

vMRF Security Management

Virtual Multimedia Resource Function

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.



Contents

1	Introduction	1
2	Functions and Concepts	2
2.1	Traffic Separation	2
2.2	O&M Traffic Protection	2
2.3	O&M Administrator Access Control	2
2.4	Idle Session Time-out	6
2.5	Brute-Force Attack Protection	7
3	Services, Ports, and Protocols	8
4	Security Configuration	10
4.1	O&M Administrator Access Control	10
4.2	Recommended Periodic Operations	12
4.3	Handling of Patches	13
5	Privacy	14
5.1	Notice and Consent	14
5.2	Personal Data Classification	14





1 Introduction

This document describes the security functions implemented by the vMRF. The document also describes the security-related procedures that can be performed.



2 Functions and Concepts

This document covers the following security functions provided by vMRF:

- Traffic separation
- O&M Traffic Protection
- O&M Administrator Access Control

For a complete list of vMRF functions, including other security functions, refer to the [vMRF Overview](#).

2.1 Traffic Separation

The traffic for O&M, signaling, trusted payload, and untrusted payload uses separate vNICs. Virtual switch traffic separation is also a requirement in the cloud environment for vMRF. For more information on security requirements in the cloud environment for vMRF, refer to the [vMRF Infrastructure Requirements](#).

2.2 O&M Traffic Protection

The Northbound Interface (NBI) is assumed to be accessed from a trusted O&M network. O&M traffic is secured using various security protocols, see [Services, Ports, and Protocols](#) on page 8 for the details. Other protocols, for example, Telnet or FTP, are not permitted on the O&M interface.

It is recommended to configure a rate limit in an external firewall for protection of the NBI. For a description of the O&M traffic architecture, refer to [Security Management for ECLI, NETCONF, and SFTP Users](#).

2.3 O&M Administrator Access Control

vMRF uses Role-Based Access Control (RBAC) with different rules that can be granted to various role groups. vMRF uses an external Lightweight Directory Access Protocol (LDAP) server to provide user authentication. It is recommended to follow the operator's security policy when defining O&M users and assigning specific roles to them. It is recommended that access to sensitive information is restricted to those roles and operations personnel who need the access.

[Table 1](#) shows the default roles defined in vMRF:



Table 1 vMRF Roles

Role	Permission	MOM Fragment	Command and File Access
SystemAdministrator	R	ManagedElement, SystemFunctions, SecM (only the MO, but not the attributes) ManagedElement, SystemFunctions, SecM,CertM,*	Access to all vMRF CLI commands except for MSR
	RW	ManagedElement, SystemFunctions, SwInventory,*	
	RWX	ManagedElement ManagedElement, SystemFunctions ManagedElement, SystemFunctions, Fm,* ManagedElement, SystemFunctions, Pm,* ManagedElement, SystemFunctions, SwM,* ManagedElement, SystemFunctions, SysM,* ManagedElement, Transport	
SystemSecurityAdministrator	R	ManagedElement ManagedElement, SystemFunctions ManagedElement, SystemFunctions, Fm,* ManagedElement, SystemFunctions, SwInventory,*	Access to system logs and logs produced by the vMRF for troubleshooting purposes Access to all vMRF CLI commands for information printing
	RWX	ManagedElement, SystemFunctions, SecM*	



Role	Permission	MOM Fragment	Command and File Access
SystemTroubleshooter	-	-	<p>Access to commands of the underlying Ericsson Component Based Architecture (CBA) application</p> <p>Access to imm OpenSAF commands</p> <p>Access to system logs and logs produced by the vMRF for troubleshooting purposes</p> <p>Access to all vMRF CLI commands except for MSR</p>
MrfApplicationOperator	R	ManagedElement,*	<p>Access to all vMRF CLI commands for information printing</p> <p>Read access to PM files and alarm and event logs through SSH/SFTP</p>
	RX	ManagedElement, SystemFunctions, SysM,*	
MrfApplicationAdministrator	RWX	ManagedElement,*	<p>Access to all vMRF CLI commands for information printing</p> <p>Read and write access to PM files and alarm and event logs through SSH/SFTP</p>
	R	ManagedElement, SystemFunctions, SecM,*	
MrfApplicationSecurityAdministrator	R	ManagedElement,*	Access to all vMRF CLI commands for



Role	Permission	MOM Fragment	Command and File Access
	RWX	ManagedElement, SystemFunctions, SecM,*	information printing Read access to PM files and alarm and event logs through SSH/SFTP
MrfApplicationTroubleshooter	-	-	Access to all vMRF CLI commands except for MSR
MrfApplicationTroubleshooter	-	-	Access to MSR commands
MrfApplicationSftpUser	R	ManagedElement, SystemFunctions, FileM,*	Read access to PM files and alarm and event logs through SFTP port (115) only. Restricts all other access.

