

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

## **vMTAS Network Impact Report from native MTAS 4.15.0 to vMTAS 1.15.0**

### **Multimedia Telephony Application Server**

#### **Copyright**

© Ericsson AB 2016. 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.

#### **Trademarks**

Ericsson is the trademark or registered trademark of Telefonaktiebolaget LM Ericsson. All other product or service names mentioned in this document are trademarks of their respective companies.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

## Content

<b>1</b>	<b>Introduction .....</b>	<b>3</b>
1.1	Revision History (will be removed in final version).....	5
1.2	Prerequisites .....	5
1.3	Assumptions.....	6
<b>2</b>	<b>General Impact .....</b>	<b>6</b>
2.1	Backward Compatibility.....	6
2.2	Capacity and Performance .....	7
2.3	Hardware and Platform .....	7
2.4	Virtual Infrastructure.....	8
2.5	Components.....	8
2.6	License Handling .....	8
2.7	Upgrade Impact.....	8
2.8	Operation.....	9
2.9	Obsolete Features .....	17
2.10	Other Network Elements.....	17
2.11	Other Impacts.....	17
<b>3</b>	<b>Interfaces.....</b>	<b>17</b>
3.1	Inter-Node Interface .....	17
3.2	Man-Machine Interfaces .....	19
3.3	Operation and Maintenance .....	20
<b>4</b>	<b>Summary of Impacts per Feature.....</b>	<b>23</b>
<b>5</b>	<b>Impact on MTAS Functions.....</b>	<b>28</b>
5.1	Operation and Maintenance (virtualized) .....	28
5.2	VNF Deployment.....	29
5.3	VNF Robustness.....	30
5.4	VNF Scaling .....	31
5.5	Rebalancing by Moving Users between MTAS Instances .....	32
5.6	Auto Healing Work Flow Feature .....	33
5.7	etc Hardened Overlay .....	34
5.8	SCTP Support for DIAMETER.....	35
5.9	Hardened Etc Overlay Introduction .....	36
5.10	Unique Prompt Prefix.....	37
5.11	VMWare Instantiation and Termination Workflow .....	38
5.12	New PM Job Names .....	39
5.13	Scaling Workflows for VMware .....	39
5.14	Configurable MTU size .....	39
5.15	vMTAS NFVO-Triggered Instantiate/Terminate Workflows for OpenStack NFVI .....	40
5.16	On-site Generation of VNF Package .....	40
5.17	vMTAS, Faster and easier handling of subscriber and software trace .....	41
<b>6</b>	<b>References.....</b>	<b>41</b>

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

## 1 Introduction

This document, the Network Impact Report (NIR), describes how the release of vMTAS 1.15.0 with new and changed features compares to the previous release of native MTAS 4.15.0 and how it affects the operator's overall network, including all affected products and functions.

In this document, the term "vMTAS" refers to the product and the term "MTAS" refers to the MTAS application, independent of being deployed in a native or virtual environment.

The purpose of this document is to provide information to plan migration from native MTAS to vMTAS in the operator network.

vMTAS is a Virtual Network Function (VNF) deployed as software only on any platform fulfilling hardware and infrastructure specified in Virtual MTAS Infrastructure Requirement, [8]. Also, vMTAS is adapted to a Component Based Architecture (a new SW architecture) in which most of the middleware functions such as Software Management, File Management and Operation and Maintenance functions (CM, PM, FM, O&M Security Management) are changed compared to the native MTAS 4.15.0 release.

In short, it is primarily a platform change rather than new functionality introduction between releases.

This document describes how operation is changed in the vMTAS 1.15.0 compared to the MTAS 4.15.0 release on a high level. Since it is not possible to do a direct upgrade from native MTAS to vMTAS, this document is not intended to list every detailed configuration change, as such information is not always applicable for a product with a platform change. Most application related parameters are the same and can be mapped directly from native to virtual, while some parameters are platform specific so reusing native settings does not result in an optimal behavior in a virtual environment.

For vMTAS, the Ericsson Software Model with Base Packages and Value Packages is supported.

vMTAS contains the following Base Packages:

- Business Line AS Base (FAJ 801 0931)
- Business Mobility AS Base (FAJ 801 0287)
- Communication Interworking Function NW AS (FAJ 801 0820)
- MMTel AS Voice Base (FAJ 801 0277)
- Service Continuity AS Base (FAJ 801 0290)
- SIP Trunking AS Base (FAJ 801 0289)

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

vMTAS contains the following Value Packages:

- BL Legacy IN Reuse (FAJ 801 0935)
- BL Location Services Support (FAJ 801 0934)
- BL Multimedia (FAJ 801 0932)
- BL Service Exposure (FAJ 801 0933)
- BL UC/PBX Rerouting (FAJ 801 0930)
- BL WiFi Calling (FAJ 801 0936)
- Communication State Exposure (FAJ 801 0821)
- Lawful Intercept (FAJ 801 0284)
- Legacy IN Reuse (FAJ 801 0281)
- Location Services Support (FAJ 801 0283)
- Multi Device (FAJ 801 0278)
- Multi Persona (FAJ 801 0964)
- Multi SIM (FAJ 801 0782)
- Multimedia (FAJ 801 0280)
- Service Exposure (FAJ 801 0282)
- SRVCC (FAJ 801 0286)
- VoLTE Roaming (FAJ 801 0982)
- WiFi Calling (FAJ 801 0285)
- WiFi Calling MMTel (FAJ 801 0673)

The packages above consist of many functions (the legacy software model), where some exist in several packages. This document is structured around all functionality within the packages, where the mapping towards Base/Value Packages is described in section 4.

This NIR covers the following new functions:

- Operation and Management (virtualized), covers several functions from native; Configuration Management, Performance Management, Fault Management, Traceability and Troubleshooting
- VNF Deployment, covers deployment and software installation
- VNF Network connectivity
- VNF Scaling, covers expansion and contraction of the vMTAS cluster
- Rebalancing by Moving Users between MTAS Instances
- Auto Healing Work Flow Feature
- etc Hardened Overlay
- SCTP Support for DIAMETER
- Hardened Etc Overlay Introduction
- Unique Prompt Prefix

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

- VMWare Instantiation and Termination Workflow
- PM Measurements for maximum CPU Load and Memory utilization
- vMTAS, Scaling Workflows for VMware
- Configurable MTU size
- vMTAS Workflow package supports NFVO triggered Instantiate/Terminate Workflows for OpenStack NFVI
- Script for on-site generation of vMTAS VNF Package
- Tool for faster and easier handling of subscriber and software trace

This NIR covers the following obsolete functions:

- Scheduled Conference

## 1.1 Revision History (will be removed in final version)

Rev	Date	Prepared by	Comment
A	2019-06-17	EHITERA	Final version

## 1.2 P rerequisites

This section states the prerequisites for this document.

