.8 Enable IP6tables
CIS Red Hat Enterprise Linux 7 Benchmark, v1.1.0	4.7 Enable firewalld
CIS SUSE Linux Enterprise Server 12 Benchmark, v.1.0.0	7.7 SuSEfirewall2 is active (Scored)
Opensuse.org	SuSEfirewall2

3.3.19 IN_REQ046_v4: Configure TCP Wrappers

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MR-036-NW002

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level- Operating System

High Level Description- TCP Wrappers should be configured to secure network services.

Solution Proposed- TCP Wrappers is a host-based access control system that allows administrators to control who has access to various network services based on the IP address of the remote end of the connection.

TCP Wrappers can limit from where requests are allowed. Its logs show attempted access to services from non-authorized systems, which can help identify unauthorized access attempts.

Operating System

RHEL/SUSE

To determine if a client machine can connect to a service, TCP wrappers reference the following two files, which are commonly referred to as hosts access files:

`/etc/hosts.allow`

`/etc/hosts.deny`

Create `/etc/hosts.allow`, and `/etc/hosts.deny` files and define permissions for the files.

The Syntax of the file is:

```
<services> : <clients> [: <option1> : <option2> : ...]
```

where,

- `services`, is a comma-separated list of services the current rule should be applied to.
- `clients` represent the list of comma-separated hostnames or IP addresses affected by the rule. The following wildcards are accepted:
  a) `ALL` matches everything. Applies both to clients and services.
  b) `LOCAL` matches hosts without a period in their FQDN, such as localhost.
  c) `KNOWN` indicate a situation where the hostname, host address, or user are known.
  d) `UNKNOWN` is the opposite of KNOWN.
  e) `PARANOID` causes a connection to be dropped if reverse DNS lookups (first on IP address to determine host name, then on host name to obtain the IP addresses) return a different address in each case.

Finally, an optional list of colon-separated actions indicates what should happen when a given rule is triggered.

When TCP wrapped service receives a client request, the follwing sequence will apply:

- The TCP wrapped service sequentially parses the `/etc/hosts.allow` file and applies the first rule specified for that service. If it finds a matching rule, it allows the connection. If not, it moves on to the next step.

- The TCP wrapped service sequentially parses the `/etc/hosts.deny` file. If it finds a matching rule, it denies the connection. If not, access to the service is granted.

NOTE: By default, `/etc/hosts.allow` and `/etc/hosts.deny` files are empty, all commented out, or do not exist. Thus, everything is allowed through the TCP wrappers layer and your system is left to rely on the firewall for full protection. Since this is not desired, make sure both files exist.

References-

Reference Document	Chapter
3PP Library	
CIS Red Hat Enterprise Linux 6 Benchmark v1.3.0-1	4.5 Install TCP Wrappers
CIS Red Hat Enterprise Linux 7 Benchmark v1.1.0	4.5 Install TCP Wrappers
CIS SUSE Linux Enterprise Server 12 Benchmark v1.0.0	7.4 Install TCP Wrappers

3.4 Hardening (HARD): OS Hardening

3.4.1 IN_REQ052_v4: Disable Unsecured Services

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_HARD_006, OS_HARD_003, APP_HARD_006

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level- Operating System

High Level Description- Services which are unsecured must be disabled.

Solution Proposed- Potentially, any network service is insecure. therefore, turning unused services off is so important. Exploits for services are revealed and patched routinely, making it very important to keep packages associated with any network service updated**.**

List of the existing services on the node which are unsecure, must be identified and disabled

Some network protocols are inherently more insecure than others. These include any services which do the following things:

- Pass Usernames and Passwords Over a Network Unencrypted — Many older protocols, such as `Telnet` and `FTP`, do not encrypt the authentication session and should be avoided whenever possible.
- Pass Sensitive Data Over a Network Unencrypted — Many protocols pass data over the network unencrypted. These protocols include `Telnet`, `FTP`, `HTTP`, and `SMTP`. Many network file systems, such as NFS and SMB, also pass information over the network unencrypted. It is the user's responsibility when using these protocols to limit what type of data is transmitted.

Operating System

a) RHEL/SUSE

Option 1: **Ehardening tool**

Unsecured Services can be disabled by running `ConfigEngine` with `EHardeningSetup` module

Option 2 CLI

Use `chkconfig` command to see a list of system services with their status (`on/off`) running on RHEL node.

In RHEL6

```
chkconfig --list <service_name>
```

In RHEL7

```
chkconfig --list <service_name>

systemctl list-units |grep -i <service_name>
```

Unsecure services should be disabled by executing the following command:

```
chkconfig <service_name> off --level <runlevels>
```

References-

Reference Document	Chapter
CPI Library	

LE OS Hardening Guidelines and Instructions Common Foundation 2	7 Operating System Hardening Checklist
3PP Library	
Red Hat Enterprise Linux 6.8: Deployment Guide	12.2.3.1. Listing the Services
	12.2.3.3. Disabling a Service
	12.3.3. Stopping a Service
SUSE Linux Enterprise Server Documentation	2.2 Disabling Unnecessary Services

3.4.2 IN_REQ053_v4: Disable Unused Services

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_HARD_002

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level- Operating System

High Level Description- Services which are unused must be disabled.

Solution Proposed- One of the easiest ways to start securing your server (and speeding it up) is to turn off unused services that are usually running by default.

Operating System

a) RHEL

List of the existing services on the node which are not in use must be identified and disabled using `EHardening` tool or `chkconfig` in RHEL.

b) SUSE

List of the existing services on the node which are not in use must be identified and disabled using `chkconfig` in SUSE.

NOTE

Disabling of unused services can be performed in a similar way for RHEL and SUSE; as in IN_REQ052_v4: Disable Unsecured Services

References-

Reference Document	Chapter
CPI Library	
LE OS Hardening Guidelines and Instructions Common Foundation 2	7 Operating System Hardening Checklist
3PP Library	
Red Hat Enterprise Linux 6.8: Deployment Guide	12.2.3.1. Listing the Services
	12.2.3.3. Disabling a Service
	12.3.3. Stopping a Service
SUSE Linux Enterprise Server Documentation	2.2 Disabling Unnecessary Services

3.4.3 IN_REQ054_v4: Secure RPC Portmapper

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_OS_HARD_001

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level- Operating System

High Level Description- The portmap service is a dynamic port assignment daemon for RPC services such as NIS and NFS.

When an RPC server is started, it will tell portmap what port number it is listening to, and what RPC program numbers it is prepared to serve. When a client wishes to make an RPC call to a given program number, it will first contact portmap on the server machine to determine the port number where RPC packets should be sent.

The figure below describes the mapping sequence steps between client and server to get appropriate port number via port mapper to start RPC services.

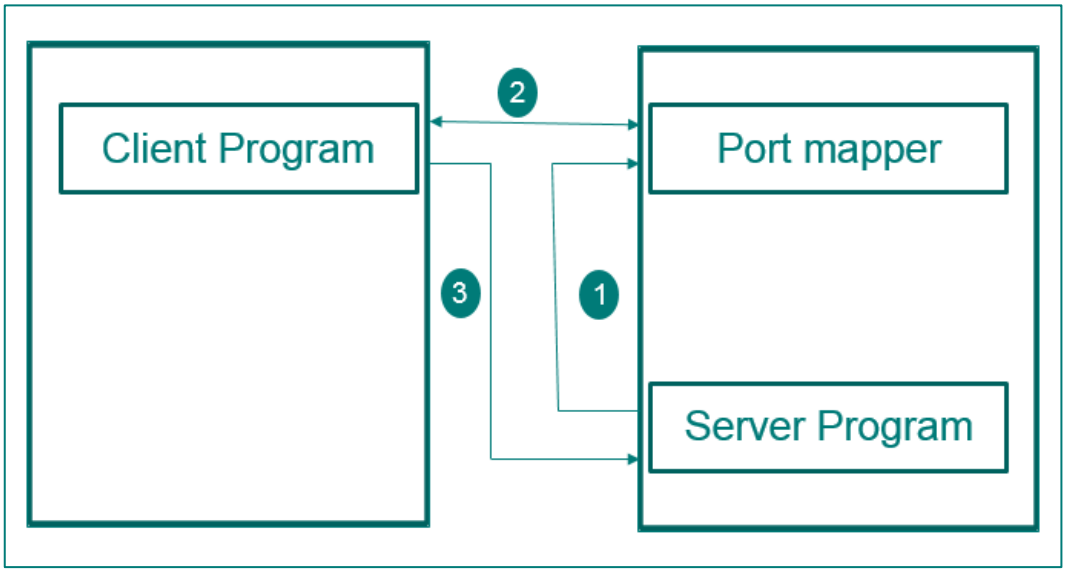

Figure 1 Typical Port Mapping Sequence

Step 1: Server registers port with the port mapper

Step 2: Client gets server's port from port mapper

Step 3: Client calls server's port directly

NOTE: Every port mapper on every host is associated with port number 111. The port mapper is the only RPC network service that must have such a well-known (dedicated) port. Other network services can be assigned port numbers statically or dynamically if they register their ports with the host port mapper.

Solution Proposed- The portmap service has weak authentication mechanisms and can assign a wide range of ports for the services it controls. For these reasons, it is difficult to secure

NOTE: Securing portmap only affects NFSv2 and NFSv3 implementations, since NFSv4 no longer requires it. If you plan to implement an NFSv2 or NFSv3 server, then portmap is required, and the following section applies

You can protect portmap with:

- TCP Wrappers
- Iptables

a) Protect portmap With TCP Wrappers

It is important to use TCP Wrappers to limit which networks or hosts have access to the portmap service since it has no built-in form of authentication.

Further, use only IP addresses when limiting access to the service. Avoid using hostnames, as they can be forged by DNS poisoning and other methods.

To protect the portmapper, use the name "`portmap`" for the daemon name. Only the use the keyword "ALL" and IP addresses (NOT host or domain names) are allowed for the portmapper, as well as for `rpc.mountd` (the NFS mount daemon).

Edit & Update `/etc/hosts.allow` file:

Sample entries for portmap server to allow access from `xxx.xxx.x.x/xx (IP/CIDR mask)` only.

```
sshd : ALL

portmap : xxx.xxx.x.x/xx (IP/CIDR mask)
```

Save and **close** the file

b) Protect the portmap with iptables

To further restrict access to the portmap service, it is a good idea to add iptables rules to the server and restrict access to specific networks. The second allows TCP connections to the same port from the localhost

Below is two example `iptables` commands. The first allow TCP connections to the port 111 (used by the portmap service) from the 193.167.1.0/23 network.

- Drop TCP port 111 packets if they are NOT from `xxx.xxx.x.x/xx (IP/CIDR mask`

```
~]# iptables -A INPUT -p tcp ! -s xxx.xxx.x.x/xx (IP/CIDR
mask --dport 111 -j DROP
```

- Drop TCP port 111 packets if they are NOT from `xxx.xxx.x.x/xx (IP/CIDR mask` and localhost (`xxx.x.x.x`)

```
~]# iptables -A INPUT -p tcp ! -s xxx.xxx.x.x/xx (IP/CIDR
mask --dport 111 -j DROP

~]# iptables -A INPUT -p tcp -s xxx.x.x.x --dport 111 -j
ACCEPT
```

References-

Reference Document	Chapter
3PP Library	

Redhat Product Documentation RHEL &: Security Guide	2.2.2.2. Protect portmap with iptables
nixCraft: Linux & Unix tutorial for new and seasoned sysadmin	How to Secure portmap service using iptables and TCP Wrappers under Linux

More details are described here:

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/sect-Security_Guide-Securing_Portmap-Protect_portmap_With_iptables.html
- https://www.cyberciti.biz/faq/linux-secure-portmap-with-iptables-tcp-wrappers/

3.4.4 IN_REQ055_v4: Enable ExecShield Buffer Overflows Protection in LINUX

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_HARD_009

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- Enable `ExecShield` protection against buffer overflow, marking the stack as non-executable.

Solution Proposed- Exec Shield patch attempts to flag data memory as non-executable and program memory as non-writeable. This suppresses many security exploits, such as those stemming from buffer overflows and other techniques relying on overwriting data and inserting code into those structures.

Operating System

a) *RHEL*:

`ExecShield` Kernel feature provides protection against stack, buffer, or function pointer overflows, and against other types of exploits that rely on overwriting data structures and/or putting code into those structures.

`ExecShield` can be enabled by editing the `/etc/sysctl.conf` and adding the following line:

```
kernel.exec-shield = 1
```

b) SUSE:

SUSE includes, by default, security-focused kernel tuning parameters, you will find the existing `/etc/sysctl.conf` file to be sparsely populated.

Step 1:

Check whether the `ExecShield` is enabled:
`# sysctl kernel.exec-shield`

Step 2:

In case `ExecShield` is supported by SUSE and not enabled, proceed as with SOLARIS/RHEL by setting the `kernel.exec-shield` parameter to `1`.

References-

Reference Document	Chapter
3PP Library	
CIS Red Hat Enterprise Linux 6 Benchmark v1.4.0	1.6.2 Configure ExecShield

3.4.5 IN_REQ056_v4: Disable CTRL-Alt -DEL Functionality

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag-MTNG_CSBL_NEW_OS_HARD_002

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- In Linux, it's a security concern for us to allow anyone to reboot the server using `Ctrl-Alt-Del` keys. It is always recommended in production boxes that one should disable reboot using `Ctrl-Alt-Del` keys.

Solution Proposed-

a) RHEL 6

On RHEL6, `/etc/inittab` file still exists, but disabling `Control-Alt-Delete` cannot be done in the file.

To disable this behavior, open `/etc/init/control-alt-delete.conf` and then find out following 2 lines and add a hash mark at its very beginning of the line.

```
# start on control-alt-delete

# exec /sbin/shutdown -r now Control-Alt-Delete pressed
```

The following link provides more information about the subject:

https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c02847279

b) RHEL 7.x

Link the system "`/dev/null`" to the system file so the system will not react to the key strokes

```
# ln -sf /dev/null /etc/systemd/system/ctrl-alt-del.target
```

If `<Ctrl>+<Alt>+Del>` keys stroke was pressed, syslog messages file will show:

```
Failed to enqueue ctrl-alt-del.target job: Unit ctrl-alt-
del.target is masked.
```

NOTE:

We do not need to restart the OS or any daemon, because the `init` daemon will automatically reload this change

References-

Reference Document	Chapter
3PP Library	
LINUX Tutorial & Guide	Disable reboot using Ctrl-Alt-Del Keys in RHEL / CentOS

3.4.6 IN_REQ057_v4: Prevent SMTP Information Disclosure

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_VUL&PAT_005

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- SMTP Information should be protected. It is possible to enumerate the name of valid users on the remote host. The remote SMTP server answers to the `EXPN` and `VRFY` commands. The `EXPN` command can be used to find the delivery address of mail aliases and the `VRFY` command may be used to check the validity of an account.