Users are given access to CLI commands based on their roles as shown in [Table 1](#). It is recommended that access to sensitive information is restricted to those roles and operations personnel who need the access. A user can be assigned multiple roles simultaneously. MrfApplicationSftpUser is a special role that restricts all other access and allows only SFTP access even when combined with other roles. Media Stream Recording (MSR) access must only be granted to Ericsson troubleshooters. For more information, refer to [Media Stream Recording](#).

2.3.1 Reserved POSIX Groups

[Table 2](#) lists POSIX groups, their corresponding Group Identifiers (GIDs), and their function in vMRF. Users are automatically given command access based on their role, as described in [O&M Administrator Access Control](#) on page 2. The following GID ranges are reserved and should not be assigned for LDAP users to avoid unintentional command access assignment: 0–1001, 2000–2008, and 7000–7999.

Table 2 Reserved vMRF POSIX Groups

Name	GID	Description
system-ts	2000	Troubleshooter; Access to commands of the underlying Ericsson Component Based Architecture (CBA) application



Name	GID	Description
mrf-op	2005	Normal operator; Access to all vMRF CLI commands for information printing
mrf-ts	2006	Troubleshooter; Access to all vMRF CLI commands except for MSR
mrf-msr	2008	Ericsson troubleshooter; Access to MSR commands
cmw-imm-users	2004	IMM troubleshooter; Access to imm OpenSAF commands
sftpushers ⁽¹⁾	2007	Restricted operator; Access to PM files and alarm and event logs through SFTP port (115) only
mrsv-admin	1001	Emergency user
systemd-journal	994	Access to logs produced by the vMRF for troubleshooting

(1) The sftpushers POSIX group restricts all other group rights. A member of the sftpushers POSIX group only has SFTP access rights and cannot be a member of any other POSIX group.

The *emergency user* is a user that can log on to the system controller using SSH through the NBI, even when the LDAP server is unavailable. The *emergency user* is defined during deployment and cannot be changed during operation. The emergency user has access to all MOs and can therefore log on to the system to restore LDAP connectivity and return the system to normal operation.

Note: The emergency user must be only used for emergency recovery purposes and not as a shared account for normal O&M operations.

SSH login for the `root` user is not permitted for normal users. The `root` user is locked, so that normal users cannot change to `root` with the `su root` command. The emergency user can change to `root` with the `sudo -i` command.

Logging in through the serial port is not permitted.

SSH host keys (RSA, DSA, ECDSA) for the VMs of the VNF cluster are generated automatically by the first VM during the deployment process, and copied to all other VMs. The fingerprints of the SSH host keys are visible in the console tool after deployment.

2.4 Idle Session Time-out

An SSH session is an interval that starts when a user is authenticated and can start operations. It ends when the user exits, or when the connection to the VNF is closed because of user inactivity. If the session ends because of inactivity, the situation is called idle session time-out.



Idle session time-out is a fixed time of 30 minutes and is enforced for all CLI command, NETCONF, and file access sessions. Traffic is monitored only in the client-to-server direction.

2.5 Brute-Force Attack Protection

The vMRF SSH interface uses a mechanism to protect against password cracking with brute-force attacks. The mechanism temporarily bans login attempts from IP addresses that reach the maximum allowed number of failed login attempts. The ban period and the maximum allowed number of failed login attempts are preconfigured in vMRF.

The ban period is set to 10 minutes, and the maximum allowed number of failed login attempts is five. This means that after five unsuccessful login attempts, no more login attempts are allowed from the given IP address for 10 minutes.



3 Services, Ports, and Protocols

The services, ports, and protocols that are used by vMRF are listed in [Table 3](#).