### 1.2.1 Documents

Ensure that the following information or documents are available:

- MTAS Technical Description Common Features, see [2]
- vMTAS Technical Description Common Features, see [3]

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

### 1.3 Assumptions

When migrating from native MTAS to vMTAS it is assumed that network redundancy is introduced when possible if not already used, which is at least two vMTAS VNFs or more deployed in the network after the migration.

It is also assumed that the vMTAS VNFs will co-exist with native MTAS nodes in a hybrid network for a certain time, but that the goal is to migrate all native MTAS nodes to vMTAS VNFs as soon as possible.

## 2 General Impact

### 2.1 Backward Compatibility

vMTAS is not backward compatible with native MTAS, see table below.

Reason	Description
<b>Hardware features in vMTAS</b>	
vMTAS is neither possible to run on NSP, nor on BSP using GEP3.	There is no specific hardware resource that vMTAS depends on, but general requirements on hardware are specified in Section 2.3. This implies NSP HW from a native node is not sufficient.
<b>Operation and Maintenance (virtualized)</b>	
LDAP and the Node Management Toolbox are not supported for normal Configuration Management.	See Section 2.8.1, Configuration Management.
Modified Performance Management support.	See Section 2.8.2, Performance Management.
Modified Fault Management support.	See Section 2.8.3, Fault Management.
Traceability and Troubleshooting is adapted towards the new software architecture.	The same function level exists, but adapted towards the new software architecture, for more information see vMTAS Troubleshooting Guideline, [4].

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

Health check functionality.	Automatic health check functionality and automatic counter check functionality exist also in vMTAS, but is redesigned due to the new software architecture, The additional health check utilities that is described in the native MTAS Health Check Operating Instructions are not supported in vMTAS. For more information see vMTAS Health Check, [5].
Data Collection.	Functionality for Data Collection exist also in vMTAS but is redesigned due to the new software architecture. For more information see Data Collection Guideline for vMTAS, [38].
<b>Conference AS</b>	
The Conference AS features are not maintained and cannot be used.	Conference AS has been restricted and is only supported in native MTAS. When migrating from native to virtual MTAS, the option to configure Scheduled Conference does not exist.

Table 1 Product Not Backward Compatible Reasons

## 2.2 Capacity and Performance

Since the vMTAS product changes the deployment configurations and works as a VNF, it is not relevant to compare neither the subscriber capacity nor the network performance against native MTAS.

The subscriber/session capacity and the provisioning capacity for the vMTAS 1.15.0 product measured on certified hardware is described in vMTAS 1.15.0 Characteristics Specification and Dimensioning Guidelines, [6].

## 2.3 Hardware and Platform

vMTAS is a software only delivery, it can be deployed on CEE/BSP8100 or on any HW platform using OpenStack.

For more information about CEE and BSP, see references [32] and [33].

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

The settings related to the hardware and infrastructure used by the native MTAS 4.15.0 cannot be directly mapped to vMTAS 1.15.0. The hardware and infrastructure configuration are based on the vMTAS SW installation, [7].

## 2.4 Virtual Infrastructure

The required infrastructure for vMTAS, such as compute, network and security requirements are specified in the Virtual MTAS Infrastructure Requirements, [8].

## 2.5 Components

License agreements for third party products used by vMTAS are listed in [21].

## 2.6 License Handling

License keys for the whole network must be deployed with installation of a single License Key File in NeLS.

For more information refer to MTAS Licenses, [39].

## 2.7 Upgrade Impact

Upgrade from native MTAS to vMTAS is not possible. vMTAS 1.15.0 is deployed as a new installation. For information about how to install vMTAS, refer to vMTAS SW Installation, [7].

Migration from native MTAS to vMTAS can either be done as an expansion of the network resulting in a hybrid network with co-existence of both native MTAS nodes and vMTAS VNFs, or a native MTAS node can be replaced by a vMTAS VNF when network redundancy already exists in the network.

When a vMTAS VNF have been deployed in the network, it is possible to gradually move traffic from a native MTAS node to the vMTAS VNF, and at some point, in time later the native MTAS can be gracefully shut down and de-commissioned.

Differences in functionality between native MTAS and vMTAS as described in this NIR must be considered in a hybrid network.

Much of the configuration data from native MTAS can be mapped to vMTAS so that similar functionality is available in both network functions, see [20].



Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

A general recommendation is to keep a network with at least two vMTAS VNFs after the migration, this makes it possible to perform future software upgrades of vMTAS VNFs with a minimum network impact.

## 2.8 Operation

### 2.8.1 Configuration Management

The vMTAS configuration data is presented as a set of Management Objects (MOs). Their relationships are described in a Managed Object Model (MOM) corresponding to the IMS Managed Information Model (MIM) in the native MTAS. However, the structure of the vMTAS MOM is changed to align to the Ericsson Common Information Model (ECIM) MOM. For the vMTAS MOM structure see, [9].

The protocol used to manage the configuration data has changed from LDAP to NETCONF. In addition, Ericsson Command Line Interface (ECLI) can be used to manage the vMTAS. For more information regarding the Ericsson NETCONF interface and the Ericsson Command-Line Interface (ECLI), see [10] and [11].

Certain parts of the vMTAS configuration data needs to be managed using a Provisioning LDAP interface. For more information regarding the Provisioning LDAP interface see, [16]. For more information regarding what configuration data that should be managed using the Provisioning LDAP interface see, [17].

A Node Management Toolbox, including CM browser and TelORB manager as provided in the native MTAS is not provided in vMTAS. For configuration management purposes ECLI or for example the Ericsson NETCONF Browser (ENB), see [31], which is a model driven tool supporting NETCONF can be used.

There are multiple User Guides, Managed Area Descriptions and Operating Instructions available in the customer product information library to facilitate the configuration procedures and options in vMTAS.