Solution Proposed-

Operating System

a) RHEL:

`VRFY` and `EXPN` commands can be disallowed in `/etc/mail/sendmail.cf` by configuring `PrivacyOptions` option. `noexpn` keyword disallows all SMTP EXPN commands and `novrfy` keyword disallows all SMTP VRFY commands.

b) SUSE:

Option 1:

In case `sendmail` is used, the same procedures as for RHEL will apply.

Option 2 (as per SUSE 11 recommendation):

`postfix` is a replacement for `sendmail` and has several security advantages over `sendmail`. `postfix` is the default mail system in SUSE Linux Enterprise Server. Postfix contains two configuration files `main.cf` and `master.cf`.

NOTE:

Further investigation required to check whether the `postfix` (in case installed and used) security includes the prevention of SMTP information disclosure.

References-

Reference Document	Chapter
3PP Library	
SUSE Linux Enterprise Server 11 SP4	Security and Hardening

More details are described here:

- SUSE Linux Enterprise Server 11 SP4, Security and Hardening https://www.suse.com/documentation/sles11/singlehtml/book_hardening/book_hardening.html

3.4.7 IN_REQ058_v4: SMTP Version shall not be disclosed

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_VUL&PAT_006

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- It has been identified that SMTP discloses the version information. This could be a potential attack vector which reveals the vulnerabilities associated with the platforms. The malicious attackers can exploit this loop hole and gain unauthorized access to the target information asset.

Solution Proposed-

Operating System

a) RHEL

Updating `SmtpGreetingMessage` parameter in `sendmail.cf` file will prevent the SMTP version disclosure

b) SUSE

Option 1:

In case `sendmail` is used, the same procedures as for RHEL.

Option 2 (as per SUSE 11 recommendation):
`postfix` is a replacement for `sendmail` and has several security advantages over `sendmail`. `postfix` is the default mail system in SUSE Linux Enterprise Server. `postfix` contains two configuration files `main.cf` and `master.cf`.

References-

Reference Document	Chapter
3PP Library	
SUSE Linux Enterprise Server 11 SP4	Security and Hardening

More details are described here:

- SUSE Linux Enterprise Server 11 SP4, Security and Hardening https://www.suse.com/documentation/sles11/singlehtml/book_hardening/book_hardening.html

3.4.8 IN_REQ059_v4: Restrict Concurrent Unauthenticated User Access from Different Terminals

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_026

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- User access from different terminals at the same time shall be restricted. It is possible to set a threshold for the number of concurrent users allowed.

Solution Proposed - The maximum number of concurrent unauthenticated connections via SSH can be configured in `sshd_config` file with following keyword-arguments.

Operating System

a) *RHEL/SUSE*

- `MaxAuthTries`: Specifies the maximum number of authentication attempts permitted per connection. Once the number of failures reaches half this value, additional failures are logged. The default is 6.
- `MaxSessions`[25]: Specifies the maximum number of open sessions permitted per network connection. The default is 10.
- `MaxStartups`: Specifies the maximum number of concurrent unauthenticated connections to the SSH daemon. Additional connections will be dropped until authentication succeeds or the `LoginGraceTime` expires for a connection. The default is 10.

References-

[25] *Specifies the maximum number of open shell, login, or subsystem (e.g. sftp) sessions permitted per network connection. Multiple sessions may be established by clients that support connection multiplexing. Setting `MaxSessions` to 1 will effectively disable session multiplexing, whereas setting it to 0 will prevent all shell, login and subsystem sessions while still permitting forwarding. The default is 10.*

Reference Document	Chapter
3PP Library	
CIS Red Hat Enterprise Linux 6 Benchmark V1.4.0	6.2.5 Set SSH MaxAuthTries to 4 or Less
CIS SUSE Linux Enterprise Server 12 Benchmark v1.0.0	9.2.5 Set SSH MaxAuthTries to 4 or Less (Scored)

3.5 Hardening (HARD): DB Hardening

3.5.1 IN_REQ067_v4: Resource Limits Initialization for DB

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- DB_ACC_021

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Database

High Level Description- Profile resource limits are enforced in database.

Solution Proposed – Use the `ulimit -a` command to view the current limits. Although limits can also be temporarily set.

Database

a) Oracle

Oracle database initialization parameter, `RESOURCE_LIMIT`, should be set `TRUE` to enable the enforcement of resource limits.

b) PostgreSQL

Configuration parameters affect categories of server behaviors, such as resource consumption, query tuning etc.

Parameter related to Memory, Kernel Resource Usage & Cost-Based Vacuum Delay should be analyzed.

Monitoring and observation should be done in coordination with the Managed Services Team regarding system resource utilization. After analyzing the results, the exact value of the parameters must be identified.

The following link provides more information about the subject:

https://www.postgresql.org/docs/9.2/static/runtime-config-resource.html

c) Cassandra

To achieve this, a file `/etc/security/limits.conf` must have the below entries

```
<cassandra_user> - memlock unlimited

<cassandra_user> - nofile <value>

<cassandra_user> - nproc <value>

<cassandra_user> - as unlimited
```

And the following line should be added to `/etc/sysctl.conf` file

```
vm.max_map_count = <value>
```

In RHEL based server, limit can also be set in `/etc/security/limits.d/90-nproc.conf` file with below entry:

```
<cassandra_user> - nproc <value>
```

The following link provides more information about the subject:

https://books.google.co.in/books?id=-WZCDwAAQBAJ&pg=PA74&lpg=PA74&dq=cassandra+limit+resource&source=bl&ots=_iZAiB5riQ&sig=c1-TZg5KdTmhMWHDKNegtC37J8E&hl=en&sa=X&ved=0ahUKEwjCl7TqwPXaAhVLPo8KHfTZClMQ6AEIaTAH#v=onepage&q=cassandra%20limit%20resource&f=false

References-

Reference Document	Chapter
3PP Library	
PostgreSQL 9.2.24 Documentation	18.4. Resource Consumption

3.6 Hardening (HARD): Web Server Hardening

3.6.1 IN_REQ073_v4: Web Server Version shall not be disclosed

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_001

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description-- Web services discloses the version information. This could be a potential attack vector which reveals the vulnerabilities associated with the platforms. The malicious attackers can exploit this loop hole and gain unauthorized access to the target information asset.

Solution Proposed-

Apache HTTP Server

The following parameters should be updated in `/etc/httpd/conf/httpd.conf` file

- `ServerSignature`

This will ensure that Apache does not display the server version in the footer of server generated pages.

- `ServerTokens`

This will configure Apache to not send any version numbers in the HTTP header, so that the server line will be: Server: Apache

Apache Tomcat 8.X:

The following attributes should be updated in in the `server.xml` file

- `Server`

It overrides the Server header for the http response. If set, the value for this attribute overrides the Tomcat default and any Server header set by a web application. If not set, any value specified by the application is used.

- `xpoweredBy`

Set this attribute to `true` to cause Tomcat to advertise support for the Servlet specification using the header recommended in the specification. The default value is `false`.

The `server` attribute of the HTTP connector to a nondescript value should be set to `oamServer`

If the `xpoweredBy` attribute is present, it should be set to `"false"`

The following link provides more information about the subject:

https://tomcat.apache.org/tomcat-8.0-doc/config/http.html

NOTE:

In CCN, `ServerSignature` and `ServerTokens` parameter should be updated in `global.conf` file.

References-

Reference Document	Chapter
3PP Library	
CIS Apache HTTP Server 2.2 Benchmark v1.2.0	1.8.1 Limit Information in the Server Token
	1.8.2 Limit Information in the Server Signature

3.6.2 IN_REQ074_v4: Disable Trace/Track in Web Server

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_HARD_012

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description - 'TRACE' is a HTTP request method used for debugging which echo's back input back to the user. The TRACE method is not needed and is easily subjected to threat.

Solution Proposed – TRACE requests can be disabled by making a change to the Apache server configuration.

Apache HTTP Server

The `TraceEnable` parameter should be set to `off` in `httpd.conf` file.

Apache Tomcat 8.X:

Tomcat 8.X does not allow the TRACE HTTP verb by default. Tomcat will only allow TRACE if the `allowTrace` attribute is present and set to `true` in the `server.xml` file.

`allowTrace` is a Boolean value which can be used to enable or disable the TRACE HTTP method. If not specified, this attribute is set to false.

The `allowTrace` attribute should be set to `false` in `server.xml` file.

NOTE:

In CCN, The `TraceEnable` parameter should be set to `off` in `default-server.conf` file.

References-

Reference Document	Chapter
3PP Library	
CIS Apache HTTP Server 2.2 Benchmark	1.5.8 Disable HTTP TRACE Method (Scored)
Apache Tomcat 8 Configuration Reference	The HTTP Connector

3.6.3 IN_REQ075_v4: Use WAF and DoS Protection for Web Server

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_APP_HARD_003

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- Mod_security and Mod_evasive are free Apache modules which protect web server from various brute force or (D)DoS attacks, including SQL injection, cross-site scripting, session hijacking, and many others. These modules can be deployed and integrated into your infrastructure without having to modify your internal network.

Solution Proposed – Mod_security and Mod_evasive configuration directives are added to configuration file (typically `httpd.conf`) directly. These directives can be enclosed in a container tag.

The mod_evasive Apache module, formerly known as mod_dosevasive, helps protect against DoS, DDoS (Distributed Denial of Service), and brute force attacks on the Apache web server. It can provide evasive action during attacks and report abuses via email and syslog facilities.

The mod_security is an open source web application firewall (WAF) and intrusion detection and prevention system for web applications. It operates embedded into the web server, acting as a powerful umbrella, shielding applications from attacks. It is used to protect and monitor real time HTTP traffic and web applications from brute force attacks

The modules mod_security and mod_evasive are not installed by default. If they are installed, implementation can be done.

a) *Configuring Mod_security*

The mod_security module should be loaded in httpd.conf file:

The following lines should be added at the httpd.conf file

```
LoadModule unique_id_module modules/mod_unique_id.so

LoadModule security2_module modules/mod_security2.so
```

The mod_unique_id module is pre-requisite for Mod Security. This module provides an environment variable with a unique identifier for each request, which is tracked and used by Mod Security.

Below lines of code should be updated at the end of the httpd.conf file:

```
<IfModule security2_module>

    Include conf/crs/modsecurity_crs_10_setup.conf

    Include conf/crs/base_rules/*.conf

</IfModule>
```

In above configuration, we are loading Mod Security main configuration file modsecurity_crs_10_setup.conf and base rules base_rules/*.conf provided by Mod Security Core Rules to protect web applications.

b) Configuring Mod_evasive

The mod_evasive module should be loaded in httpd.conf file:

The following lines should be added at the httpd.conf file

```
LoadModule evasive20_module
/usr/lib/httpd/modules/mod_evasive20.so
```

By default, installation adds the line above of `mod_evasive` configuration to Apache configuration file.

The `mod_evasive` configuration parameters mentioned below should be added at the end of the Apache configuration file

```
<IfModule mod_evasive20.c>
DOSHashTableSize    3097
DOSPageCount        2
DOSSiteCount        50
DOSPageInterval     1
DOSSiteInterval     1
DOSBlockingPeriod   60
DOSEmailNotify someone@somewhere.com
</IfModule>
```

References-

Reference Document	Chapter
3PP Library	
Mod_security Homepage	http://www.modsecurity.org/
Mod_evasive Homepage	https://www.linode.com/docs/web-servers/apache-tips-and-tricks/modevasive-on-apache

3.6.4 IN_REQ076_v4: Run Web Server as Separate User and Group

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_APP_HARD_004

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- The "`nobody`" `userid` & `group` that comes default on Unix variants should NOT be used to run the web server, since the account is commonly used for other separate daemon services. Instead, an account used only by the apache software so that it cannot give unnecessary access to other services.

Also, the `userid` used for the apache user should be a unique value between 1 and 499 as these lower values are reserved for the special system accounts not used by regular users, such as discussed in User Accounts section of the CIS Red Hat benchmark.

Solution Proposed –. One of the best ways to reduce your exposure to attack when running a web server is to create a unique, unprivileged `userid` and `group` for the server application.

A user account must be created which runs the web server software.

Apache HTTP Server:

Both `User` and `Group` parameter should be updated in the "`httpd.conf`" file.

- User

The option User specifies the UID that Apache server will run as. It's important to create a new user that has minimal access to the system, and functions just for the purpose of running the web server daemon.

- Group

The option Group specifies the GID the Apache server will run as. It's important to create a new group that has minimal access to the system and functions to run the web server daemon.

NOTE:

In SDP the user and group in `/etc/httpd/conf/httpd.conf` are set to `sdpuser` & `staff` respectively. DONOT change the login shell of these users to `/sbin/nologin.`

In AIR the user and group in `/etc/httpd/conf/httpd.conf` are set to `fdsuser` & `staff`.respectively. DONOT change the login shell of these users to `/sbin/nologin`.

IN CCN, user and group in `/etc/apache2/uid.conf` are set to `wwwrun` & `www` respectively. DONOT change the login shell of these users to `/sbin/nologin`.

Apache Tomcat 8.X:

It should be identified, which user is running Tomcat by following command:

```
# ps -ef | grep -i tomcat| awk '{print $1}'
```

If Tomcat process is running as `root` or other user than `system user`

`TOMCAT8_USER` and `TOMCAT8_GROUP` parameter should be updated in `/etc/default/tomcat8`

The following link provides more information about the subject:

https://code.stanford.edu/puppetpublic/shibb_idp3/blob/master/files/etc/default/tomcat8

NOTE:

In OCC**,** If the Tomcat process is running as `root` or another user than `ogw`, verify that the startup script (`startup.sh`) in `/opt/webstart/bin/tomcat` is configured to start as `ogw`.

```
# cat /opt/webstart/bin/tomcat | grep -i ogw
```

References-

Reference Document	Chapter
3PP Library	
CIS Apache HTTP Server 2.2 Benchmark v3.2.0: 1.3 Restricting OS Privileges	1.3.1 Run the Apache Web Server as a non-root user (Scored

3.6.5 IN_REQ077_v4: Restrict Access to root Directory in Web Server

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_APP_HARD_005

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- Access to root directory must be restricted.

Solution Proposed – Access to an Apache directory can be allowed or denied using `option` directive. `Option` directive is included in the Apache HTTP Server configuration file, `/etc/httpd/conf/httpd.conf` file.

The root directory access can be allowed or denied using an `option` directive It's also better to turn this option off.

The `option` directive should be set to none in the `httpd.conf` file (under the `DocumentRoot`).

```
<Directory "/usr/local/apache2/htdocs">
Options None
```

NOTE:

In SDP and AIR, this is not applicable as it will prevent the FDS application from opening.

In CCN, the `option` directive should be set to `none` in the `/etc/apache2/default-server.conf` file under the `DocumentRoot`.