Table 3 Services, Ports, and Protocols on the O&M Interface

Service or Interface Name	Protocol	IP Address Type	Port	Transport Protocol	IP Version
CLI access	SSH	O&M IP	22	TCP	IPv4
PM report file access	SFTP	O&M IP	115	TCP	IPv4
Alarm and alert log file access					
LDAP	TLS	O&M IP	389	TCP	IPv4
	LDAPS	O&M IP	636	TCP	IPv4
NeLS	TLS	LM	9095	TCP	IPv4 or IPv6
NETCONF	SSH	O&M IP	830	TCP	IPv4
	TLS	O&M IP	6513	TCP	IPv4
SNMP	SNMP	O&M IP	161 (configurable)	UDP	IPv4
	SNMP over DTLS	O&M IP	10161 (configurable)	UDP	IPv4
Synchronization	NTP	O&M IP	123	UDP	IPv4

Table 4 Services, Ports, and Protocols on the Control Plane Interface

Service or Interface Name	Protocol	IP Address Type	Port	Transport Protocol	IP Version
Ia, Ix, or Iq	H.248	Signaling IP	2944 (configurable)	SCTP	IPv4



Table 5 Services, Ports, and Protocols on the User Plane Interfaces

Service or Interface Name	Protocol	IP Address Type	Port	Transport Protocol	IP Version
Trusted network (IMS Core)	RTP, RTCP	Traffic IP	1024–65535	UDP	IPv4 or IPv6
Untrusted network	RTP, RTCP	Traffic IP	1024–65535	UDP	IPv4 or IPv6



4 Security Configuration

This section describes how to configure the security functions in vMRF.

4.1 O&M Administrator Access Control

This section provides the instructions for operating the security functionality of the product.

4.1.1 Configure LDAP Authentication and Authorization in vMRF

This procedure describes how to configure vMRF to use an LDAP server for authentication and authorization.

Prerequisites

- vMRF has been deployed.
- LDAP authentication and authorization has not yet been configured in the vMRF VNF, or the configuration needs to be changed. For instructions on how to import the LDAP configuration below into the VNF during deployment, refer to the relevant [deployment guide](#).
- An LDAP server is available for vMRF and its IP address and port are known.
- The LDAP server has TLS enabled and one issuer certificate of its node credentials has been installed as trusted certificate.
- You have logged in to vMRF either as the emergency user, or as the security administrator.
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.

Steps

1. Install vMRF node credentials using offline enrollment, as described in [Install or Renew Node Credential by PKCS 12](#).
2. Install trusted certificates for the CA and the LDAP server, as described in [Install Trusted Certificate](#).
3. Create a trust category for the LDAP server certificate, as described in [Create Trust Category](#).



4. In the MOM, navigate to the Ldap MO and configure it:

```
>ManagedElement=1,SystemFunctions=1,SecM=1,UserManagement=1,LdapAuthenticationMethod=1,Ldap=1
```

```
(Ldap=1)>configure
```

```
(config-Ldap=1)>baseDn="dc=example,dc=org"
```

```
(config-Ldap=1)>bindDn="cn=admin,dc=example,dc=org"
```

Note: Replace the values with the actual DNs.

```
(config-Ldap=1)>ldapIpAddress="<IP address of the LDAP server>"
```

```
(config-Ldap=1)>serverPort=<Port of the LDAP server>
```

Note: Available LDAP server ports are the following:

- 389, if attribute useTls is false.
- 389, if attribute useTls is true and tlsMode is STARTTLS.
- 636, if attribute useTls is true and tlsMode is LDAPS.

```
(config-Ldap=1)>nodeCredential="ManagedElement=1,SystemFunctions=1,SecM=1,CertM=1,NodeCredential=1"
```

```
(config-Ldap=1)>trustCategory="ManagedElement=1,SystemFunctions=1,SecM=1,CertM=1,TrustCategory="<Trust category created for the LDAP server certificate>"
```

```
(config-Ldap=1)>useTls=true
```

```
(config-Ldap=1)>profileFilter=ERICSSON_FILTER
```

Note: The profileFilter attribute configuration is needed for RBAC.

```
(config-Ldap=1)>EricssonFilter=1
```

```
(config-EricssonFilter=1)>roleAliasesBaseDn="dc=example,dc=com"
```

```
(config-EricssonFilter=1)>up
```

```
(config-Ldap=1)>up
```

```
(config-LdapAuthenticationMethod=1)>administrativeState=UNLOCKED
```

```
(config-LdapAuthenticationMethod=1)>commit
```



5. Activate the local authorization method in the VNF to prevent all LDAP users from having full access to configuration data:

```
(config-LdapAuthenticationMethod=1)>LocalAuthorizationMethod=1
```

```
(config-  
LocalAuthorizationMethod=1)>administrativeState=UNLOCKED
```

```
(config-LocalAuthorizationMethod=1)>commit
```

For more information, refer to Operating Instructions [Unlock Local Authorization Method](#).