### 2.8.2 Performance Management

vMTAS provides similar Performance Management (PM) functionality as in native MTAS. Major differences are:

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

- The PM jobs and PM report files are configurable by means of PmJob definitions. The default report files per PM counter group in native MTAS is replaced by a common report file per granularity period in vMTAS. The PmJobs related to the vMTAS application corresponds to the functional PM groups in the native MTAS PM CPI. The PmJobs related to the platform is not mapped between native MTAS and vMTAS.
- Shortest measurement granularity period (GP) for PM report files has been reduced from five minutes to one minute.
- PM report file format
  - Native MTAS can generate files in 3 formats as described in [26]:  
XSD File Format (3GPP TS 32.435 V6.0, measCollec.xsd),  
nPMF DTD File Format (3GPP TS 32.401 v5.0, MeasDataCollection.dtd version 2.0) that is used in the default configuration (tspPmMjReportingFormat: DTD),  
oPMF DTD File Format (3GPP TS 32.401 v3.2, MeasDataCollection.dtd version 1.1) that is converted from nPMF DTD files if conversion script is enabled and that is disabled in the default TSP and MTAS configuration and can be enabled by the operator.  
The 2 DTD format are backwards compatible in terms of XML elements but require different parser logic due to different XML structure and content.
  - vMTAS generates files in XSD File Format (3GPP TS 32.435 V10.0) that is described in [27].
- PM report file location
  - Native MTAS writes PM files in a PM root folder and in several PM subfolders under the PM root folder.
  - vMTAS writes all PM files in a single PM root folder.
- PM report file naming
  - Both native MTAS and vMTAS is partially compliant to the 3GPP standard type A file naming with some differences. Examples for difference are handling of PM job name (only in native) and unique Id (only in vMTAS).
- PM report file content
  - MTAS PM function provides the same measurements in native and virtual MTAS however different measurements are provided for Operating System resources and signaling. PM counters for SS7/SCTP that exist in native MTAS are also available in vMTAS 1.15.0 with some exceptions related to SCTP.
    - SCTP Unordered Chunks Sent to the Remote Side
    - SCTP Unordered Chunks Received from the Remote Side

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

- SCTP Fragmented User Messages Sent
  - SCTP Received Fragmented User Messages
  - SCTP Sent a Congestion Ceasing Indication to User
  - SCTP User Data Transmit Buffer is Full
  - SCTP Heartbeat Timeouts
  - SCTP Connection Restarted
  - SCTP Control Chunks Received
  - SCTP Control Chunks Sent
  - SCTP Packages Received
  - SCTP Packages Sent
  - SCTP Received Chunks Dropped
  - SCTP Sent Chunks Dropped
- PM report file transfer
  - Native MTAS supports both pull and push style PM report file transfers, while vMTAS supports pull style, only.
- PM report file notifications
  - Native MTAS sends PM file preparation notifications (file ready or faulty) as SNMP traps according to ERICSSON-TSP-EVENTS-MIB [30]. File ready notification is also sent in standard 3GPP CORBA PM notifications.
  - vMTAS does not send PM file preparation notifications.
- PM Threshold Alarms
  - Native MTAS sends threshold alarms as standard 3GPP CORBA PM notifications and as SNMP traps according to ERICSSON-ALARM-IRP-MIB [28].
  - vMTAS sends threshold alarms as SNMP traps according to ERICSSON-ALARM-MIB [29].
- PM counters shown in CLI
  - Native MTAS shows real-time values of PM measurements in CLI, NETCONF and LDAP in tspPmSnapshotProvider object.
  - vMTAS will support showing real-time values of PM measurements in CLI by show-counter command in a very near time release.
  - In both native MTAS and vMTAS it's possible to show application related counters in CLI by MtasCounterCheck command.
- PM function overload protection and load regulation is supported in native MTAS, only.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

- PM function is configurable in OaM NBI in both MTAS cases, however the configuration models have different structure and provide different level of configurability.
- All PM Counters related to the native platform and hardware is removed/replaced.

For more information regarding performance management in vMTAS, see [34].

### 2.8.3 Fault Management

vMTAS provides similar Fault Management (FM) functionality as the native MTAS. Major differences are:

- The NBI for providing alarms offers the SNMPv1 besides the SNMPv2 and SNMPv3. The SNMPv3 is also possible to run over Datagram Transport Layer Security (DTLS). It is possible to configure multiple alarm receivers. The CORBA IRP is not supported.
- A heartbeat mechanism over SNMP between the managed element and external management system exists to avoid leaving the managed element unattended.
- The alarm reporting is done using ERICSSON-ALARM-MIB instead of the ERICSSON-ALARM-IRP-MIB.
- Active alarms are visible in MOM via ECLI or NETCONF, and no longer via the NM Toolbox (Alarm Viewer), or TSP CLI.  
For more information see the O&M/Fault Management section in the MTAS Demo Description, [12].
- Alarms related to specific VMs can be configured to include a universally unique identifier (UUID) as additional information to identify which VM the alarm is related to.
- The vMTAS alarms are available in the view “Instances” of the MTAS MOM, see [9], and there is still one Operating Instructions for each alarm in the CPI.
- All alarms related to the native platform and hardware is removed/replaced. See [35] for the complete list of alarms.

### 2.8.4 Software Management

#### 2.8.4.1 Installation

Deployment of a vMTAS VNF comes with completely new mechanisms compared to the native MTAS deployment:

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

- Dedicated vMTAS images are prepared for deployment in OpenStack based virtual infrastructures.
- The image loading, instantiation and initial configuration is to be performed through the related Cloud Management System.
- vMTAS is initial deployed with a minimal redundant cluster setup. That is, 2 controller node and 2 payload nodes. A scale-out operation (see chapter 5) should follow the initial deployment to reach the aimed vMTAS cluster size.

For more information on vMTAS deployment in OpenStack based virtual infrastructure, see [7].

#### 2.8.4.2 Upgrade

The vMTAS upgrade principles are similar to the upgrade principles of a native MTAS. That is, an upgrade package is to be applied on the target system to bring vMTAS from a certain SW version to the wanted target SW version (this also means, the vMTAS upgrade - in contrast with the initial deployment - is not image based). The vMTAS upgrade package format, the operation flow used to apply it, the interfaces and tools used to operate with are different compared to what was used in native MTAS context:

- New upgrade package format is introduced (called CSP package). The package format is new therefore, not compatible with the native MTAS upgrade package format.
- The package is to be applied on the target system by operating on the SW Management fragment related objects published through the NETCONF/ECLI NBI.
- The MTAS/TSP Upgrade Automation Tool cannot be used to apply a vMTAS upgrade package.
- The upgrade commit and eventual rollback is not automatic as it was in case of native MTAS. For vMTAS the commit of an applied upgrade package needs dedicated operation over related managed object through NETCONF/ECLI. This is in order to let operator validate by provided health-check operations whether the upgrade was successful or not. If the upgrade is considered successful it is to be committed. In contrast rollback or fallback can be initiated.
- The vMTAS upgrade package and used procedure is agnostic of the used virtual infrastructure. That is, same package is to be applied using same flow on both OpenStack and VMware based virtual infrastructures.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

- Similar to native MTAS two different upgrade procedures are supported, one for in-service upgrade and one for network redundant upgrade. For native MTAS different upgrade packages are used for the different upgrade procedures, where for vMTAS the same upgrade package is used and instead the procedure to be used is specified as part of the preparation phase.

For more information on vMTAS upgrade, see [14] and [15].