References-

Reference Document	Chapter
3PP Library	
Apache Core Features: Version 2.2: Modules	Options Directive
How to secure Apache web server?	5. Deny directory access
CentOS Docs: Apache 2.2 (httpd.conf file)	21.5. Configuration Directives in httpd.conf: All Options (Apache 2.2)

More details are described here:

- http://httpd.apache.org/docs/2.2/mod/core.html#options

3.6.6 IN_REQ078_v4: Set Appropriate Permissions for Web Server Directories

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_APP_HARD_006

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- Setting the appropriate ownership and permissions of the web server directories (Apache configuration (conf) and binary (bin)) directories can help to prevent/mitigate exploitation severity.

Solution Proposed- The file system should be configured in such a way that the group and others do not have permission to edit or write the files which it then executes.

Apache HTTP Server

In the `Web_Server` directory, permission of `bin` and `conf` folder should be changed to 750. (`rwxr_x___`)

It can be done by executing the below command:

```
# chmod –R o-rwx <file_or_directory>
```

It can be verified by

```
# ls -ld <file_or_directory>
```

Apache Tomcat 8.X:

There are several directories and files where the default permission is world readable, executable, and/or writable by the group.

Read, Write, execute permissions should be removed for world as well as write permissions for group.

```
# chmod g-w,o-rwx <file_or_directory>
```

NOTE:

Any permission changes must be verified with PDU beforehand to ensure that no functionality is impacted.

Ideally, all sensitive files that should not be served, should be placed in the `WEB-INF` directory of the `Document Root`. The `WEB-INF` directory is not part of the public document tree of the application. No file contained in the `WEB-INF` directory can be served directly to a client by the container. The contents of the `WEB-INF` directory would still be visible to servlet code.

Any file not within the `WEB-INF` folder of the `Document Root` will be served unless a <`security-constraint`> has been configured in the applications corresponding `web.xml` file, to explicitly prevent the directories or files from being served.

References-

Reference Document	Chapter
3PP Library	

APACHE HTTP: Apache Web Server Hardening & Security Guide	3.2 Protect binary and configuration directory permission

3.6.7 IN_REQ079_v4: Disable Directory Listing in Web Server

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_APP_HARD_007

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- The Apache web server, lists all the files and folder of the root web document directory. Directory listings or Indexing of web server is enabled by default on Apache Configuration setting. If Directory Listing is enabled on server, it is very vulnerable to attacks as the directory listing gives out vital information about web server such as Server Name, Server Version, and the Listening Port

Solution Proposed- Directory Listing can be disabled by updating the server configuration file.

Apache HTTP Server

The `option` directive should be updated in the `httpd.conf` file under `DocumentRoot`.An `Index` parameter should be disabled by adding a "-" in front of the parameter.

```
<Directory /opt/apache/htdocs>
Options -Indexes
```

If the line `IndexOptions FancyIndexing` is present, comment it out.

CAUTION:

Setting `Options` to `-Indexes` can affect the launch of FDS GUI.

Apache Tomcat 8.X:

In Tomcat, directory listing is disabled by default. However, it is possible to disable directory listing if it was enabled because of a regression or configuration changes.

The `listings` parameter should be set to false in the `web.xml` file.

The `<init-param></init-param>` block with the `<param-name>listings</param-name>`. should be identified and `<param-value>` must be set to `false`:

References-

Reference Document	Chapter
3PP Library	
Configuration Directives in httpd.conf	
Httpd Wiki: DirectoryListings	Directory Listing Configuration: Directory Listings (Prevent Directory listing)
Apache hardening checklist: How to secure Apache web server?	3. Prevent Directory Listing
APACHE HTTP: Apache Web Server Hardening & Security Guide	2.2 Disable directory browser listing
Apache Tomcat 8	Security Considerations

More details are described here:

- https://www.netsparker.com/blog/web-security/disable-directory-listing-web-servers/
- https://tomcat.apache.org/tomcat-8.0-doc/security-howto.html

3.6.8 IN_REQ080_v4: Disable Directory Browsing in Web Server

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_APP_HARD_008

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description -Directory Browsing should be disabled to make the server secure. Usually apache comes with this feature enabled but it is always a good idea to get it disabled

Solution Proposed – Directory Browsing can be disabled by updating the server configuration file.

Apache HTTP Server

The `option` directive should be updated in the `httpd.conf` file under `DocumentRoot`.Word `Index` should be removed.

The line should look like this one:

```
Options Includes FollowSymLinks MultiViews
```

NOTE:

Disabling of Directory Browsing (same as Listing) in Apache is also achievable through procedure in 3.6.7

Apache Tomcat 8.X:

Disabling of Directory Browsing (same as Listing) in Apache is achievable through procedure in 3.6.7

References-

Reference Document	Chapter
3PP Library	
Configuration Directives in httpd.conf	
Httpd Wiki: DirectoryListings	Directory Listing Configuration: Directory Listings (Prevent Directory listing)
Apache hardening checklist: How to secure Apache web server?	3. Prevent Directory Listing
APACHE HTTP: Apache Web Server Hardening & Security Guide	2.2 Disable directory browser listing
Apache Tomcat 8	Security Considerations

3.6.9 IN_REQ081_v4: Disable Unnecessary Components of Web Server

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_APP_HARD_009

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- Apache typically comes with several modules installed. It's important to have a minimal and compact Apache installation based on documented business requirements

Solution Proposed- Modules should be reviewed and disabled if not required for business purposes. However, it's very important that the review and analysis of which modules are required for business purpose not be limited to the modules explicitly listed.

Apache HTTP Server

Modules are defined in `httpd.conf` file. Any unnecessary modules should be disabled by commenting them out in the `httpd.conf` file.

The Following are the default enabled modules:

```
fds_module
proxy_module
proxy_ajp_module
proxy_balancer_module
proxy_connect_module
proxy_ftp_module
proxy_http_module
log_config_module
autoindex_module
dir_module
authz_host_module
mime_module
ssl_module
rewrite_module
headers_module
```

If Directory Listings have been disabled in IN_REQ079_v4: Disable Directory Listing in Web Server then the autoindex_module can be disabled.

Apache Tomcat 8.X:

For Apache Tomcat, any unused applications e.g. test applications, manager applications (if not used) should be removed. Unused connectors should also be removed from the `server.xml` file.

NOTE:

Removal of any applications must be approved by Customer and cleared with PDU in advance.

CCN uses customized Linux (TSP). Apache modules which are required for the standard functionality of the Node are only Loaded.

References-

Reference Document	Chapter

3PP Library	
CIS Apache HTTP Server 2.2 Benchmark v3.2.0	1.2 Minimize Apache Modules
Apache Web Server Hardening & Security Guide	7.3 Disable Loading unwanted modules
Apache Tomcat 8	Security Considerations

3.6.10 IN_REQ082_v4: Cross Site Scripting (XSS) Protection in Web Server

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_APP_HARD_010

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- Cross site scripting (XSS) is a common security problem of web applications where an attacker gains access to the users' current web browser session.

Cross-site scripting (XSS) is one of the most common application-layer vulnerabilities in Apache server. XSS enables attackers to inject client-side script into web pages viewed by other users.

Solution Proposed- Cross Site Scripting (XSS) protection can be bypassed in many browsers. The "X-XSS-Protection" header forces the Cross-Site Scripting filter into Enable mode, even if disabled by the user.

Apache HTTP Server

In Web Server, XSS prevention is accomplished through the addition of Header directive.

The following block (if not present) should be updated in `httpd.conf` file:

```
<IfModule mod_headers>

    Header set X-XSS-Protection: "1; mode=block"

</IfModule>
```

Apache Tomcat 8.X:

`xssProtectionEnabled` HTTP headers can be added to the response to improve the security of the connection.

- `xssProtectionEnabled`

Should the header that enables the browser's cross-site scripting filter protection `(X-XSS-Protection: 1; mode=block)` be set on every response. If already present, the header will be replaced. If not specified, the default value of true will be used.

The `xssProtectionEnabled` parameter should be set to true in the `web.xml` file.

The block with the `<param-name> xssProtectionEnabled </param-name>`. should be identified and `<param-value>` must be set to `true:`

```
<param-name>xssProtectionEnabled</param-name>
<param-value>true</param-value>
```

The following link gives more information on it:

https://tomcat.apache.org/tomcat-8.0-doc/config/filter.html

NOTE:

In CCN, the Header directive should be updated in the `/etc/apache2/default-server.conf:`

```
<IfModule mod_headers>

    Header set X-XSS-Protection: "1; mode=block"

</IfModule>
```

References-

Reference Document	Chapter
3PP Library	
Apache HTTP: Apache Web Server Hardening & Security Guide	4.4 X-XSS Protection
How to secure Apache web server	13. Cross Site Scripting protection
How to Harden the Apache Web Server on CentOS 7	Secure Apache from XSS attacks
Apache Tomcat 8 Configuration Reference	HTTP Header Security Filter

3.6.11 IN_REQ083_v4: Disable/Remove CGI Test Script

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- APP_HARD_004

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- The CGI (Common Gateway Interface) defines a way for a web server to interact with external content-generating programs, which are often referred to as CGI programs or CGI scripts. It is a simple way to put dynamic content on your web site, using whatever programming language you're most familiar with.

Solution Proposed – Certain conditions in the `test-cgi` file, shipped with older NCSA and Apache HTTP server packages, could allow a remote attacker to submit a query to view the contents of the `cgi-bin` directory or other directories on the Web server. This information could be useful to an attacker in performing future attacks on the system.

This vulnerability can be used to change the contents of a Web page. Exploit information for this vulnerability has been widely distributed.

Apache HTTP Server

`test-cgi` and `printenv` file from the `cgi-bin` directory should be removed (if present).

NOTE:

Configuration will be done from OS layer however the BL tag is referring to Application layer as modification must be done in Apache HTTP server package

References-

Reference Document	Chapter
3PP Library	
CIS Apache HTTP Server 2.2 Benchmark	1.5.5 Remove Default CGI Content `printenv`
	1.5.6 Remove Default DGI Content `test-cgi`

3.6.12 IN_REQ084_v4: Disallow .htaccess in Apache HTTP Server

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_APP_HARD_011

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- `.htaccess` files (or "distributed configuration files") provide a way to make configuration changes on a per-directory basis. A file, containing one or more configuration directives, is placed in a document directory, and the directives apply to that directory, and all subdirectories thereof.

Solution Proposed – When `AllowOverride` is set to allow the use of `.htaccess` files, httpd will look in every directory for `.htaccess` files. Thus, permitting `.htaccess` files causes a performance hit, Also, the `.htaccess` file is loaded every time a document is requested.

Apache HTTP Server

The `AllowOverride` parameter should be set to `None` in the `httpd.conf` file for each `<Directory></Directory>` block.

```
<Directory /opt/apache/htdocs>
AllowOverride None
```

NOTE:

In CCN, the `AllowOverride` parameter should be set to `none` in the `/etc/apache2/default-server.conf` for each `<Directory></Directory>` block.

References-

Reference Document	Chapter
3PP Library	
Apache HTTP Server Tutorial	.htaccess files
Apache .htaccess Guide & Tutorial	What is .htaccess?

More details are described here:

- https://httpd.apache.org/docs/2.2/howto/htaccess.html

- http://www.htaccess-guide.com/

3.6.13 IN_REQ085_v4: Protect the Shutdown Port in Apache Tomcat

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_APP_HARD_012

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- Tomcat is configured to be shut down on 8005 port by default. This default configuration leads to high-security risk.

Solution Proposed- Tomcat's shutdown procedure should be put on lockdown. Setting the port attribute to (-1) disables the shutdown port. This prevents malicious actors from shutting down Tomcat's web services.

Either disable the shutdown port by setting the port attribute in the `server.xml` file to (-1). If the port must be kept open, be sure to configure a strong password for shutdown.

The following parameter must be updated in `server.xml` file

- `port`

The TCP/IP port number on which this server waits for a shutdown command. This connection must be initiated from the same server computer that is running this instance of Tomcat. Set to -1 to disable the shutdown port.

- `Shutdown`

The command string that must be received via a TCP/IP connection to the specified port number, to shut down Tomcat.

References-

Reference Document	Chapter
3PP Library	
Apache Tomcat 8	Security Considerations

More details are described here:

- https://tomcat.apache.org/tomcat-8.0-doc/security-howto.html

3.6.14 IN_REQ086_v4: Prevent ETag Information Leakage

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_APP_HARD_013

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description – Entity tags (ETags) are a mechanism that web servers and browsers used to determine whether the component in the browser's cache matches the one on the origin server. `ETag` is a validator which can be used instead of, or in addition to, the Last-Modified header. By sending a `ETag`, the server promises that the content is not changed until the `ETag` changes for a resource.

The problem with the ETags is that they are generated with attributes that make them unique to a server. By default, Apache will generate an Etag based on the file's inode number, last-modified date, and size. So, if you have one file on multiple servers with same file size, permissions, timestamp, etc., even after that their `ETag` won't be same as they can't have the same inode number.

This creates the problem in the scenarios where you are having a cluster of web servers to serve the same content. When a file is served from one server and later validated from another server then the ETags for that file won't match and hence complete file will be fetched again. That means if you are having a cluster serving as a web server, then you shouldn't use ETags.

Solution Proposed – A weakness has been discovered in Apache web servers that are configured to use the FileETag directive. The way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number. So `ETag` information leakage must be prevented by updating the `httpd.conf` file

Apache HTTP Server

The following line should be added to the `httpd.conf` file

```
FileETag None
```

Run the following command and ensure that `ETag` is not present:

```
# curl -I -L http://<node_IP_address>:<port>
```

References-

Reference Document	Chapter
3PP Library	
Apache HTTP Server Version 2.0	FileETag Directive

More details are described here:

- http://httpd.apache.org/docs/2.0/mod/core.html#fileetag

3.7 Logging(LOG): Audit Log

3.7.1 IN_REQ090_v4: Enable Audit Logging

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_LOG_001, OS_LOG_002, DB_LOG_001, DB_LOG_002, DB_LOG_004, APP_LOG_001

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System, Database, Application

High Level Description- Auditing should be enabled on Operating System, Database, and Application levels to track user activities, and to monitor logins and logouts to identify unauthorized access. Enabling audit logging implies that periodic cleanup of log information, either manual or automatic, is performed.

Audit rules shall define:

- What to log
- When to log
- Where to log

Solution Proposed- The Audit system provides a way to track security-relevant information on your system. Based on pre-configured rules, Audit generates log entries to record as much information about the events that are happening on your system as possible. This information is crucial for mission-critical environments to determine the violator of the security policy and the actions they performed.

Operating System

Auditing should be enabled for RHEL and SUSE wherever applicable.

The following list summarizes some of the information that Audit is capable of recording in its log files:

- Date and time, type, and outcome of an event.
- Sensitivity labels of subjects and objects.
- Association of an event with the identity of the user who triggered the event.
- All modifications to Audit configuration and attempts to access Audit log files.
- All uses of authentication mechanisms, such as SSH, Kerberos, and others.
- Changes to any trusted database, such as `/etc/passwd`.
- Attempts to import or export information into or from the system.
- Include or exclude events based on user identity, subject and object labels, and other attributes.

