

vMRF Hardening Guideline

Virtual Multimedia Resource System

User Guide

Copyright

© Ericsson AB 2016–2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document *Trademark Information*.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	System Overview	2
3	Hardening during vMRF Life Cycle	3
3.1	Hardening before Installation	3
3.2	Hardening during Installation	3
4	Product Security Maintenance	5





1 Introduction

This document describes the hardening procedure for vMRF. It also provides a list of the hardening activities that have been performed during product development.

1.1 Prerequisites

This section provides information on the documents, tools, and conditions that apply to the procedures in this document.

1.1.1 Tools

No tools are required.

1.1.2 Conditions

Before starting these procedures, ensure that the following conditions are met:

- The required infrastructure for installing and activating security is in place. For the details on security configuration and the site security infrastructure, see [vMRF Security Management](#) and [Security Management for ECLI, NETCONF, and SFTP Users](#).
- The O&M connection to the node is correctly configured.



2 System Overview

For an overview and details of the product and security issues, see the following documents:

- vMRF Security Management
- Security Management for ECLI, NETCONF, and SFTP Users



3 Hardening during vMRF Life Cycle

This section describes hardening during the product life cycle.

3.1 Hardening before Installation

vMRF provides the system pre-hardened so that unused services have been removed or disabled.

Ports likely to be attacked are not available at installation time. Standard ports defined for FTP (21) and Telnet (23) are not available in the system and secure versions of the protocols are used instead. For more information about the used protocols and ports, see [vMRF Security Management](#).

Application-sensitive data is stored in encrypted form in the database and access to sensitive data in system logs is restricted to appropriate users by rule-based access control.

vMRF allows the definition of administrators and accounts to manage their specific configuration attributes with roles and rules-based access control. This provides the hardening adapted to fulfill the operator access methods, administrator access rights, and definition of password security policy.

The logging function in the guest operating system of vMRF VMs is essential to monitor the security and general operation in the system. It is enabled, by default, to log the activities performed to detect and trace any fraudulent use. The logging function provides information related to both Operations, Administration, and Maintenance (OAM) operations executed in the system and traffic events in the system.

3.2 Hardening during Installation

The following hardening activities are performed during installation:

1. Software version control is done automatically by installing the latest SW maintenance package.

Note: Patching on site is not supported.

2. Automatic creation of emergency user. The default name (`misv-admin`) of the emergency user can be changed by editing the deployment template. For more information, see the relevant [deployment instruction](#).

Note: The emergency user is configured as a Linux local user, therefore, its name must use valid Linux user ID syntax.

The default password of the emergency user must be changed after creation. This can be done by replacing the password hash generated for the default



password in the deployment template with a password hash that is manually generated from the newly chosen password. For more information, see the relevant deployment instructions.

Avoid the use of a shared emergency user account.

3. The LDAP server address and the bind password are configured automatically to support remote authentication of other users. LDAP user hardening must be performed. The deployment template can be edited to match the LDAP server configuration and packed into the `tar.gz` file used for deployment. For more information, see the relevant deployment instructions.
4. The X.509 node credential is automatically installed on the vMRF. The deployment template can be edited to include the chosen node certificate and packed into the `tar.gz` file used for deployment. For more information, see the relevant deployment instructions.
5. The X.509 trusted certificate for the LDAP server is automatically installed on the vMRF. The deployment template can be edited to include the X.509 trusted certificate applicable for the used LDAP server and packed into the `tar.gz` file used for deployment. For more information, see the relevant deployment instructions.
6. During the recommended Simple Network Management Protocol (SNMP) configuration the following tasks must be performed:
 - a. To prevent modification of the management information base (MIB) files, it is recommended to set the `isMibWritable` attribute of the SNMP target MOs to `false` during target creation.
 - b. To grant access only to the ERICSSON-ALARM-MIB, that is needed for fault management purposes, the `readOids` attribute of the used SNMP View MO must be set to `1.3.6.1.4.1.193.183` during the creation process.

For more information, see the Initial Configuration Guide.



4 Product Security Maintenance

Security maintenance activities are to be performed regularly after installation.
For details, see [vMRF Security Management](#).