#### 2.8.4.3 Software Inventory

The verification of actual vMTAS version and composing component/module SW versions on the target system can be performed through the SW inventory fragment of the NBI by using NETCONF/ECLI. The SW information representation format differs to the one seen for native MTAS deployment.

#### 2.8.4.4 Backup and Restore

Backup and restore functionality is changed in the following way:

- Legacy backup and restore functionality is obsolete
- Manual backup of configuration data, node credentials and trusted certificates is done by executing a script and exporting the (compressed) configuration file out from the VNF.

For more information of backup and restore, see [36].

### 2.8.5 License Management

The Network License Server (NeLS) must be configured into the LM information model fragment, see [9].

For more information refer to MTAS Licenses, [39].

### 2.8.6 Security Management

Security Management for O&M is different, and the most important differences are:

- To control NBI user access to the MOM the vMTAS uses Role-Based Access Control (RBAC) with different rules that can be granted to different roles. The authorization rules for each role are locally pre-defined in the vMTAS.
- The vMTAS has predefined “emergency user” that has full access to the system without LDAP authentication.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

- Logging of security related events to an external Syslog server is not available in vMTAS.

For details of vMTAS security solution see [37].

### 2.8.7 Network Connectivity

The VIP concept in TSP middleware has now been replaced by the eVIP concept that comes with CBA middleware in the VNF.

The eVIP is used to connect to external networks. A VIP address is used to address distributed functions in the VNF and it also provides a load balancing function. Two eVIP gateway routers, implemented in the Cloud Edge switches, are connected to the eVIP based VNF to achieve redundancy.

In order to send ICMP messages, use routable IP-addresses on links as well.

The vMTAS uses multiple ALB FEEs distributed over the corresponding VMs to connect to the Cloud Edge switches. Therefore, the Cloud Edge switch may have multiple routes with different next hops to a VIP address used as service address. The Cloud Edge switch should use ECMP to distribute service traffic between the FEEs.

OSPF dynamic routing or static routing can be used between the FEEs and the Cloud Edge switch:

- Static routing with BFD (recommended and described below)
- OSPFv2/OSPFv3 with BFD (not further described in NIR)
- OSPFv2/OSPFv3 with short OSPF timers (not further described in NIR)

The choice between the different routing alternatives is mainly influenced by the protocols supported in the Cloud Edge switch and the scaling capabilities.

The same network setup should be used in the cloud for both routing scenarios to promote simplification and ease the migration between static and dynamic routing configurations.

#### Static routing with BFD

Figure 1 shows an eVIP based VNF connected to the Cloud Edge switches with static routing and BFD. A single FEE is used per VM to connect to one IMS VPN in the Cloud Edge switches. A single virtual network is used in the cloud infrastructure to connect the FEEs to the Cloud Edge switches.

With static routing, BFD is required to detect a connection failure.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

Scaling the number of FEEs per ALB may require manual configuration. For example, if the number of VMs with a FEEs is increased, each Cloud Edge switch is configured with additional static routes and Equal-Cost Multipath (ECMP) is used to load balance downlink traffic, see Figure 1.

The scale-out/scale-in of eVIP is controlled by an eVIP.xml file. Secure that the FEEs are distributed over both switches (next hop) in scale-out/scale-in scenarios.

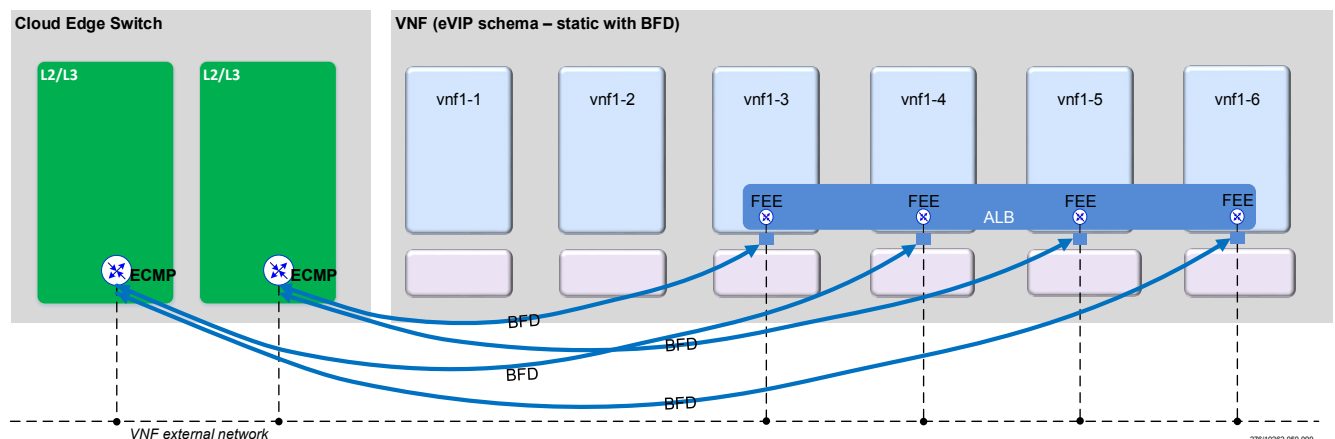


Figure 1 eVIP with Static, Single Default Route in FEE, four FEEs in ALB

It must be considered if the same logical networks configured in MTAS are to be maintained also for the vMTAS, or if the recommended logical networks indicated by the vMTAS Internal and External Connectivity Overview should be configured, see [13].

It shall be noted that vMTAS may operate in a cloud solution, and if frequent scaling operations (to add and remove VMs) takes place, it shall be considered to use static routing instead of OSPF which is the typical method in native MTAS.

The vMTAS eVIP Front-End implementation reassembles fragmented IP packets before passing it on to MTAS application logic. As the eVIP Front-End runs on multiple VM instances, it is required that all IP fragments are received by the same VM instance. This means that to avoid that IP fragments ends up in different VMs, flow-based Equal-Cost Multipath (ECMP) is required. ECMP in this context means that all IP packets within the same IP flow are received by the same vMTAS VM instance. If ECMP is not supported, the network must fallback from using UDP to TCP if the SIP message size is above 1300 bytes (this is also indicated in RFC 3261). See [13] for further details.



Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

### 2.8.8 Provisioning

There are no major differences in provisioning between native MTAS and vMTAS.

If a security certificate has been created for provisioning it can be reused if the same logical networks configured in native MTAS are to be maintained also for the vMTAS. The security certificate can then be exported from the native MTAS and imported in vMTAS.

### 2.9 Obsolete Features

Conference AS is not applicable for vMTAS, the option to configure Scheduled Conference does not exist.