The `/etc/audit/audit.rules` file should be updated with the recommended audit rules from `stig.rules` file

Status of System Auditing can be checked by `auditctl -s` command.

Database

Audit Logging should be enabled on Database (PostgreSQL, TimesTen, Cassandra) wherever applicable.

a) Oracle

b) TimesTen

Audit logging for SDP TimesTen database is **enabled by default**, audit logfile stored under the path `/var/log/ttlog`.

c) PostgreSQL

PostgreSQL supports several methods for logging server messages.

The following parameters should be set in `postgresql.conf` file

- `log_destination`
- `syslog_facility`
- `syslog_ident`
- `client_min_messages`
- `log_min_messages`
- `log_error_verbosity`
- `log_min_error_statement`
- `log_connections`
- `log_disconnections`
- `log_line_prefix`
- `log_statement`
- `log_statement_stats`

On most Unix systems, you will need to alter the configuration of your system's syslog daemon to make use of the syslog option for `log_destination`.

PostgreSQL can log to syslog facilities LOCAL0 through LOCAL7 but the default syslog configuration on most platforms will discard all such messages. You will need to update `/etc/rsyslog.conf` file with below entry:

```
local0.*    /var/log/postgresql
```

The following link provides more information about the subject:

https://www.postgresql.org/docs/9.4/static/runtime-config-logging.html

d) Cassandra

Audit Logging is not supported in Cassandra 2.x. This feature is being enabled in the Enterprise version of DataStax Cassandra.

For information on Audit Logging in DataStax Enterprise (DSE) Cassandra refer: https://docs.datastax.com/en/datastax_enterprise/4.8/datastax_enterprise/sec/secAudit.html#secAudit

Application

Audit Logging at application level is performed per node type and depending on type of Java GUI applications used and administration tools.

References-

Reference Document	Chapter

CPI Library	
SDP Hardening Guideline and Instruction, RHEL	4.5 Audit and Logging for Application
	4.6 Audit and Logging for OS
SDP User Guide System Administration Tool	4.4 General Setting
	4.5 Audit Schema
AIR Hardening Guideline and Instruction, RHEL	4.5 Audit and Logging
AIR: User Guide System Administration Tool	4.6 Authority Window – General
	4.7 Authority Window - Audit Schema
CCN: TSP Node Hardening Guideline and Instruction	3.3.21.1 Auditing
LE OS Hardening Guidelines and Instructions	5 System Auditing
EMM: Interface Description	5.4 Event Log

3.7.2 IN_REQ093_v4: Logging of User Activities on OS Level

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_LOG_003

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- User Activities should be logged.

Solution Proposed–Logging of user activity will identify suspicious behavior and risks will be mitigated before it result in data breaches.

User Activity can be logged by updating the `audit.rules` file and `/etc/login.defs` file.

The `audit.rules` file should have following entries:

```
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
-w /var/run/faillock -p wa -k logins
```

The `/etc/login.defs` file should have below entry:

```
FAILLOG_ENAB yes
```

References-

Reference Document	Chapter
CPI Library	
CCN Hardening Guidelines, and Checklist	3.3.8 Log user events
3PP Library	
CIS Red Hat Enterprise Linux 6 Benchmark, v1.4.0,	5.2 Configure System Accounting (auditd) 5.2.8 Collect Login and Logout Events
CIS SUSE Linux Enterprise Server 12 Benchmark v1.0.0	8.1 Configure System Accounting (auditd) 8.1.8 Collect Login and Logout Events

3.7.3 IN_REQ094_v4: Restrict Access of Audit Logs

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_LOG_005, DB_LOG_007, APP_LOG_004

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System, Database, Application

High Level Description- Restriction must be enabled on audit logs. Log files are supposed to be stored in secured way with limited read and write privileges.

Solution Proposed- All audit log files at Operating system, Application and Database layer should have read and write privileges only for the super user.

The file permission for all audit log files (OS, DB, APP) for all node types in scope, shall be checked and set to the appropriate permission level.

For `PostgreSQL` database, the archive logs will have read and write privileges only for the super user.

References-

Reference Document	Chapter
CPI Library	
SDP System Administrator's Guide	3.5 Log Files
SDP System Administrator's Guide, RHEL	3.5 Log Files
Security Management User Guide	3 Logging
Overall Guide Security Recommendations and Policies	4.4 Audit Logs

LE OS Hardening Guidelines and Instructions	7 Operating System Hardening Checklist

3.7.4 IN_REQ095_v4: Configuring Remote Syslog from UNIX/LINUX Server

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_LOG_004, DB_LOG_006, APP_LOG_002, APP_LOG_003

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System, Database, Application

High Level Description- It is recommended that one or more centralized logging servers are deployed, and logging devices are configured to send duplicates of their log entries to the centralized logging servers. The centralized log management solution should compromise the following tiers:

- Log generation (IN nodes will generate the logs at APP, DB, and OS layers)
- Log analysis and storage, and
- Log monitoring

Solution Proposed- Log file integrity can be achieved by enabling remote logging. Logs and audit files can be transferred to a remote server using protected protocols. In case of security incidence, for example tampered log files, the remote files can be used for verification of the local log files.

The remote logging function `rsyslog` is installed for using syslog at OS, DB, and APP levels.

To achieve this, below parameter should be updated in `/etc/audisp/plugins.d/syslog.conf` file:

- `active`
- `direction`
- `path`
- `type`

- `args`
- `format`

And, the `/etc/rsyslog.conf` file should have following entry:

```
*.* @@remote-host:514
```

NOTE:

SDP, AIR and ngCRS applications do not support `syslog`. Storage of audit logs occurs locally.

ngCRS has an external storage, Network Access Storage (NAS), which can be configured for this purpose

Ericsson Centralized Audit Logging (ECAL) can be used for remote logging.

In CCN, it is possible to redirect all log records to an external server through File Transfer Utility of CCN

References-

Reference Document	Chapter
CPI Library	
Charging Compound Overall Guide Security Recommendations and Policies	4.4 Audit Logs
	5.5 Audit Logs
	6.3 Audit Log Administration and Performance
SDP Hardening Guideline and Instruction, RHEL	4.5 Audit and Logging for Application
	4.6 Audit and Logging for OS
SDP System Administrator's Guide, RHEL	4.2.2.2 Check TimesTen Log
	4.2.2.3 Check syslog Configuration
LE OS Hardening Guidelines and Instructions	4.2.2 Logging
	5.6 Configure Remote Logging
AIR Hardening Guideline and Instruction, RHEL	4.5 Audit and Logging
CCN: Logging User Guide	3.4 Central Syslog Service Configuration
CCN: File Transfer Utility User Guide	1.1 Outgoing File Transfer
EMM: System Administrator's Guide	8.4.1 log_destination (string)
3PP Library	
TimesTen In-Memory Database Operations Guide	3 Working with the TimesTen Data Manager Daemon
CIS Red Hat Enterprise Linux 6 Benchmark v1.4.0	5.1 Configure rsyslog

CIS SUSE Linux Enterprise Server 12 Benchmark v.1.0.0	8.2 Configure rsyslog

3.8 Logging(LOG): Archive Log

3.8.1 IN_REQ091_v4: Enable Archive Logging

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- DB_LOG_003

Internal/External Audit Finding Reference-

Nodes –ngCRS, ngVS, ECMS, EDA, EMM

Level – Database

High Level Description-Archive Logs should be enabled.

Solution Proposed- Most of the High Availability features require you to enable `ARCHIVELOG` mode for your database. When the database is running in `ARCHIVELOG` mode, the log writer process cannot reuse and hence overwrite a redo log group until it has been archived.

Database

a) *Oracle*

The archive logging function is supported in Oracle 11g database.

b) *TimesTen*

TimesTen does not support archive logging.

c) *PostgreSQL*

Archive logging is enabled by configuring the WAL Archiving feature. `wal_level` parameter should be updated in `postgresql.conf` file.

The following link provides more information about the subject:

https://www.postgresql.org/docs/9.3/static/continuous-archiving.html

d) Cassandra

Cassandra provides commit log archiving and point-in-time recovery.

The following parameters are related to `commitlog` in the `/etc/cassandra/default.conf/cassandra.yaml` file

`commit_failure_policy`: Policy for commit disk failures. Values:

- `die`: Shut down gossip[26] and kill the JVM, so the node can be replaced.
- `stop`: Shut down gossip, leaving the node effectively dead, but can be inspected using JMX. This is the default value
- `stop_commit`: Shut down the commit log, letting writes collect but continuing to service reads (as in pre-2.0.5 Cassandra).
- `ignore`: Ignore fatal errors and let the batches fail

`commitlog_directory:` The directory where the commit log is stored.

`commitlog_segment_size_in_mb:` The size of an individual commitlog file segment. The default value is 32MB

`commitlog_sync:` The method that Cassandra uses to acknowledge writes in milliseconds. Values:

- `periodic`: With `commitlog_sync_period_in_ms`, controls how often commit log is synchronized to disk. Periodic syncs are acknowledged immediately
- `batch`: Used with `commitlog_sync_batch_window_in_ms` (Default: 2 ms), which is the maximum length of time that queries may be batched together.

The above-mentioned parameter should be updated.in `cassandra.yaml` file

IMPORTANT NOTE:

Implementing this Work Package would generate huge amount of Archive log files. Hence there should be enough space available and frequent monitoring and cleanup done.

References-

Reference Document	Chapter
CPI Library	

[26] *`Gossip` is a peer-to-peer communication protocol in which nodes periodically exchange state information about themselves and about other nodes they know about. The `gossip` process runs every second and exchanges state messages with up to three other nodes in the cluster.*

LE OS Hardening Guidelines, and Instructions Common Foundation 2	5.3.3 Configure Audit Rules for Customized Auditing

3.8.2 IN_REQ092_v4: Separate Disk Drives for Archive Logs Storage

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- DB_LOG_003

Internal/External Audit Finding Reference-

Nodes – ngCRS, ngVS, ECMS, EDA, EMM

Level – Database

High Level Description- Redo archive logs will be mirrored on a separate disk.

Solution Proposed-. When archive mode is enabled, redo logs will be archived instead of overwritten. The `archivelogs` are stored in a separate place usually in a separate disk or it can be backed up regularly by your standard filesystem backup system.

Database

a) *Oracle*

For Oracle database, each archived redo log file can possibly be mirrored. The parameter `LOG_ARCHIVE_DUPLEX_DEST, LOG_ARCHIVE_DUPLEX_DEST` must be set in the `init.ora` file accordingly.

b) *TimesTen*

TimesTen does not support archive logging.

c) *PostgreSQL*

The `archive_command` parameter should be updated in `postgresql.conf` file in the below mentioned way:

```
archive_command = 'test ! -f <directory path of the
additional storage>/%f && cp %p <directory path of the
additional storage> /%f'
```

NOTE:

In `archive_command` parameter, "`%p`" represents the path name of the file to archive, while "`%f`" represents the archive log file name.

If `Selinux` is in Enabled or Enforcing state, the mount point or the directory which would host this backup of Archive logs should have the same `type/tag` as that of `pg_xlog`. File

d) Cassandra

Cassandra provides commit log archiving and point-in-time recovery. The commit log is archived at node startup and when a commit log is written to disk, or at a specified point-in-time.

The `archive_command` parameter should be updated in `commitlog_archiving.properties` file in the below mentioned way:

```
archive_command=/bin/cp -f %path <directory path of the additional storage>/%name
```

NOTE:

In `archive_command` parameter, "`%path`" represents fully qualified path of the segment to archive, while "`%name`" represents name of the commit log.

If `Selinux` is in Enabled or Enforcing state, the mount point or the directory which would host this backup of Commit logs should have the same `type/tag` as that of `commitlog` file

IMPORTANT NOTE:

MTN IRANCELL needs to provide the additional filesystem with required space along with the mount point and directory details where backup of DB Archive logs will be stored.

References-

Reference Document	Chapter
3PP Library	
PostgreSQL 9.6.8 Documentation	25.3. Continuous Archiving and Point-in-Time Recovery

3.9 Encryption (ENCRYPT): Secure Protocols (TLS)

3.9.1 IN_REQ102_v4: Disable SSLv3 and TLSv1 Protocol Weak CBC Mode

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_HARD_014

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- SSL, and its successor TLS, are cryptographic protocols designed to provide communication security. In the web realm, they are providing HTTPS, but they are also used for other application protocols. SSLv1 was never publicly released, and SSLv2 was quickly found to be insecure. SSLv3 was created, and, together with the newer TLSv1/1.1/1.2, it is being used to secure the transport layer. But old protocol versions, including SSL version 3 (“SSLv3”) and TLS version 1.0, are no longer considered secure.

Solution Proposed- The Apache `SSLProtocol` directive specifies the SSL and TLS protocols allowed. Both the SSLv3 & TLSv1.0 protocols should be disabled

SSLv3:- The SSLv3 (and SSLv2) protocol is vulnerable to the POODLE attack which allows decryption and extraction of information from the server's memory. Due to this vulnerability disabling the SSLv3 protocol is highly recommended.

TLSv1:- The TLSv1.0 protocol is vulnerable to the BEAST attack when used in CBC mode. TLSv1.0 uses CBC modes for all the block mode ciphers, which only leaves the RC4 streaming cipher.

The RC4 cipher is not vulnerable to the BEAST attack; however, it is weak and not recommended. Therefore, it is recommended to upgrade the SSL version to support TLSv1.1 or higher and TLSv1.0 protocol to be disabled. Where the situation does not allows upgrading the system to TLSv1.1 or above, use strong algorithm in `SSLCipherSuite`.

The Table 10 below lists the available SSL protocols in Apache web server.

Table 10: Available SSLProtocol in Apache

Available Protocols	Description
`SSLv2`	This is the Secure Sockets Layer (SSL) protocol, version 2.0. It is the original SSL protocol as designed by Netscape Corporation.
`SSLv3`	This is the Secure Sockets Layer (SSL) protocol, version 3.0. It is the successor to SSLv2 and the currently (as of February 1999) de-facto standardized SSL protocol from Netscape Corporation. It's supported by almost all popular browsers.

`TLSv1`	This is the Transport Layer Security (TLS) protocol, version 1.0. It is the successor to SSLv3 and currently (as of February 1999) still under construction by the Internet Engineering Task Force (IETF). It's still not supported by any popular browsers.
`All`	This is a shortcut for ``+SSLv2 +SSLv3 +TLSv1'' and a convenient way for enabling all protocols except one when used in combination with the minus sign on a protocol as the example above shows.

Below is an example on how to enable/disable SSL protocols:

```
# enable SSLv3 and TLSv1, but not SSLv2
SSLProtocol all -SSLv2
```

NOTE:

RC4 recommendation is only in situations where upgrade to TLSv1.2 is not possible. RC4 in TLS v1.0 has output bias problem. Therefore, it is recommended to upgrade to TLS v1.2 or later.