6. Add the Ericsson schema to the LDAP server, and extend the LDAP server user accounts to use role based access control (RBAC).
 - Define the directory entry representing the users Posix account for each user.
 - Define the role of the user by setting the `ericssonUserAuthorizationScope` attribute of the Posix account. The value of the authorization scope must have the format `<target_type>:<role>`, for example, **`ericssonUserAuthorizationScope:MrfApplicationOperator`**.
 - To access logs produced by vMRF, give the `SystemSecurityAdministrator` or `SystemTroubleshooter` role to the user.
 - To have users with access rights only to PM files, alarm and event logs via SFTP, define users with `MrfApplicationSftpUser` role.

For more information on LDAP server user accounts, refer to [LDAP-Based Authentication and Authorization Interface](#).

4.2 Recommended Periodic Operations

Even though vMRF has been installed and hardened securely, administrator and user activity over time can introduce security exposures. Also, new vulnerabilities which need to be mitigated are frequently found in the existing products. Therefore it is necessary to maintain the security posture of the product in service on a regular, ongoing basis.

This section describes recommended periodic operations.

- Take system backups regularly according to the [vMRF Backup and Restore Guideline](#).
- Restrict access to backup files so that unauthorized persons cannot view or modify the included sensitive data. This recommendation also refers to backups stored in an external server.



- Apply password policies on the LDAP server to enforce password complexity, aging, and recovery.
- Ensure that no unnecessary accounts exist.
- Ensure that no unnecessary listening ports are open.
- Ensure that no shared user accounts are used.
- Ensure that the *emergency user* password is not known by more people than necessary.
- Ensure that user rights are assigned only to real needs.
- Monitor the log of access and authorization events in the system by using the following commands:
 - `journalctl _COMM=sshd` – sshd access logs
 - `journalctl SYSLOG_FACILITY=10` – authentication logs
 - `journalctl _COMM=com` – NBI audit logs

4.3 Handling of Patches

Patches are delivered as new vMRF SW packages. A new SW package is deployed as a new vMRF VNF, and if needed, the old VNF can be deleted.



5 Privacy

vMRF includes features for troubleshooting and media plane problem solving that have privacy impacts. These features can be used by both Ericsson and operator trusted personnel.

To be able to provide services in the network, vMRF handles sensitive personal data. To restrict access to personal data, vMRF uses RBAC for roles and operations personnel who need access to such information. It is the responsibility of operators to use these security controls appropriately to protect personal data and mitigate any possible privacy impact. For more information on RBAC roles see [O&M Administrator Access Control](#) on page 2.

5.1 Notice and Consent

To ensure that personal information is collected and processed in a fair and lawful manner, operators have the following responsibilities regarding personal information privacy:

- Locally applicable privacy statements must be made available to users whose data is being collected.
- Locally applicable user consent must be in place for processing personal information.

Furthermore, it is assumed that all personal privacy related information is handled by the operator according to all applicable local and international laws and regulations in the countries in which they operate.

5.2 Personal Data Classification

The following table lists the collected data item types by Personal Data Category:

Table 6 Collected Data Item Types

Personal Data Category	Data Item
Basic data	<p>IP address. IP addresses of media plane packets are considered as Personally Identifiable Information (PII) and may be included in log files.</p> <p>To provide services, vMRF processes the IP addresses in RTP and IP packets sent from or received by the UE. These IP addresses are not stored by vMRF, except possibly in troubleshooting logs.</p>



Personal Data Category	Data Item
	In most deployments, the IP addresses visible for vMRF are not UE IP addresses, but internal IP addresses of the operator's border gateway (vBGF), or media gateway (IM-MGW) instances used for connecting the UE to the IMS core network.
Sensitive data (identifiable user activity)	Content of media plane traffic when Media Stream Recording (MSR) is active: voice, text, sound, pictures, or other content of the communication. MSR is used for troubleshooting only by Ericsson personnel only, and only after the operator has explicitly requested Ericsson to analyze the problem and has agreed with Ericsson on the use of MSR. The produced recording files are sent to Ericsson vMRF support for analysis. For more information on MSR, refer to Media Stream Recording .