### 2.10 Other Network Elements

The interface for operation and maintenance, the Northbound Interface (NBI), towards Operations Support System for Radio and Core (OSS-RC), or any non-Ericsson network or node management system is changed from LDAP and IMS Management Information Model (MIM) to a NETCONF/ECLI and ECIM Management Object Model (MOM).

### 2.11 Other Impacts

-

## 3 Interfaces

This section describes interface changes between the existing and new revisions of the product.

### 3.1 Inter-Node Interface

The changes to the inter-node interfaces are listed in table below.

The description of impact is as follows:

- **No Impact** means that the new version can be installed without affecting other nodes.
- **Minor Impact** means that there are changes, but with additional configuration the previous behavior can be kept.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

- **Major Impact** implies that the change has made an interface backward incompatible.
- **New Interface** indicates that the interface did not exist in previous revision.
- **Obsolete** means that the interface no longer exists.

Interface	Protocol	Impact	Description of changes compared to MTAS 4.15.0
E4	Thrift	New	<p>This is an Ericsson proprietary interface used by the vMTAS license management client and the NeLS node.</p> <p>Thrift is a framework to create interoperable, high-performance, and scalable services that can be called from multiple languages.</p> <p>Thrift allows to choose independently between protocol, transport and server threading model.</p> <p>Network License service traffic is secured using Thrift/TLS.</p>
O&M-CM	NETCO NF over SSH/TLS	New	<p>This is the Northbound O&amp;M interface for configuration management. In SSH case user passwords or keys must be managed. In TLS case, certificates must be deployed to secure the interface. In both cases users with proper authorization must be defined.</p>
O&M-CM	Provisioning LDAP	New	<p>This is the Northbound O&amp;M interface for configuration management of certain data.</p>
O&M-FM	SNMP v1	New	<p>This is the Northbound O&amp;M interface for fault management. SNMPv3 can use DTLS</p>

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

			or TLS, while SNMP v1 and v2 can use TLS. SNMP targets must be defined with v3 USM authentication model or TSM with DTLS. In USM case pre-shared keys, whereas in TSM case certificates are needed. SNMP views must be defined for proper authorization of targets.
O&M-FM	CORBA	Obsolete	The CORBA IRP for FM is not supported.
SEC	TLS	New	Certificates (e.g. used for TLS security and requires Ericsson extension).
FILES	SFTP	New	Used for, PM report, Alarm log, ISP log, BRM Backup.

Table 2 Inter-node Interfaces

### 3.2 Man-Machine Interfaces

The changes to the man-machine interfaces are listed in table below.

Interface	Protocol	Impact	Description of changes compared to MTAS 4.15.0
ECLI	SSH/TLS	New	New CLI interface for vMTAS configuration management.
TelORB, T-Util, NM ToolBox	SSH	Obsolete	Tools for MTAS configuration and troubleshooting.
Cli_tool	SSH	New	New CLI interface for vMTAS troubleshooting.
CLI	SSH /	Obsolete	CLI interface for MTAS troubleshooting.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

	Telnet		
--	--------	--	--

Table 3 Changes in man-machine interfaces

### 3.3 Operation and Maintenance

This section describes changes to attributes, alarms, events and notifications, triggers, and counters.

The general changes are stated in section 3.3. The subsections below only describe the changes related to function parity comparing the application part of native MTAS 4.15.0 with vMTAS 1.15.0.

#### 3.3.1 Configuration

##### 3.3.1.1 Changed Attributes

There are no functionally changed MTAS application attributes.

##### 3.3.1.2 Deleted Attributes

There are no functionally deleted MTAS application attributes.

##### 3.3.1.3 Deprecated Attributes

There are no functionally deprecated MTAS application attributes.

##### 3.3.1.4 Obsolete Attributes

There are no functionally obsolete MTAS application attributes, but note the obsolete functions in section 2.1.

##### 3.3.1.5 New Attributes

The new attributes are shown in table below.

Attribute Name	Description
<b>Rebalancing by Moving Users between MTAS Instances</b>	
mtasReBalancingAdministrativeState	This attribute defines the administrative state of the Rebalancing feature. The activation/deactivation of the Rebalancing feature is performed using mtasReBalancingActivate/mtasReBalancingDeActivate Administrative Operations after

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

	enabling mtasReBalancingAdministrativeState  The default is set to 0 (LOCKED).
mtasReBalancingState	This attribute indicates the operational state of the Rebalancing feature. It has 3 possible values: INACTIVE(0), ACTIVE(1), and DEACTIVATING(2).  The default is set to 0 (INACTIVE).
mtasReBalancingTargetNodeSipUri	This attribute defines the target MTAS node SIP URI to be used for redirected registration requests.
mtasReBalancingThreshold	This attribute defines target limit for the number of subscribers remaining in the source MTAS node when the Rebalancing feature is activated.

Table 4 New Attributes

### 3.3.2 Fault Management

#### 3.3.2.1 Changed Alarms

There are no functionally changed MTAS application alarms.

#### 3.3.2.2 Deleted Alarms

There are no functionally deleted MTAS application alarms.

#### 3.3.2.3 New Alarms

There are no functionally new MTAS application alarms.

### 3.3.3 Events and Notifications

There are no events and notifications used by vMTAS.

### 3.3.4 IFC Triggers

Initial Filter Criteria (IFC) triggers used to trigger MTAS functions are unchanged for vMTAS 1.15.0, and are described in MTAS External Network Configuration, [18].

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

### 3.3.5 PM Counters

This section lists changed, deleted, deprecated, obsolete and new counters.

#### 3.3.5.1 Changed Counters

There are no functionally changed MTAS application counters.

#### 3.3.5.2 Deleted Counters

There are no functionally deleted MTAS application counters.

#### 3.3.5.3 Deprecated Counters

There are no functionally deprecated MTAS application counters.

#### 3.3.5.4 Obsolete Counters

There are no functionally obsolete MTAS application counters, but note the obsolete functions in section 2.1.

#### 3.3.5.5 New Counters

The new PM Counters are shown in table below.

Counter Name	Description
<b>Rebalancing by Moving Users between MTAS Instances</b>	
MtasSubsDataServedUsers	Incremented when an initial REGISTER request is received. Also incremented if an initial INVITE is received on a registered or unregistered port or a SUBSCRIBE to DEN service is received on the registered port for a new user. Decrement when the user's last device is de-registered from the MTAS node.
MtasSubsDataRegisteredUsers	Incremented when an initial REGISTER request is received. Also incremented if an initial INVITE or SUBSCRIBE to DEN service is received on the registered port from a not yet registered subscriber. Decrement when the de-registration of the subscriber is finished.
MtasReBalancingMovedUsers	Incremented when a subscriber's re-

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

	REGISTER request is answered with SIP 305 'Use Proxy' message, cleared when mtasReBalancingState is set to ACTIVE.
MtasReBalancingRedirections	Incremented when a subscriber's Initial REGISTER or re-REGISTER request is answered with SIP 305 'Use Proxy' message, cleared when mtasReBalancingState is set to ACTIVE.