For CCN, the POODLE (Padding Oracle on Downgraded Legacy Encryption) vulnerability is applicable for the customers who use SSL v2 and v3 protocol.CCN uses this protocol on two interfaces, HTTPS and LDAPS.

Patch for POODLE Vulnerability (CVE-2014-3566) was released to mitigate Charging System 5 CCN Customers. However, a check shall be performed also for CCN running charging system 6 or higher.

For OCC RHEL node, SSLv3 protocol can be disabled by setting `dtls.protocol.sslv3.disable=true` in `online.property` file

References-

Reference Document	Chapter
3PP Library	
CIS Apache HTTP Server 2.2 Benchmark	1.7.4 Restrict Weak SSL Protocols and Ciphers (Scored)
Red Hat JBoss Fuse 6.1 Security Guide	3. Securing the Jetty HTTP Server
Red Hat Customer Portal	Disabling SSLv3 in JBoss Fuse 6.x and JBoss A-MQ 6.x

More details are described here:

- Red Hat JBoss Fuse 6.1 Security Guide
  https://access.redhat.com/documentation/en-US/Red_Hat_JBoss_Fuse/6.1/html/Security_Guide/WebConsole.html

- Red Hat Customer Portal
  Disabling SSLv3 in JBoss Fuse 6.x and JBoss A-MQ 6.x
  https://access.redhat.com/solutions/1237613

- Stackoverflow: How to disable the SSLv3 protocol in Jetty to prevent Poodle Attack
  https://stackoverflow.com/questions/26382540/how-to-disable-the-sslv3-protocol-in-jetty-to-prevent-poodle-attack

3.9.2 IN_REQ104_v4: Setting X11 Protocol Forwarding

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_028

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, EDA, EMM, ECMS, CS-NMT

Level – Operating System

High Level Description- X11 forwarding is a mechanism that allows graphical interfaces of X11 programs running on a remote Linux/Unix server to be displayed on a local client machine.

Behind the scene, the X11 output of a remotely running program is authorized to be sent to localhost via an X11 connection between client and a remote server.

Hence the X11 forwarding sessions should be encrypted and encapsulated.

Solution Proposed- SSH has an option to securely tunnel such X11 connections, so that X11 forwarding sessions are encrypted and encapsulated.

Operating System

a) *RHEL/SUSE*

To set up X11 forwarding over SSH, update the `/etc/ssh/sshd_config` file with the following entry:

```
X11Forwarding yes
```

References-

Reference Document	Chapter
CPI Library	
TSP Node Hardening Guideline and Instruction	3.3.23 Setting X11 Protocol Forwarding
3PP Library	
CIS Red Hat Enterprise Linux 6 Benchmark v2.4.0	6.2 Configure SSH
CIS SUSE Linux Enterprise Server 12 Benchmark v1.0.0	9.2 Configure SSH

3.10 Encryption (ENCRYPT): SSL/TLS Cipher

3.10.1 IN_REQ101_v4: Disable SSL Weak Ciphers in Web Server

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_HARD_013

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level – Operating System

High Level Description- `SSLCipherSuite` is a complex directive uses a colon-separated cipher-spec string consisting of OpenSSL cipher specifications to configure the Cipher Suite the client is permitted to negotiate in the SSL handshake phase.

The SSL/TLS protocols support many encryption ciphers including many weak ciphers that are subject to man-in-the-middle attacks and information disclosure. Therefore, it is critical to ensure the configuration only allows strong ciphers greater than or equal to 128bit to be negotiated with the client, also enabling the `SSLHonorCipherOrder` further protects the client from the man-in-the-middle downgrade attacks by ensuring the servers preferred ciphers will be used rather than the client preferences.

In addition, the RC4 ciphers are stream ciphers that are widely used. However, the RC4 ciphers also have known cryptographic weaknesses and are no longer recommended and should be disabled.

Solution Proposed-

Operating System

a) Apache 2.x

Most versions of Apache have SSL 2.0 enabled by default. In an Apache server, SSL and weak ciphers can be disabled First, verify that weak ciphers or SSL enabled by local `OpenSSL` command.

```
# openssl s_client -connect <ip_address>:<port> -ssl2
```

`ssl2` can be replaced with `-ssl3, -tls1, -tls1_1,tls1_2`

Disable weak SSL ciphers using the `SSLCipherSuite`, and `SSLHonorCipherOrder` directives. The `SSLCipherSuite` directive specifies which ciphers are allowed in the negotiation with the client. While the `SSLHonorCipherOrder` causes the servers preferred ciphers to be used instead of the clients specified preferences.

If the `ssl.conf` is being called by the `httpd.conf` file, `SSLCipherSuite` parameter should be updated in `/etc/httpd/conf.d/ssl.conf` file and `SSLHonorCipherOrder`(if present) parameter should be set to `on`.

If the `ssl.conf` is not being called by the `httpd.conf` file, the same parameter should be updated in `/etc/httpd/conf/httpd.conf` file.

The following link provides more information about the subject:

https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslciphersuite

b) Apache Tomcat 8.x

The `ciphers` are specified using the JSSE cipher naming convention. The special value of `ALL` will enable all supported ciphers. This will include many that are not secure. `ALL` is intended for testing purposes only. If not specified, a default (using the OpenSSL notation) of `HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!kRSA` will be used

The `ciphers` attribute of the HTTP connector should be updated in `server.xml` file

```
ciphers =" HIGH:!MEDIUM:!NULL:!MD5"
```

The following link provides more information about the subject:

https://tomcat.apache.org/tomcat-8.0-doc/config/http.html

NOTE:

In CCN, it should be identified that whether `nss-global.conf` or `ssl-global.conf` file is present

If `ssl-global.conf` file is present, `SSLCipherSuite` parameter should be updated in `ssl-global.conf` file.

And if `nss-global.conf` file is present `NSSCipherSuite` parameter should be updated in `nss-global.conf` file

References-

Reference Document	Chapter
3PP Library	
CIS Apache HTTP Server 2.2 Benchmark	1.7.4 Restrict Weak SSL Protocols and Ciphers (Scored)

3.11 Encryption (ENCRYPT): SSH Cipher

3.11.1 IN_REQ103_v4: Disable SSH Weak CBC Mode Ciphers

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_HARD_016

Internal/External Audit Finding Reference-

Nodes – SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

High Level Description- The symmetric portion of the SSH Transport Protocol has security weaknesses that allows recovery of up to 32 bits of plaintext from a block of cipher text that is encrypted with the Cipher Block Chaining (CBC) method. New Counter mode algorithms are designed that are not vulnerable to these types of attacks and these algorithms are now recommended for standard use.

Solution Proposed- The SSH connection is implemented using a client-server model. This means that for an SSH connection to be established, the remote machine must be running a piece of software called an SSH daemon. This software listens for connections on a network port, authenticates connection requests, and spawns the appropriate environment if the user provides the correct credentials.

When SSH client attempts to open a SSH connection, the server and client change the list of ciphers that they support for encrypting the SSH sessions. The first cipher that the client and the server have common is used for encrypting the connection. If there are no ciphers in common between the client and the server, the system will prompt "*no matching cipher found*" error message.

The directive SSH `Ciphers` and `MACs` are used to limit the types of ciphers that SSH uses during communication.

Operating System

a) RHEL/SUSE

To determine the ciphers that an SSH server is configured to use, search for the '`Ciphers`' setting in the `sshd_config` file, as in the following example:

```
$ grep Ciphers /etc/ssh/sshd_config

Ciphers arcfour,3des-cbc
```

Edit the `/etc/ssh/sshd_config` file to set the parameter as follow:

```
Ciphers aes128-ctr,aes192-ctr,aes256-
ctr,arcfour256,arcfour128
```

If the below entry is in the `/etc/ssh/sshd_config` file, comment out the same and replace with the following secure MAC settings:

```
# MACs hmac-sha1,umac-64@openssh.com,hmac-ripemd160
```

In RHEL6, it should be

```
MACs hmac-sha2-512,hmac-sha2-256
```

In RHEL7

```
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-
sha2-256,umac-128@openssh.com
```

References-

Reference Document	Chapter
3PP Library	
CIS Red Hat Enterprise Linux 6 Benchmark v1.4.0	6.2.11 Use Only Approved Cipher in Counter Mode
CIS SUSE Linux Enterprise Server 12 Benchmark v1.0.0	9.2.11 Use Only Approved Cipher in Counter Mode (Scored)

4 Non-Functional Requirements (NFR)

4.1 Upgrade(UPG): Patching (PATCH)

4.1.1 IN_REQ131_v4: Upgrade Database to the Latest Patch Version

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- DB_VUL&PAT_001, DB_VUL&PAT_003

Internal/External Audit Finding Reference-

Nodes- SDP, ngCRS, ngVS, ECMS, EDA, EMM

Level- Operating System

High Level Description- The database patch set needs to be at the latest version.

Solution Proposed- Upgrade the node to the latest available ICP (Intermediate Correction Package).

NOTE: This is not a functional requirement that should be covered by MBSSv3 scope.

References-

N/A

4.1.2 IN_REQ132_v4: Upgrade Operating System to the Latest Patch Version

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_VUL&PAT_001, OS_VUL&PAT_002, OS_VUL&PAT_003, DB_VUL&PAT_002

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- OS patch set needs to be at the latest version.

Solution Proposed- Upgrade the node to the latest ICP (Intermediate Correction Package).

NOTE: This is not a functional requirement that should be covered by MBSSv3 scope.

References-

N/A

4.1.3 IN_REQ133_v4: Upgrade a Supported Version of Web Server

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_VUL&PAT_001, OS_VUL&PAT_002, OS_VUL&PAT_003, DB_VUL&PAT_002

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- The Apache patch set needs to be at the latest version.

Solution Proposed- Upgrade the node to the latest ICP (Intermediate Correction Package).

NOTE: This is not a functional requirement that should be covered by MBSSv3 scope.

References-

N/A

4.2 Relevant Artifact (AF): Predefined System Accounts & Security Implementation Validation (VAL)

4.2.1 IN_REQ135_v4: Provide Screenshot for Security Control Validation

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_VUL&PAT_ADD_001, DB_VUL&PAT_ADD_001, APP_VUL&PAT_ADD_001

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, and Application

High Level Description- Audit Internal/External auditor requires validation to verify that secure Operating system, Database, and Application configurations are in place.

Solution Proposed- After MBSSv4 implementation, screenshot and evidences on the following security areas could be provided, which are applicable and possible:

- SU Logging
- Review of audit logs
- Direct root login
- Cron tabs
- Legal warning
- Account ownership and authorization

References-

N/A

4.2.2 IN_REQ136_v4: Provide Consistent Information Regarding Security Control Configuration

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_VUL&PAT_ADD_002

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- Consistent information regarding the `/etc/passwd` and `/etc/shadow` configuration should be provided.

Solution Proposed- Screenshot on `/etc/passwd` and `/etc/shadow` files could be taken after MBSSv4 implementation and be provided to the auditor team on time.

References-

N/A

4.2.3 IN_REQ139_v4: Disable Browser Autocomplete

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_OS_AF_001,

MTNG_CSBL_NEW_APP_AF_001

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- Most of the Charging System nodes are delivered with statistic web page (sometimes called flat page/stationary page) that is a web page delivered to the user exactly as stored, in contrast to dynamic web pages which are generated by a web application.

By default, browsers remember information that the user submits through input fields on websites. This enables the browser to offer **autocomplete** (i.e. suggest possible completions for fields that the user has started typing in) or autofill (i.e. pre-populate certain fields upon load).

These features can be a **privacy** concern for users, so while browsers can enable users to disable them, they are usually enabled by default. However, some data submitted in forms are either not useful in the future (e.g. a one-time pin) or contain sensitive information (e.g. a unique government identifier or credit card security code). A website might prefer that the browser not remember the values for such fields, even if the browsers **autocomplete** feature is enabled.

Solution Proposed- Autocomplete is a HTML tag attribute used to disable the form auto completion mechanism of the browser. An attacker able to access the browser cache can retrieve sensible information in cleartext. An example of such data is a credit card number or in the case of JIRA, username and password when creating a new user.

Although auto-completion is a useful feature it should be disabled (`autocomplete=”off”`) in forms, which process sensitive data, such account credentials, banking and personal information.

Disabling procedure for "`autocomplete`" depends on the type of used Web Browser.

To **disable** autocompletion in forms, a website can set the autocomplete attribute to "off":

```
autocomplete="off"
```

To **disable** autocomplete for a field, add `autocomplete="off"` attribute to that field, e.g. text input field for a name:

```
<form ...>
...
<input type="text" name="name" autocomplete="off">
...
</form>
```

OR

```
<form method="post" action="/form">
  […]
  <div>
    <label for="cc">Credit card:</label>
    <input type="text" id="cc" name="cc" autocomplete="off">
  </div>
</form
```

To **disable** autocomplete for a whole form, add autocomplete="off" attribute to the form tag:

```
<form autocomplete="off" ...>
...
<input type="text" name="name">
...
</form>
```

OR

```
<form method="post" action="/form" autocomplete="off">
[…]
</form>
```

References-

Reference Document	Chapter
3PP Library	
Form Autocomplete	Turn autocomplete ON/OFF programmatically **NOTE:** Atlassian Blog (Public Information)

Web Security (Securing your site): How to Turn Off Form Autocompletion	Disabling autocompletion **NOTE:** MDN Mozilla Developer Network

4.3 Compliance Monitoring (CPL)

4.3.1 IN_REQ138_v4: Initiate a Vulnerability Scan after Implementation

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_VUL&PAT_004, DB_VUL&PAT_004

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- After MBSSv4 implementation MTN IRANCELL should run a vulnerability scanning to check their charging system security compliance status to MTN Group CS baseline.

Solution Proposed- No matter how securely a system has been installed and hardened, administrator and user activity over time can introduce security exposures. After MBSSv4 implementation, Ericsson recommends running a vulnerability scanning on a regular basis

References-

N/A

4.3.2 IN_REQ141_v4: Security Compliance Checklist Automation

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_OS_CPL_001,

MTNG_CSBL_NEW_DB_CPL_001,

MTNG_CSBL_NEW_APP_CPL_001

Internal/External Audit Finding Reference- N/A

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- Checklist is to be used to audit the baseline security requirements(MBSS) installation and track the compliance status. This checklist is just that “a checklist” and does not contain any script or CLI commands because it is intended to be just a list rather than a “how to” implement the baseline requirements.

Solution Proposed- Ericsson Security Manager (ESM) product provides a Security Compliance and Monitoring tool to help automate checklist serial of tasks intended to be performed regularly.

ESM compliance tool is all about monitoring and assessing overall security architecture and security program (implemented MBSS security controls for charging network and mediation nodes) and help to ensure that MTN Irancell operations for charging system remain within an acceptable level of risk when changes are made to the hardware, software, computer code, or environment of operation.

References-

NA

4.4 Audit Logs Review (REV)

4.4.1 IN_REQ137_v4: Perform Regular Reviews of Audit Logs

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_VUL&PAT_ADD_003, DB_VUL&PAT_ADD_002

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database

High Level Description- The audit logs should be reviewed on a regular basis by an independent individual e.g. Business Risk Management (BRM).

Solution Proposed- Usage of Security Information and Event Management (SIEM) solution e.g. Ericsson Centralized Audit Logging (ECAL), Arcsight, Imperva, etc., will help MTN IRANCELL management to capture, analyze and subsequently act on log and alert information collected from a wide array of systems across the operational network including charging and mediation.

References-

N/A

4.5 Password Recovery (RECOV)

4.5.1 IN_REQ0134_v4: Reset/Recover Root Password

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- OS_ACC_031

Internal/External Audit Finding Reference-

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System

High Level Description- There is chance to lose the root password due to mistyping in case of defective keyboard while changing the password or due to bad password management. In that situation recovering the root password is the only solution and there are various methods available for resetting a root password in Solaris and Linux distributions. However, these methods require the physical access of the server or the remote console mechanism.

Solution Proposed-

Operating System

a) Linux:

Recovering root password with CD/DVD – For recovering the root password in RHEL distribution use the Rescue mode to boot the system with CD/DVD and mount the rescue filesystem. After successful mount change the environment to root and use `passwd` command to change the root password.

Recovering root password without CD/DVD – For recovering the root password in RHEL distribution use GRUB to enter in single user mode which automatically tries to mount the file system. Remount the file system with `rw` permissions and then use `passwd` command to change the root password.

NOTE: Recovering root password require physical access to the server to perform any of the recovery method.

References-

Reference Document	Chapter
3PP Library	
Red Hat Enterprise Linux 6.8 Installation Guide	36 Basic System Recovery
	36.1.1.3 Root Password
	36.1.2 Booting into Rescue Mode
	36.1.3 Booting into Single-User Mode

4.6 Pre-Defined System Accounts Properties (PREDSA)

4.6.1 IN_REQ140_v4: Predefined System Accounts Properties

The requirement is defined to meet the following MTN CS security baseline standards:

Requirement Tag- MTNG_CSBL_NEW_OS_PREDSA_001, MTNG_CSBL_NEW_DB_ PREDSA _001, MTNG_CSBL_NEW_APP_ PREDSA _001

Internal/External Audit Finding Reference- N/A

Nodes- SDP, AIR, ngCRS, ngVS, CCN, ECMS, EDA, EMM, CS-NMT

Level- Operating System, Database, Application

High Level Description- The Charging System and Mediation nodes include several predefined system accounts (user IDs and passwords).

This REQ is considered as main input for IN_REQ015_v4: Assign or Change Password to Default System Account.

Solution Proposed- User Management principles are defined within charging system. It provides guidelines and information for managing groups and user accounts. Different types of default accounts are provided:

- **Predefined** User and group accounts installed with the operating system.
- **Built-In** User and group accounts installed with the operating system, applications, and services, for example during node installation and or upgrade operation.
- **Implicit Special** groups created implicitly when accessing network resources; also known as special identities.

It’s not possible to delete or change the predefined user IDs, but with admin permissions, it is possible to change the passwords for the predefined user IDs in the user management access tools provided by the node.

Predefined System accounts are demonstrated in Table 6: Predefined system accounts with high privilege

References-

5 The Baseline Scope - Enhancement

5.1 MTN Group CS Security Baseline Extension – The Mapping

The Table 11 below illustrates the list of MTN Group CS Security Baseline Extension/Enhancement requirements on the current Charging and mediation deployed nodes in scope.

A control objective (REQ tag Slogan) based on the nodes security capabilities, has been identified to mitigate the risks associated with each requirement. The applicability of those requirements and control objectives has also been checked against the target nodes security functionalities.

Table 11 MTN Group Baseline Extension vs. Requirement Analysis (REQ Tags)

REQ Tag	Requirement Slogan	Security Area	Baseline Requirement Tag
IN_REQ_002_v4	Minimize the Use of Generic User Accounts	Access Control (ACC)	MTNG_CSBL_NEW_OS_ACC_001
IN_REQ33_v4	Force System to Prompt for Password in Single User Mode	Access Control (ACC)	MTNG_CSBL_NEW_OS_ACC_002
IN_REQ040_v4	Set Permission for Cron Job File	Access Control (ACC)	MTNG_CSBL_NEW_OS_ACC_003
IN_REQ041_v4	Remove SUID Bit for the Keys Files	Access Control (ACC)	MTNG_CSBL_NEW_OS_ACC_004
IN_REQ042_v4	Set Default Shell for User/Service Accounts to Null	Access Control (ACC)	MTNG_CSBL_NEW_OS_ACC_005
IN_REQ043_v4	Set appropriate UMASK default value	Access Control (ACC)	MTNG_CSBL_NEW_OS_ACC_006
IN_REQ054_v4	Secure RPC Portmapper	Hardening (HARD)	MTNG_CSBL_NEW_OS_HARD_001
IN_REQ056_v4	Disable CTRL-Alt -DEL Functionality	Hardening (HARD)	MTNG_CSBL_NEW_OS_HARD_002
IN_REQ075_v4	Use WAF and DoS Protection for Web Server	Hardening (HARD)	MTNG_CSBL_NEW_APP_HARD_003

IN_REQ076_v4	Run Web Server as Separate User and Group	Hardening (HARD)	MTNG_CSBL_NEW_APP_HARD_004
IN_REQ077_v4	Restrict Access to root Directory in Web Server	Hardening (HARD)	MTNG_CSBL_NEW_APP_HARD_005
IN_REQ078_v4	Set Appropriate Permissions for Web Server Directories	Hardening (HARD)	MTNG_CSBL_NEW_APP_HARD_006
IN_REQ079_v4	Disable Directory Listing in Web Server	Hardening (HARD)	MTNG_CSBL_NEW_APP_HARD_007
IN_REQ080_v4	Disable Directory Browsing in Web Server	Hardening (HARD)	MTNG_CSBL_NEW_APP_HARD_008
IN_REQ081_v4	Disable Unnecessary Components of Web Server	Hardening (HARD)	MTNG_CSBL_NEW_APP_HARD_009
IN_REQ082_v4	Cross Site Scripting (XSS) Protection in Web Server	Hardening (HARD)	MTNG_CSBL_NEW_APP_HARD_010
IN_REQ084_v4	Disallow .htaccess in Apache HTTP Sever	Hardening (HARD)	MTNG_CSBL_NEW_APP_HARD_011
IN_REQ085_v4	Protect the Shutdown Port in Apache Tomcat	Hardening (HARD)	MTNG_CSBL_NEW_APP_HARD_012
IN_REQ086_v4	Prevent Etag Information Leakage	Hardening (HARD)	MTNG_CSBL_NEW_APP_HARD_013
IN_REQ0139_v4	Disable Browser Autocomplete	Non-Functional (AF)	MTNG_CSBL_NEW_OS_AF_001, MTNG_CSBL_NEW_APP_AF_001
IN_REQ038_v4	SDP Dump Tool Configuration and File Transfer Permission	Non-Functional (AF)	MTNG_CSBL_NEW_OS_AF_002, MTNG_CSBL_NEW_APP_AF_002
IN_REQ0140_v4	Predefined System Accounts Properties	Non-Functional (PREDSA)	MTNG_CSBL_NEW_OS_ PREDSA_001, MTNG_CSBL_NEW_DB_PREDSA_001, MTNG_CSBL_NEW_APP_PREDSA_001,
IN_REQ0141_v4	Security Compliance Checklist (Automation)	Non-Functional (CPL)	MTNG_CSBL_NEW_OS_CPL_001, MTNG_CSBL_NEW_DB_CPL_001, MTNG_CSBL_NEW_APP_CPL_001

6 Traceability Matrix

The purpose of the requirements tracing is to document the links between the MTN Group CS Baseline and the IN Nodes (in scope) security capabilities. The process will facilitate to define the amount of the work and time required to capture and meet all applicable requirements intended to be implemented in MTN Irancell Charging environment

Table 12 Traceability Matrix-MTN Group Baseline

REQ Tag	Requirement Slogan	Baseline Requirement Tag	Comments
Functional Requirements (FR)			
IN_REQ001_v4	Prevent Sharing of Privileged Accounts	OS_ACC_001, OS_ACC_006, OS_ACC_007, OS_ACC_008, DB_ACC_001, DB_ACC_002, DB_ACC_003, DB_ACC_004, APP_ACC_001, APP_ACC_002	
IN_REQ002_v4	Minimize the Use of Generic User Accounts	MTNG_CSBL_NEW_OS_ACC_001	Baseline enhancement Requirement
IN_REQ003_v4	Remove or Disable Inactive Users	OS_ACC_004, DB_ACC_008, APP_ACC_006	
IN_REQ004_v4	Prevent Excessive Privileges on DB Public Roles	DB_ACC_010	
IN_REQ015_v4	Assign or Change Password to Default System Account	OS_ACC_024, DB_ACC_019, DB_ACC_023, APP_ACC_016	
IN_REQ016_v4	Change Default Passwords after Node Installation/Upgrade	OS_ACC_024, DB_ACC_019, DB_ACC_020, DB_ACC_023, APP_ACC_016	
IN_REQ017_v4	Change default ILOM password	OS_ACC_024	
IN_REQ018_v4	Set Password Ageing	OS_ACC_019, OS_ACC_020, OS_ACC_022, DB_ACC_013, DB_ACC_015, DB_ACC_016, DB_ACC_018, APP_ACC_007, APP_ACC_008, APP_ACC_015	

IN_REQ019_v4	Set Password Complexity	OS_ACC_016, OS_ACC_017, OS_ACC_018, OS_ACC_025, OS_ACC_021, OS_ACC_023, APP_ACC_009, APP_ACC_014, DB_ACC_014, DB_ACC_024, DB_ACC_012	
IN_REQ020_v4	Set Password Complexity Verification Function	OS_ACC_016, OS_ACC_017, OS_ACC_023, OS_ACC_025, OS_ACC_030, DB_ACC_024, APP_ACC_009, APP_ACC_014	
IN_REQ026_v4	Disable Direct Root Login in LINUX	OS_ACC_007	
IN_REQ027_v4	Disallow Root Access via FTP	OS_ACC_009	
IN_REQ028_v4	Disable Anonymous FTP Login	OS_HARD_011	
IN_REQ029_v4	Use of SSH Key Based Authentication	OS_ACC_010, OS_ACC_011	
IN_REQ030_v4	Configure the SSH Session Timeout	OS_ACC_027	
IN_REQ031_v4	Disable/Configure Weak SNMP Community String	OS_HARD_004	
IN_REQ032_v4	Set Account Lockout Threshold for Invalid Logon Attempts	OS_ACC_005, DB_ACC_011, APP_ACC_003, DB_ACC_017	
IN_REQ033_v4	Force System to Prompt for Password in Single User Mode	MTNG_CSBL_NEW_OS_ACC_002, OS_ACC_029	Baseline enhancement Requirement
IN_REQ034_v4	Enable Database Authentication	DB_ACC_019, DB_ACC_023, DB_ACC_020	
IN_REQ035_v4	Prevent Direct Login to the Database	DB_ACC_001, DB_ACC_002	
IN_REQ036_v4	Restrict Mounting of NFS Shares	OS_ACC_013, OS_ACC_014	
IN_REQ038_v4	SDP Dump Tool Configuration and File Transfer Permission	MTNG_CSBL_NEW_OS_AF_002, MTNG_CSBL_NEW_APP_AF_002	Baseline enhancement Requirement

IN_REQ040_v4	Set Permission for Cron Job File	MTNG_CSBL_NEW_OS_ACC_003	Baseline enhancement Requirement
IN_REQ041_v4	Remove SUID Bit for the Keys Files	MTNG_CSBL_NEW_OS_ACC_004	Baseline enhancement Requirement
IN_REQ042_v4	Set Default Shell for User/Service Accounts to Null	MTNG_CSBL_NEW_OS_ACC_005	Baseline enhancement Requirement
IN_REQ043_v4	Set appropriate UMASK default value	MTNG_CSBL_NEW_OS_ACC_006	Baseline enhancement Requirement
IN_REQ044_v4	Create and Enable Warning Banners	OS_HARD_007	
IN_REQ045_v4	Configure Host Based Firewall	MR-036-NW002	
IN_REQ046_v4	Configure TCP Wrappers	MR-036-NW002	
IN_REQ052_v4	Disable Unsecured Services	OS_HARD_006, OS_HARD_003, APP_HARD_006	
IN_REQ053_v4	Disable Unused Services	OS_HARD_002	
IN_REQ054_v4	Secure RPC Portmapper	MTNG_CSBL_NEW_OS_HARD_001	Baseline enhancement Requirement
IN_REQ055_v4	Enable ExecShield Buffer Overflows Protection in LINUX	OS_HARD_009	
IN_REQ056_v4	Disable CTRL-Alt -DEL Functionality	MTNG_CSBL_NEW_OS_HARD_002	Baseline enhancement Requirement
IN_REQ057_v4	Prevent SMTP Information Disclosure	OS_VUL&PAT_005	
IN_REQ058_v4	SMTP Version shall not be disclosed	OS_VUL&PAT_006	
IN_REQ059_v4	Restrict Concurrent Unauthenticated User Access from Different Terminals	OS_ACC_026	

IN_REQ067_v4	Resource Limits Initialization for DB	DB_ACC_021	
IN_REQ073_v4	Web Server Version shall not be disclosed	OS_ACC_001	
IN_REQ074_v4	Disable Trace/Track in Web Server	OS_HARD_012	
IN_REQ075_v4	Use WAF and DoS Protection for Web Server	MTNG_CSBL_NEW_APP_HARD_003	Baseline enhancement Requirement
IN_REQ076_v4	Run Web Server as Separate User and Group	MTNG_CSBL_NEW_APP_HARD_004	Baseline enhancement Requirement
IN_REQ077_v4	Restrict Access to root Directory in Web Server	MTNG_CSBL_NEW_APP_HARD_005	Baseline enhancement Requirement
IN_REQ078_v4	Set Appropriate Permissions for Web Server Directories	MTNG_CSBL_NEW_APP_HARD_006	Baseline enhancement Requirement
IN_REQ079_v4	Disable Directory Listing in Web Server	MTNG_CSBL_NEW_APP_HARD_007	Baseline enhancement Requirement
IN_REQ080_v4	Disable Directory Browsing in Web Server	MTNG_CSBL_NEW_APP_HARD_008	Baseline enhancement Requirement
IN_REQ081_v4	Disable Unnecessary Components of Web Server	MTNG_CSBL_NEW_APP_HARD_009	Baseline enhancement Requirement
IN_REQ082_v4	Cross Site Scripting (XSS) Protection in Web Server	MTNG_CSBL_NEW_APP_HARD_010	Baseline enhancement Requirement
IN_REQ083_v4	Disable/Remove CGI Test Script	APP_HARD_004	
IN_REQ084_v4	Disallow .htaccess in Apache HTTP Sever	MTNG_CSBL_NEW_APP_HARD_011	Baseline enhancement Requirement
IN_REQ085_v4	Protect the Shutdown Port in Apache Tomcat	MTNG_CSBL_NEW_APP_HARD_012	Baseline enhancement Requirement
IN_REQ086_v4	Prevent ETag Information Leakage	MTNG_CSBL_NEW_APP_HARD_013	Baseline enhancement Requirement