Table 5 New PM Counters

## 4 Summary of Impacts per Feature

This section summarizes the impact per feature when the feature is turned on.

- **Major Impact** implies that the change has made an interface backward incompatible
- **Minor Impact** means that there are changes, but with additional configuration the previous behavior can be kept.
- **No Impact** means that the new version can be installed without affecting other nodes.

A summary of impacts per feature is shown in table below.

Function	Impact	Basic or Optional New, Modified or Obsolete	Included in Basic/Value Package (names only)	Relation to Other Features or Nodes

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

Operation and Maintenance(virtualized)	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	OSS-RC
VNF Deployment	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	
VNF Network connectivity	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	
VNF Scaling	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service	



Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

			Continuity AS SIP Trunking AS	
Rebalancing by Moving Users between MTAS Instances	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	CSCF
Auto Healing Work Flow Feature	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	
etc Hardened Overlay	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	
SCTP Support for DIAMETER	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS	HSS, Charging Server

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

			MMTel AS Voice Service Continuity AS SIP Trunking AS	
Hardened Etc Overlay Introduction	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	
Unique Prompt Prefix	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	
VMWare Instantiation and Termination Workflow	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	
New PM Job Names	Major	Basic New	Business Mobility AS Communication	

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

			Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	
Scaling Workflows for VMware	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	
Configurable MTU size	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	
vMTAS NFVO-Triggered Instantiate/Terminate Workflows for OpenStack NFVI	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

On-site Generation of VNF Package	Major	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	
Tool for faster and easier handling of subscriber and software trace	No impact	Basic New	Business Mobility AS Communication Interworking Function NW AS MMTel AS Voice Service Continuity AS SIP Trunking AS	

Table 6 Summary of Impacts per Feature

## 5 Impact on MTAS Functions

This section shows the impact on the MTAS functions when the function is turned on or utilized.

### 5.1 Operation and Maintenance (virtualized)

This section describes the new function OAM management (virtualized). The new function is merging a number of native operation and maintenance functions; Configuration Management, Performance Management, Fault Management, Traceability and Troubleshooting.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

### 5.1.1 Description

The function is adapted to the new OAM SW architecture and the Ericsson Common Information Model (ECIM) using NETCONF and Ericsson Command Line Interface (ECLI). The functional level is on the same level as in native MTAS.

For Configuration Management, see Section 2.8.1 and [22].

For Performance Management, see Section 2.8.2 and [23].

For Fault Management, see Section 2.8.3 and [24].

For SW Management, see Section 2.8.4 and [25].

### 5.1.2 Impact

This section describes the impact on capacity, performance, network elements and operation.

#### 5.1.2.1 Capacity and Performance

This section describes the impact on subscriber capacity and network performance.

##### 5.1.2.1.1 Subscriber Capacity

N/A.

##### 5.1.2.1.2 Network Performance

N/A.

#### 5.1.2.2 Other Network Elements

No significant impact.

#### 5.1.2.3 Operation

See references above.

## 5.2 VNF Deployment

This section describes the new function VNF Deployment, which replaces the native MTAS Installation.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

## 5.2.1 Description

See [3] for general information about the vMTAS VNF deployment and [25] for the description of the SW management.

## 5.2.2 Impact

This section describes the impact on capacity, performance, network elements and operation.

### 5.2.2.1 Capacity and Performance

This section describes the impact on subscriber capacity and network performance.

#### 5.2.2.1.1 Subscriber Capacity

N/A.

#### 5.2.2.1.2 Network Performance

N/A.

#### 5.2.2.2 Other Network Elements

No significant impact.

#### 5.2.2.3 Operation

For how to deploy vMTAS, see vMTAS SW Installation, [7]

## 5.3 VNF Robustness

This section describes the new function VNF Robustness, which covers several functions from native; Load Regulation, Node Protection, and Node Robustness in vMTAS.

### 5.3.1 Description

The virtual infrastructure provides a less robust and predictable environment on which to deploy the vMTAS application. Consequently, the vMTAS robustness and recovery mechanisms are enhanced compared to the native MTAS to handle the less secure and less predictable environment:

- vMTAS provides enhanced survivability during multiple System Controller, Payload or interface failures.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

- The system continues to handle traffic during failure of both System Controllers. The vMTAS system can handle and recover from multiple simultaneous failures on Payloads within the same vMTAS VNF.

### 5.3.2 Impact

This section describes the impact on capacity, performance, network elements and operation.

#### 5.3.2.1 Capacity and Performance

This section describes the impact on subscriber capacity and network performance.

##### 5.3.2.1.1 Subscriber Capacity

N/A.

##### 5.3.2.1.2 Network Performance

N/A.

#### 5.3.2.2 Other Network Elements

No significant impact.

#### 5.3.2.3 Operation

No significant impact.

### 5.4 VNF Scaling

This section describes the new function VNF Scaling.

#### 5.4.1 Description

The VNF Scaling is a key feature in cloud network. A scale-out operation is performed by adding one or more VMs to the Virtualized Network Function (VNF) cluster. Preboot Execution Environment (PXE) boot is used to distribute software to new VMs. For graceful scale-in, the VNF cluster reallocates the resources from VMs to be scaled-in and moves to other VMs to prevent data loss. Performance counters can be used as input to decide which scaling operation is to be performed.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

## 5.4.2 Impact

This section describes the impact on capacity, performance, network elements and operation.

### 5.4.2.1 Capacity and Performance

This section describes the impact on subscriber capacity and network performance.

#### 5.4.2.1.1 Subscriber Capacity

The VNF Scaling is used to adapt the VNF to the processing needed. During the actual scaling procedure, there is however a CPU peak to redistribute the data base in the cluster. A scale-out procedure takes around 5 minutes (redistribute data and start-up the OS). A scale-in procedure takes around 1 minute (redistribute data and shutdown the OS). During the redistribution, there is a load peak for about 15 seconds, which may lead to increased number of rejected SIP requests.

#### 5.4.2.1.2 Network Performance

The purpose with the VNF scaling is to adapt the network performance to meet the needs. Because of the short load peak during the actual scaling procedure, see section 5.4.2.1.1, the scale-out is recommended to be done before the increased need becomes a fact and that the scale-in shall be done when the decreased need is a fact.

### 5.4.2.2 Other Network Elements

There is no need for any reconfigurations in the rest of the network when vMTAS scaling takes place.

### 5.4.2.3 Operation

For how to scale vMTAS, see MTAS Scaling Management Guide, [19].

## 5.5 Rebalancing by Moving Users between MTAS Instances

This section describes the new function Rebalancing.