IN_REQ090_v4	Enable Audit Logging	OS_LOG_001, OS_LOG_002, DB_LOG_001, DB_LOG_002, DB_LOG_004, APP_LOG_001	
IN_REQ091_v4	Enable Archive Logging	DB_LOG_003	
IN_REQ092_v4	Separate Disk Drives for Archive Logs Storage	DB_LOG_003	
IN_REQ093_v4	Logging of User Activities on OS Level	OS_LOG_003	
IN_REQ094_v4	Restrict Access of Audit Logs	OS_LOG_005, DB_LOG_007, APP_LOG_004	
IN_REQ095_v4	Configuring Remote Syslog from UNIX/LINUX Server	OS_LOG_004, DB_LOG_006, APP_LOG_002, APP_LOG_003	
IN_REQ101_v4	Disable SSL Weak Ciphers in Web Server	OS_HARD_013	
IN_REQ102_v4	Disable SSLv3 and TLSv1 Protocol Weak CBC Mode	OS_HARD_014	
IN_REQ103_v4	Disable SSH Weak CBC Mode Ciphers	OS_HARD_016	
IN_REQ104_v4	Setting X11 Protocol Forwarding	OS_ACC_028	
Non-Functional Requirements (NFR)			
IN_REQ131_v4	Upgrade Database to the Latest Patch Version	DB_VUL&PAT_001, DB_VUL&PAT_003	
IN_REQ132_v4	Upgrade Operating System to the Latest Patch Version	OS_VUL&PAT_001, OS_VUL&PAT_002, OS_VUL&PAT_003, DB_VUL&PAT_002	
IN_REQ133_v4	Upgrade a Supported Version of Web Server	OS_VUL&PAT_001, OS_VUL&PAT_002, OS_VUL&PAT_003, DB_VUL&PAT_002	

IN_REQ134_v4	Reset/Recover Root Password	OS_ACC_031	
IN_REQ135_v4	Provide Screenshot for Security Control Validation	OS_VUL&PAT_ADD_001, DB_VUL&PAT_ADD_001, APP_VUL&PAT_ADD_001	
IN_REQ136_v4	Provide Consistent Information Regarding Security Control Configuration	OS_VUL&PAT_ADD_002	
IN_REQ137_v4	Perform Regular Reviews of Audit Logs	OS_VUL&PAT_ADD_003, DB_VUL&PAT_ADD_002	
IN_REQ138_v4	Initiate a Vulnerability Scan after Implementation	OS_VUL&PAT_004, DB_VUL&PAT_004	
IN_REQ139_v4	Disable Browser Autocomplete	MTNG_CSBL_NEW_OS_AF_001, MTNG_CSBL_NEW_APP_AF_001	Baseline enhancement Requirement
IN_REQ140_v4	Predefined System Accounts Properties	MTNG_CSBL_NEW_OS_AF_003, MTNG_CSBL_NEW_DB_AF_001, MTNG_CSBL_NEW_APP_AF_003,	Baseline enhancement Requirement
IN_REQ141_v4	Security Compliance Checklist (Automation)	MTNG_CSBL_NEW_OS_CPL_001, MTNG_CSBL_NEW_DB_CPL_001, MTNG_CSBL_NEW_APP_CPL_001	Baseline enhancement Requirement

7 References

7.1 Ericsson Documentation

[1] CS Security Baseline
https://erilink.ericsson.se/eridoc/erl/objectId/09004cff8cef475b?docno=BICS-18:000166Uen&action=current&format=excel12book

[2] CPI Library, CS 18
http://cpistore.internal.ericsson.com/alexserv?li=EN/LZN7410241R6A

[3] CAL Library, CS 18
http://calstore.internal.ericsson.com/alexserv?li=EN/LZN7410242R6A

[4] CPI Library, Ericsson Multi Mediation 18
http://cpistore.internal.ericsson.com/alexserv?li=EN/LZN7059062R1A

[5] CPI Library, Ericsson Dynamic Activation 1 Sep-17
http://cpistore.internal.ericsson.com/alexserv?id=8795

[6] CPI Library, Ericsson SNMP Agent (ESA) 4.0
http://cpistore.internal.ericsson.com/alexserv?li=EN/LZN7020358R1A

[7] Overall Guide Security Recommendations and Policies
http://cpistore.internal.ericsson.com/alexserv?ac=LINKEXT&li=EN/LZN7410193R11B&FN=6_1543-FAV10172_4Uen.L.html&SL=EN/LZN7410241R3B

[8] Security Management User Guide, 1/1553-ANA 901 05/1 Uen J
http://cpistore.internal.ericsson.com/alexserv?ac=LINKEXT&li=EN/LZN7410076R14D&FN=1_1553-ANA90106Uen.J.html

[9] System Capability Description – Security Management in Charging System, 2/1551-FAY 311 21/3 Uen C
https://erilink.ericsson.se/eridoc/erl/objectId/09004aac8211b800?docno=2/1551-FAY31121/3Uen&format=sdif

7.2 3PP Documentation

[10] CIS Red Hat Enterprise Linux 6 Benchmark v1.4.0
https://benchmarks.cisecurity.org/tools2/linux/CIS_Red_Hat_Enterprise_Linux_6_Benchmark_v1.4.0.pdf

[11] CIS Red Hat Enterprise Linux 7 Benchmark, v2.1.0
https://benchmarks.cisecurity.org/tools2/linux/CIS_Red_Hat_Enterprise_Linux_7_Benchmark_v2.1.0.pdf

[12] CIS SUSE Linux Enterprise Server 12 Benchmark, v1.0.0
https://benchmarks.cisecurity.org/tools2/linux/CIS_SUSE_Linux_Enterprise_Server_12_Benchmark_v1.0.0.pdf

[13] CIS Apache HTTP Server 2.2 Benchmarks, v3.2.0
https://benchmarks.cisecurity.org/tools2/apache/CIS_Apache_HTTP_Server_2.2_Benchmark_v3.2.0.pdf

[14] Red Hat Enterprise Linux 6.8 Deployment Guide
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/s2-ftp-servers-vsftpd.html

[15] Red Hat Enterprise Linux 6.8 Installation Guide
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Installation_Guide/ap-rescuemode.html

[16] Red Hat Enterprise Linux 6.8 Security Guide
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf

[17] Red Hat Enterprise Linux 7 Security Guide
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Controlling_Root_Access.html

[18] Red Hat Enterprise Linux 7 System Administrator's Guide
https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/sect-Managing_Services_with_systemd-Services.html#sect-Managing_Services_with_systemd-Services-List

[19] SUSE LINUX Enterprise Server Documentation
https://www.suse.com/documentation/sles11/book_sle_tuning/data/cha_tuning_resources_services.html

[20] Opensuse.org SuSEfirewall2
https://en.opensuse.org/SuSEfirewall2

[21] Cassandra: The Definitive Guide
https://pdfs.semanticscholar.org/9b82/7d55167f6a60957f7e9f38178d61e74d8db1.pdf

[22] TimesTen In-Memory Database Operations Guide
https://docs.oracle.com/cd/E11882_01/timesten.112/e21633/daemon.htm#TTOPR211

[23] PostgreSQL 8.4.22 Documentation
https://www.postgresql.org/docs/8.4/static/ddl-priv.html

[24] PostgreSQL 9.0.22 Documentation
https://www.postgresql.org/files/documentation/pdf/9.0/postgresql-9.0-A4.pdf

8 Appendix

8.1 Appendix A: Logging in CCN

TSP provides the following logs that record events important from security auditing perspective.

Table 13:List of logs provided by TSP

Log	Logged Command	Location
Debug Shell Logs[27]	1. Commands issued in `TelORB` Shell are logged in `applog.telorbshell` applog file 2. Commands issued in `U-Qtil` are logged in `applog.qutil` applog file. 3. Commands issued in `T-Util` are logged in `applog.tutil` applog file.	`/opt/telorb/axe/tsp/applog/applog.<telorbshell,qutil,tutil>`
Bash Command Log[28]	The log record consists of the following fields: **UserId:** The Linux user who executed the command **Host:** The host name of the client **Processor:** The host name of the processor the command was executed on **SessionId:** Session identifier **Director:** The current directory of the user.	`/opt/telorb/axe/tsp/syslog_collector/sec_log/bashcommand/bashcommand.log`

[27] *Commands issued in debug shells (TelORB Shell, Q-Util, T-Util) are logged in the applog files.*
[28] *This log contains all commands executed in the bash shell of the IO and Linux Traffic processors.*

	Command: The actual command executed	
TSP Security Applog	1. The log records have the fields in the `TSP_Security` logging database. See details in [8], Table 6 Log Record Fields in the TSP_Security Logging Database 2. The TSP events that are initiated from TelORB Manager or by the CM are logged into the `TSP_Security applog` file. See details regarding the TelORB Manager Events in [8], Table 7	`/opt/telorb/axe/tsp/applog/\` `applog.TSP_Security.*`
TSP IKE Applog[29]	The logged operations include the following: 1. Start of TSP IKE daemon 2. Successful negotiations 3. Failed negotiation attempts 4. Informational and error messages emerged during negotiations	`/opt/telorb/axe/tsp/applog/applog.IKE.*`
IO Firewall Log	See details in [8], Chapter 3.5	`/var/log/firewall.log`
IO Kernel Audit Log	See details in [8], Chapter 3.6	`/var/log/audit/kernelaudit.log`
Linux Authentication Log	See details in [8], Chapter 3.7	`/var/log/sec.audit.log`

[29] *This log contains operations carried out by TSP-IKE daemon*

Node Management Toolbox Audit Log	See details in [8], Chapter 3.8	`/opt/telorb/axe/tsp/syslog_collector/\sec_log/apache/access.log`
User Database Audit Log for Fail-safe and COM Accounts[30]	See details in [8], Chapter 3.9	`/var/log/io.ldap.log`

Role required viewing the logs: `tspSecAdmin`

[30] *This log contains all access attempts to the local user database that stores the fail-safe users and, if configured so, the COM users.*

8.2 Appendix B: How to Configure SSH Key-Based Authentication on a LINUX Server

Introduction

SSH, or secure shell, is an encrypted protocol used to administer and communicate with servers. When working with a Linux server, chances are, you will spend most of your time in a terminal session connected to your server through SSH.

While there are a few different ways of logging into an SSH server, in this guide, we'll focus on setting up SSH keys. SSH keys provide an easy, yet extremely secure way of logging into your server. For this reason, this is the method we recommend for all users.

How Do SSH Keys Work?

An SSH server can authenticate clients using a variety of different methods. The most basic of these is password authentication, which is easy to use, but not the most secure.

Although passwords are sent to the server in a secure manner, they are generally not complex or long enough to be resistant to repeated, persistent attackers. Modern processing power combined with automated scripts make brute forcing a password-protected account very possible. Although there are other methods of adding additional security (fail2ban, etc.), SSH keys prove to be a reliable and secure alternative.

SSH key pairs are two cryptographically secure keys that can be used to authenticate a client to an SSH server. Each key pair consists of a public key and a private key.

The client retains the private key and should be kept secret. Any compromise of the private key will allow the attacker to log into servers that are configured with the associated public key without additional authentication. As an additional precaution, the key can be encrypted on disk with a passphrase.

The associated public key can be shared freely without any negative consequences. The public key can be used to encrypt messages that only the private key can decrypt. This property is employed as a way of authenticating using the key pair.

The public key is uploaded to a remote server that you want to be able to log into with SSH. The key is added to a special file within the user account you will be logging into called `~/.ssh/authorized_keys`.

When a client attempts to authenticate using SSH keys, the server can test the client on whether they are in possession of the private key. If the client can prove that it owns the private key, a shell session is spawned, or the requested command is executed.

An overview of the flow is shown in this diagram:

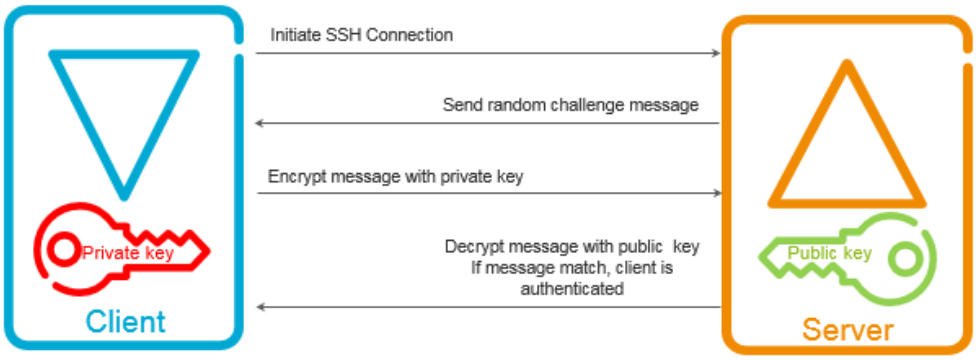

Figure 2 SSH Key Authentication

The diagram shows a laptop connecting to a server, but it could just as easily be one server connecting to another server.

How to Create SSH Keys

The first step to configure SSH key authentication to your server is to generate an SSH key pair on your local computer.

To do this, we can use a special utility called ssh-keygen, which is included with the standard OpenSSH suite of tools. By default, this will create a 2048-bit RSA key pair, which is fine for most uses.

On your local computer, generate a SSH key pair by typing:

```
ssh-keygen

Generating public/private rsa key pair.
Enter file in which to save the key
(/home/username/.ssh/id_rsa):
```

The utility will prompt you to select a location for the keys that will be generated. By default, the keys will be stored in the `~/.ssh` directory within your user's home directory. The private key will be called `id_rsa` and the associated public key will be called `id_rsa.pub`.

Usually, it is best to stick with the default location at this stage. Doing so will allow your SSH client to automatically find your SSH keys when attempting to authenticate. If you would like to choose a non-standard path, type that in now, otherwise, press ENTER to accept the default.

If you had previously generated an SSH key pair, you may see a prompt that looks like this:

```
/home/username/.ssh/id_rsa already exists.
Overwrite (y/n)?
```

If you choose to overwrite the key on disk, you will **not** be able to authenticate using the previous key anymore. Be very careful when selecting yes, as this is a destructive process that cannot be reversed.

```
Created directory '/home/username/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

Next, you will be prompted to enter a passphrase for the key. This is an optional passphrase that can be used to encrypt the private key file on disk.

You may be wondering what advantages an SSH key provides if you still need to enter a passphrase. Some of the advantages are:

- The private SSH key (the part that can be passphrase protected), is never exposed on the network. The passphrase is only used to decrypt the key on the local machine. This means that network-based brute forcing will not be possible against the passphrase.
- The private key is kept within a restricted directory. The SSH client will not recognize private keys that are not kept in restricted directories. The key itself must also have restricted permissions (read and write only available for the owner). This means that other users on the system cannot snoop.
- Any attacker hoping to crack the private SSH key passphrase must already have access to the system. This means that they will already have access to your user account or the root account. If you are in this position, the passphrase can prevent the attacker from immediately logging into your other servers. This will hopefully give you time to create and implement a new SSH key pair and remove access from the compromised key.

Since the private key is never exposed to the network and is protected through file permissions, this file should never be accessible to anyone other than you (and the root user). The passphrase serves as an additional layer of protection in case these conditions are compromised.

A passphrase is an optional addition. If you enter one, you must provide it every time you use this key (unless you are running SSH agent software that stores the decrypted key). We recommend using a passphrase, but if you do not want to set a passphrase, you can simply press ENTER to bypass this prompt.

```
Your identification has been saved in
/home/username/.ssh/id_rsa.
Your public key has been saved in
/home/username/.ssh/id_rsa.pub.
The key fingerprint is:
a9:49:2e:2a:5e:33:3e:a9:de:4e:77:11:58:b6:90:26
username@remote_host
The key's randomart image is:
+--[ RSA 2048]----+
|     ..o         |
|   E o= .        |
|    o. o         |
|        ..       |
|      ..S        |
|     o.        |
|   =o.+.         |
|. =++..          |
|o=++.            |
+-----------------+
```

You now have a public and private key that you can use to authenticate. The next step is to place the public key on your server so that you can use SSH key authentication to log in.

How to Copy a Public Key to your Server

If you already have a server available and did not embed keys upon creation, you can still upload your public key and use it to authenticate to your server.

The method you use depends largely on the tools you have available and the details of your current configuration. The following methods all yield the same result. The easiest, most automated method is first and the ones that follow each require additional manual steps if you are unable to use the preceding methods.

Copying your Public Key Using SSH-Copy-ID

The easiest way to copy your public key to an existing server is to use a utility called `ssh-copy-id`. Because of its simplicity, this method is recommended if available.

The `ssh-copy-id` tool is included in the OpenSSH packages in many distributions, so you may have it available on your local system. For this method to work, you must already have password-based SSH access to your server.

To use the utility, you simply must specify the remote host that you would like to connect to and the user account that you have password SSH access to. This is the account where your public SSH key will be copied.

The syntax is:

```
ssh-copy-id username@remote_host
```

You may see a message like this:

```
The authenticity of host '111.111.11.111 (111.111.11.111)'
can't be established.
ECDSA key fingerprint is
fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.
Are you sure you want to continue connecting (yes/no)? yes
```

This just means that your local computer does not recognize the remote host. This will happen the first time you connect to a new host. Type "yes" and press ENTER to continue.

Next, the utility will scan your local account for the `id_rsa.pub` key that we created earlier. When it finds the key, it will prompt you for the password of the remote user's account:

```
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new
key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed
-- if you are prompted now it is to install the new keys
username@111.111.11.111's password:
```

Type in the password (your typing will not be displayed for security purposes) and press ENTER. The utility will connect to the account on the remote host using the password you provided. It will then copy the contents of your `~/.ssh/id_rsa.pub` key into a file in the remote account's home `~/.ssh` directory called `authorized_keys`.

You will see output that looks like this:

```
Number of key(s) added: 1
```

```
Now try logging into the machine, with:   "ssh
'username@111.111.11.111'"
and check to make sure that only the key(s) you wanted were
added.
```

At this point, your `id_rsa.pub` key has been uploaded to the remote account. You can continue onto the next section.

Copying your Public Key Using SSH

If you do not have `ssh-copy-id` available, but you have password-based SSH access to an account on your server, you can upload your keys using a conventional SSH method.

We can do this by outputting the content of our public SSH key on our local computer and piping it through an SSH connection to the remote server. On the other side, we can make sure that the `~/.ssh` directory exists under the account we are using and then output the content we piped over into a file called `authorized_keys` within this directory.

We will use the >> redirect symbol to append the content instead of overwriting it. This will let us add keys without destroying previously added keys.

The full command will look like this:

```
cat ~/.ssh/id_rsa.pub | ssh username@remote_host "mkdir -p
~/.ssh && cat >> ~/.ssh/authorized_keys"
```

You may see a message like this:

```
The authenticity of host '111.111.11.111 (111.111.11.111)'
can't be established.
ECDSA key fingerprint is
fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.
Are you sure you want to continue connecting (yes/no)? yes
```

This just means that your local computer does not recognize the remote host. This will happen the first time you connect to a new host. Type "yes" and press ENTER to continue.

Afterwards, you will be prompted with the password of the account you are attempting to connect to:

```
username@111.111.11.111's password:
```

After entering your password, the content of your `id_rsa.pub` key will be copied to the end of the `authorized_keys` file of the remote user's account. Continue to the next section if this was successful.

Copying your Public Key Manually

If you do not have password-based SSH access to your server available, you must do the above process manually.

The content of your `id_rsa.pub` file must be added to a file at `~/.ssh/authorized_keys` on your remote machine somehow.

To display the content of your `id_rsa.pub` key, type this into your local computer:

```
cat ~/.ssh/id_rsa.pub
```

You will see the key's content, which may look something like this:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQCqql6MzstZYh1TmWWv11q5O3pISj2Z
Fl9HgH1JLknLLx44+tXfJ7mIrKNx
```

Access your remote host using whatever method you have available.

Once you have access to your account on the remote server, you should make sure the `~/.ssh` directory is created. This command will create the directory if necessary, or do nothing if it already exists:

```
mkdir -p ~/.ssh
```

Now, you can create or modify the `authorized_keys` file within this directory. You can add the contents of your `id_rsa.pub` file to the end of the `authorized_keys` file, creating it if necessary, using this:

```
echo public_key_string >> ~/.ssh/authorized_keys
```

In the above command, substitute the `public_key_string` with the output from the `cat ~/.ssh/id_rsa.pub` command that you executed on your local system. It should start with `ssh-rsa AAAA...`.

If this works, you can move on to try to authenticate **without** a password.

Authenticate to your Server Using SSH Keys

If you have successfully completed one of the procedures above, you should be able to log into the remote host *without* the remote account's password.

The basic process is the same:

```
ssh username@remote_host
```

If this is your first time connecting to this host (if you used the last method above), you may see something like this:

```
The authenticity of host '111.111.11.111 (111.111.11.111)'
can't be established.

ECDSA key fingerprint is
fd:fd:d4:f9:77:fe:73:84:e1:55:00:ad:d6:6d:22:fe.

Are you sure you want to continue connecting (yes/no)? yes
```

This just means that your local computer does not recognize the remote host. Type "yes" and then press ENTER to continue.

If you did not supply a passphrase for your private key, you will be logged in immediately. If you supplied a passphrase for the private key when you created the key, you will be required to enter it now. Afterwards, a new shell session should be spawned for you with the account on the remote system.

If successful, continue to find out how to lock down the server.

Disabling Password Authentication on your Server

If you could login to your account using SSH without a password, you have successfully configured SSH key-based authentication to your account. However, your password-based authentication mechanism is still active, meaning that your server is still exposed to brute-force attacks.

Before completing the steps in this section, make sure that you either have SSH key-based authentication configured for the root account on this server, or preferably, that you have SSH key-based authentication configured for an account on this server with `sudo` access. This step will lock down password-based logins, so ensuring that you have will still can get administrative access is essential.

Once the above conditions are true, log into your remote server with SSH keys, either as root or with an account with `sudo` privileges. Open the SSH daemon's configuration file:

```
sudo nano /etc/ssh/sshd_config
```

Inside the file, search for a directive called `PasswordAuthentication`. This may be commented out. Uncomment the line and set the value to "no". This will disable your ability to log in through SSH using account passwords:

```
PasswordAuthentication no
```

Save and close the file when you are finished. To implement the changes we just made, you must restart the service.

On Ubuntu or Debian machines, you can issue this command:

```
sudo service ssh restart
```

On CentOS/Fedora machines, the daemon is called `sshd`:

```
sudo service sshd restart
```

After completing this step, you've successfully transitioned your SSH daemon to only respond to SSH keys.

Conclusion

You should now have SSH key-based authentication configured and running on your server, allowing you to sign in without providing an account password. From here, there are many directions you can head. If you'd like to learn more about working with SSH, take a look at SSH essentials guide.

8.3 Appendix C: Logging Support on Charging System and Mediation

RHEL use the `syslog` () function to log information to the syslog daemon, a privileged user would not have permissions to the file system where syslog messages are logged.

The following Table illustrates the logging support for the Charging & Mediation nodes in scope.

Table 14 Logging Support per Node Type

Node	Type/ Platform	Level	Logging	CPI & 3PP - Doc. Reference	Comment
CHARGING SYSTEM					
SDP	Red Hat Linux (RHEL)	APP	FDS Logging		Application stores audit logs locally Agent needed to parse and send xml to `rsyslog`
		DB	TTLOG	1. CPI Store, SDP System Administrator's Guide, RHEL, Chapter 4.2.2.3 Check syslog Configuration 2. Oracle Documentation - TimesTen	The TimesTen Data Manager uses syslog to log various progress messages. It is highly desirable to configure syslog so that all important TimesTen messages are written to disk in a single file. The following command to examine the syslog configuration `# ttSyslogCheck`
		OS	AUDITD & SYSLOG	1. CPI Store, SDP Hardening Guideline, and Instruction, RHEL, Chapter 4.6 Audit and Logging for OS	The Audit logging and syslog for the OS is active by default.
AIR	Red Hat Linux (RHEL)	APP	FDS Logging	1. CPI Store, AIR System Administrator's Guide, Linux, Chapter 5.15 Audit Logging	Application stores audit logs locally Agent needed to parse and send xml to `rsyslog`
		DB	NA	NA	

		OS	AUDITD & SYSLOG	1.CPI Store, AIR Hardening Guideline, and Instruction, RHEL, Chapter 4.5 Audit and Logging	The Audit logging and syslog for the OS is active by default
ngCRS	Red Hat Linux (RHEL)	APP	CRS – Notification History	CRS Data Collection Guideline 2 Mandatory Data	CRS captures notifications which can be extracted for a specific period using the following command: `# oamcli -c 'show-notification-history --startdate=<yyyyMMddHHmmss> --enddate=<yyyyMMddHHmmss>'`
		DB	PostgreSQL LOG	PostgreSQL 9.4.19 Documentation 18.8. Error Reporting and Logging	Audit Logging can be enabled by updating parameters in the `postgresql.conf` file. The same can be redirected to the syslog using the OS rsyslog configuration
			Oracle Audit	Oracle Database Security Guide 11g Release 2 (11.2)	Audit is enabled by default on the Oracle database for ngCRS
		OS	AUDITD & SYSLOG	RedHat Security Guide 7.6. Understanding Audit Log File	The Audit logging and syslog for the OS is active by default

ngVS	Red Hat Linux (RHEL)	APP	VS Audit	System Administrator Guide Voucher Server 5.0 3.21 Configure Permission List for Audit Log File	Audit log is enabled by default in VS 5.0 and are stored in `/var/log/vs/audit.log` The Audit Logs capture the Source IP, User ID and User Permission details when a user invokes a particular task or functionality
		DB	Cassandra log		Casandra 2.0 doesn't support Audit Logging. This feature is being enabled in the Enterprise version of DataStax Cassandra
		OS	AUDITD & SYSLOG	RedHat Security Guide 7.6. Understanding Audit Log File	The Audit logging and syslog for the OS is active by default
CCN	TSP	APP	Applog	CPI Store Logging User Guide, Security Management User Guide 3.2 Bash Command Log	TSP as a platform provides its applications with a logging framework called Applog that allows them to log events into application-specific flat database files. The Applog files are human readable and tailored for post-processing that is left for the end user once the logs are exported from the TSP node.
		DB	NA		

		OS	Bash command		It is possible to redirect all log records to an external server through the Syslog protocol. The transport protocol for the Syslog can be TCP, UDP, or TLS over TCP. Central Syslog Service is also used to collect log records from the Linux software components in the cluster and IO processors, such as firewall or apache logs.
ECMS	Red Hat Linux (RHEL)	APP			Audit Logging is enabled by default. The LogLevel, RotationFileLimit etc. are configured in the following file:igured in the following file: `/export/home/ecms/config/srv/FUNC_FRMWK_SRV_AuditLog_Registry.xml file`
		DB	Oracle Audit	Oracle Database Security Guide 11g Release 2 (11.2)	Audit is enabled by default on the Oracle database
		OS	AUDITD & SYSLOG	RedHat Security Guide 7.6. Understanding Audit Log File	The Audit logging and syslog for the OS is active by default
CS-NMT	Red Hat Linux (RHEL)	APP	NMT	SUF User Guide System Upgrade Framework 5.4.0 4.4 Audit Logs	Audit Logging is enabled by default. The following events are logged: • Successful login • Failed login • Logout
		DB	NA		

		OS	AUDITD & SYSLOG	RedHat Security Guide 7.6. Understanding Audit Log File	The Audit logging and syslog for the OS is active by default
MEDIATION					
EDA	Red Hat Linux (SUSE Linux)	APP	Dynamic Activation	Function Specification Dynamic Activation Execution Environment Ericsson Dynamic Activation 1 2.6 Logging Service	The following logs are produced: • Application log • Access log • Partially succeeded log • Audit log • Processing log
		DB	Oracle Audit	Oracle Database Security Guide 11g Release 2 (11.2)	Audit is enabled by default on the Oracle database
		OS	AUDITD & SYSLOG	RedHat Security Guide 7.6. Understanding Audit Log File	The Audit logging and syslog for the OS is active by default

EMM	Red Hat Linux (RHEL)	APP	Mediation	Security Policy and Guidelines Ericsson Multi Mediation 15 5.5.1 Multi Mediation Logs Accounting Management Guide Ericsson Multi Mediation 15 3.4 Audit Trail Log	The Multi Mediation system includes the following logs: • Event Logs • Alarm Logs • Audit Trail Log
		DB	PostgreSQL LOG	PostgreSQL 9.4.19 Documentation 18.8. Error Reporting and Logging	Audit Logging can be enabled by updating parameters in the `postgresql.conf` file. The same can be redirected to the syslog using the OS rsyslog configuration
		OS	AUDITD & SYSLOG	RedHat Security Guide 7.6. Understanding Audit Log File	The Audit logging and syslog for the OS is active by default

i