### 5.5.1 Description

vMTAS supports redistribution of registered users.

The rebalancing feature in MTAS enables the operator to move registered subscribers from a source MTAS node to a target MTAS node after node expansion, after MTAS node recovery or other maintenance activity.



Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

The rebalancing feature is activated manually by the operator after setting values for CM attributes including the target node SIP URI. When the feature is active, initial and re-registrations of a subscriber on the source MTAS node are responded with a 305 (Use Proxy) message that contains the address of the target MTAS node in the Contact header. The registration request is redirected to the target MTAS node and the subscriber is deregistered from the source MTAS node.

## 5.5.2 Impact

This section describes the impact on capacity, performance, network elements and operation.

### 5.5.2.1 Capacity and Performance

This section describes the impact on subscriber capacity and network performance.

#### 5.5.2.1.1 Subscriber Capacity

N/A

#### 5.5.2.1.2 Network Performance

N/A

### 5.5.2.2 Other Network Elements

This function will impact signaling towards HSS since the target MTAS node will fetch subscriber data for all the redirected registration requests.

### 5.5.2.3 Operation

For more information regarding the Rebalancing function in MTAS, see MTAS Subscriber Management Guide, [40].

## 5.6 Auto Healing Work Flow Feature

This section describes the new function Auto Healing.

### 5.6.1 Description

This functionality will auto heal a single PL failure or multiple PLs failures but it does not support unhealable PLs (PL-3, PL4) and System Controllers (SCs). A VNF can be healed from a computer resource or neutron port failure using the VNF-LCM in two ways:

- Manually from the VNF-LCM User Interface (UI).

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

- Automatically triggered on the reception of the “CLM Cluster Node Unavailable” alarm from the VNF instance.

## 5.6.2 Impact

This section describes the impact on capacity, performance, network elements and operation.

### 5.6.2.1 Capacity and Performance

This section describes the impact on subscriber capacity and network performance.

#### 5.6.2.1.1 Subscriber Capacity

N/A

#### 5.6.2.1.2 Network Performance

N/A

#### 5.6.2.2 Other Network Elements

N/A

#### 5.6.2.3 Operation

Automatic

## 5.7 etc Hardened Overlay

This section describes the new function etc Hardened Overlay.

### 5.7.1 Description

Hardened Etc overlay is used for hardening configuration files. Where the configurations must be applied in a non-dynamic fashion in order to prevent damaged configuration files.

With HEO RPM in place, vMTAS will introduce below functionality:

- 1 Default Umask 027
- 2 Legal Warning at Login
- 3 Inactivity Timer for Login

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

4 Inactivity timer for User Accounts

## 5.7.2 Impact

vMTAS will be more secure and hardened from security prospective.

### 5.7.2.1 Capacity and Performance

This section describes the impact on subscriber capacity and network performance.

#### 5.7.2.1.1 Subscriber Capacity

N/A

#### 5.7.2.1.2 Network Performance

N/A

#### 5.7.2.2 Other Network Elements

N/A

#### 5.7.2.3 Operation

N/A

## 5.8 SCTP Support for DIAMETER

This section describes the new function SCTP Support for DIAMETER.

### 5.8.1 Description

The purpose of this feature to introduce Profile 2 of vMTAS reference connectivity. vMTAS reference connectivity has defined evolution steps toward achieving traffic separation profile goals.

The following are introduced as part of this feature:

- Introduction of Multi-Homing for SIGTRAN.
- Introduction of SCTP for DIAMETER and multi-homing SCTP support.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

## 5.8.2 Impact

Minor impact on capacity, performance due to memory and CPU use by SCTP on multiple interfaces.

### 5.8.2.1 Capacity and Performance

This section describes the impact on subscriber capacity and network performance.

#### 5.8.2.1.1 Subscriber Capacity

See Impact.

#### 5.8.2.1.2 Network Performance

N/A

#### 5.8.2.2 Other Network Elements

N/A

#### 5.8.2.3 Operation

For configuration, please refer to [13].

## 5.9 Hardened Etc Overlay Introduction

This section describes the new function Hardened Etc Overlay Introduction.

### 5.9.1 Description

Hardened Etc overlay is used for hardening of configuration files under etc directory. Where configurations must be applied in a non-dynamic fashion in order to prevent damaged configurations files. With HEO RPM in place, MTAS will enforce the following functionality.

- Inactivity Timer for Login Session (default enabled, value 600 seconds)
- Inactivity timer for User Accounts (default enabled, value 90 days, On each login this program moves forward the account expiry by 90 days.)
- Strong Password Enforcement (default enabled)
- Auditing – Full Personal Accountability (default enabled)

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

— Legal warning at Login (configured by the customer)

For more information, refer to LDE Management Guide CPI section “etc-overlay”.

## 5.9.2 Impact

No impact on capacity, performance, network elements, and operation. MTAS will be more secure and hardened from system security prospective.

### 5.9.2.1 Capacity and Performance

This section describes the impact on subscriber capacity and network performance.

#### 5.9.2.1.1 Subscriber Capacity

N/A

#### 5.9.2.1.2 Network Performance

N/A

#### 5.9.2.2 Other Network Elements

N/A

#### 5.9.2.3 Operation

N/A

## 5.10 Unique Prompt Prefix

This section describes the new function Unique Prompt Prefix.

### 5.10.1 Description

With new LDEwS version integrated as part of baseline adaptation, vMTAS will support the configuration of a unique prompt id (using the attribute networkManagedElementId) that is displayed when logging into the VNF instance.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

New attribute to LDE configuration command is introduced to turn this feature ON Ide-config system add --unique-prompt on Once enabled, logout and login OR create a new shell to see the new prompt.

networkManagedElementId attribute value is set using below IMM configuration:

```
immcfg --attribute networkManagedElementId="Node_name"  
managedElementId=1
```

## 5.10.2 Impact

No impact on capacity, performance, network elements, and operation.

### 5.10.2.1 Capacity and Performance

This section describes the impact on subscriber capacity and network performance.

#### 5.10.2.1.1 Subscriber Capacity

N/A

#### 5.10.2.1.2 Network Performance

N/A

#### 5.10.2.2 Other Network Elements

N/A

#### 5.10.2.3 Operation

N/A

## 5.11 VMWare Instantiation and Termination Workflow

This section describes the new function VMWare Instantiation and Termination Workflow.

### 5.11.1 Description

It is now possible to deploy MTAS with a 2+2 configuration on a VMware based cloud using instantiation workflow scripts. It is possible to terminate graceful and forceful MTAS using the termination workflow scripts.

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

## 5.11.2 Impact

No impact on capacity, performance, network elements, and operation.

### 5.11.2.1 Capacity and Performance

This section describes the impact on subscriber capacity and network performance.

#### 5.11.2.1.1 Subscriber Capacity

N/A

#### 5.11.2.1.2 Network Performance

N/A

#### 5.11.2.2 Other Network Elements

N/A

#### 5.11.2.3 Operation

N/A

## 5.12 New PM Job Names

PmJob=NOOSSCONTROL\_MtasSla\_OSProcessingUnit

PmJob=NOOSSCONTROL\_MtasSla\_OSProcessingLogicalUnit

PmJob=NOOSSCONTROL\_MtasSla\_OsmDevic

## 5.13 Scaling Workflows for VMware

It is now possible to execute the scaling workflows on a VMware-based cloud.

### 5.13.1 Impact

No impact on capacity, performance, network elements, and operation.

## 5.14 Configurable MTU size

Support for configurable MTU is added, which enables an operator to choose

another value instead of default (1500) bytes. MTU up to 2140 has been tested in

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

vMTAS labs because of hardware/cloud infrastructure limitations. The customer can set higher values than this. But in that case, vMTAS behavior could be unexpected.

#### 5.14.1

##### **Impact**

MTU=1500 (default): No impact.

MTU=1500 to 2140: vMTAS will utilize bigger MTU size with expected behavior.

MTU > 2140: unexpected behavior.

MTU = 9000: vMTAS cluster will be unstable (already TRd: HX18750).

#### 5.15

##### **vMTAS NFVO-Triggered Instantiate/Terminate Workflows for OpenStack NFVI**

On OpenStack NFVI, vMTAS VNF Package now supports Instantiate and Terminate workflows from NFVO nodes through the Or-Vnfm interface

#### 5.15.1

##### **Impact**

No impact on capacity, performance, network elements, and operation.

#### 5.16

##### **On-site Generation of VNF Package**

The VNF package needs to be generated by the delivered vnfPackageCreator\_mtas.py from the vMTAS Workflow Package, the updated HOT and environment files. Manual generation of VNF Packages is no longer supported.

For more information about the structure of the generated VNF Package, refer to MTAS VNF Life Cycle Management Guide, 131/1553-AVA 901 29/9.

#### 5.16.1

##### **Impact**

Major Impact – The structure of the generated VNF Package differs from the package generated manually before.



Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

## 5.17 **vMTAS, Faster and easier handling of subscriber and software trace**

The MtasTrace tool makes it possible to manage subscriber or software trace in vMTAS system in a faster and more efficient way. The tool supports easy configuration, start and stop of trace session. Generated trace messages can be tailed to new files to avoid information loss due to log rotation. CPU load monitoring and automatic deactivation of the trace session protects against system overload.

### 5.17.1 **Impact**

No impact on capacity, performance, network elements, and operation.

## 6 **References**

Title	Doc no
[1] Glossary of Terms and Acronyms	1/0033-AVA 901 29/9 Uen
[2] MTAS Technical Product Description Common Features	1/221 02-FGC 101 2990 Uen
[3] vMTAS Technical Product Description Common Features	1/221 02-FGC 101 3266 Uen
[4] MTAS Troubleshooting Guideline	154 51-AVA 901 29/9 Uen
[5] MTAS Health Check	53/1543-AVA 901 29/9 Uen
[6] vMTAS 1.15.0 Characteristics Specification and Dimensioning Guidelines	8/155 02-AVA 901 29/9 Uen
[7] MTAS SW Installation	1/1531-AVA 901 29/9-8 Uen
[8] Virtual MTAS Infrastructure Requirements	3/1056-AVA 901 29/9 Uen
[9] Managed Object Model MTAS	1554-LZN 765 0163/9-V1 Uen
[10] Ericsson NETCONF	2/155 19-CAA 901 2587/7 Uen

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

Interface	
[11] Ericsson Command-Line Interface User Guide	6/1553-CAA 901 2587/7 Uen
[12] MTAS Demo Description	16/155 52-AVA 901 18 Uen
[13] MTAS Internal and External Connectivity	1/1551-AVA 901 29/9 Uen
[14] vMTAS Upgrade Instruction	1/153 72-AVA 901 29/9-8 Uen
[15] vMTAS Upgrade Information	2/153 72-AVA 901 29/9-8 Uen
[16] MTAS Configuration for Provisioning LDAP	118/1553-AVA 901 29/9 Uen
[17] Parameter Description for Provisioning MTAS MOCs	1/190 84-AVA 901 29/9 Uen
[18] MTAS External Network Configuration	43/1553-AVA 901 29/9 Uen
[19] MTAS Scaling Management Guide	119/1553-AVA 901 29/9 Uen
[20] MTAS to vMTAS Parameter Migration	4/154 43-AVA 901 29/9 Uen
[21] Free and Open Source Software	1/0962-AVA 901 29/9 Uen
[22] System Management	3/1551-AVA 901 29/9 Uen
[23] Performance Management	11/1551-APA 901 44/1 Uen
[24] Fault Management	3/1551-CAA 901 2587/7 Uen
[25] Software Management	2/1551-APR 901 0444/4 Uen
[26] Performance Management Report File Format	1/155 19-CRA 119 632/4 Uen
[27] Performance Management Report File Format	1/155 19-CAA 901 2587/7 Uen
[28] SNMP Alarm Subagent Interface Description	3/155 19-CRA 119 643/4 Uen

Prepared (also subject responsible if other) EHITERA Hitesh singh Rathor		No. 531/109 48-AVA 901 29/9-13 Uen		
Approved BDGSEACO [Attila Schmidt A]	Checked	Date 2019-06-177	Rev A	Reference

[29] ERICSSON-ALARM-MIB	5/196 03-CXC 172 7549 Uen
[30] Ericsson TSP Events MIB	1/155 19-CRA 119 643/3 Uen
[31] Ericsson NETCONF Browser User Guide	1/1553-LXA 119 1714 Uen
Ericsson NETCONF Browser Technical Product Description	1/221 02-LXA 119 1714 Uen
[32] CEE Technical Description, Cloud Execution Environment	221 02-FGC 101 3270 Uen
[33] BSP Technical Product Description, BSP 8100	221 02-FGC 101 2255 Uen
[34] MTAS Performance Measurements	1/1553-AVA 901 29/9 Uen
[35] MTAS Alarm List	1/006 51-AVA 901 29/9 Uen
[36] System Backup and Restore	2/1551-CAA 901 2624/4 Uen
[37] MTAS Security Management Guide	122/1553-AVA 901 29/9 Uen
[38] Data Collection Guideline for MTAS	70/1543-AVA 901 29/9 Uen
[39] MTAS Licenses	1/1555-AVA 901 29/9 Uen
[40] MTAS Subscriber Data Management Guide	10/1553-AVA 901 29/9 Uen