ERICSSON

MTAS Health Check

MTAS

OPERATING INSTRUCTIONS

53/1543-AVA 901 29/9 Uen D1

Contents

1 Introduction

This document describes how to perform the health check on the MTAS running in virtualized environment. The health check tasks described in the Health Check Procedure section are recommended to be performed before and after a system update/upgrade, a normal backup, or during the periodic maintenance.

1.1 Prerequisites

This section states the prerequisites for performing the health check procedure.

1.1.1 Documents

Before starting this procedure, ensure that the following information or documents are available:

- The release information for the MTAS software level that is intended to be run in the MTAS. The item of interest is as follows:
  - MTAS RDP versions

Note: The release information can, for example, be found in delivery reports, delivery specifications, delivery notes, release notes, or correction notes.

1.1.2 Knowledge

It is assumed that the user of this document is familiar with the Operation and Maintenance (O&M) area, in general. It is also assumed that the user is familiar with the concepts, terminology, and abbreviations within this area.

1.1.3 Tools

The following tool is required to check a summary of the health check:

- Any web browser supporting HTML 4.01.

2 Health Check Procedure

All health checks are grouped into three profiles described in the Health Check Profiles section. The mandatory profile contains basic checks that determine decision of the MTAS node health status. The MTAS node can be considered as healthy if all the checks are OK. By default health check with mandatory profile is performed periodically once per hour. In troubleshooting situations or when more information is desired, the checks can be performed manually.

2.1 Packers List

To check which profiles are available use *cdclsv-list-packers* command. As a result the list of DNs is displayed:

```
cdclsPk=HcMtasLowPriority,cdcls=CDCLSvSite
cdclsPk=HcMtasMandatory,cdcls=CDCLSvSite
cdclsPk=HcMtasMediumPriority,cdcls=CDCLSvSite
```

Each DN denotes a reference to cdclsv pack object related to proper Health Check profile. Each cdclsv pack object has its own configuration and a list of checkers.

2.2 Manual Health Check

To perform selected profile use *cdclsv-pack <DN>*.

```
cdclsv-pack cdclsPk=HcMtasMandatory,cdcls=CDCLSvSite
```

Execution status of selected DN can be checked by *cdclsv-pack-status <DN>*.

```
cdclsv-pack-status cdclsPk=HcMtasMandatory,cdcls=CDCLSvSite
```

2.3 Health Check Results

HealthCheck results are stored in directory: `/storage/no-backup/hc`. Each health check run results in a separate package with checkers status.

Package structure:

- summary.html - Contains general information about checkers status in HTML format.
- summary.xml - Contains general information about checkers status in XML format.

- <Checker name>.log - Contains data gathered by Data Collection. File may not exist if particular health check step does not return data to log.
- <Checker name> - Directory with data gathered by Data Collection step. Directory may not exist if particular health check step does not copy data or does not create specific structure.

By default data gathered by Data Collection is stored in result package only if any checker detects problems.

2.4 Health Check Verdict

The result from the checks is stored in summary files. The verdict is a way to inform the user about status of the individual checks. The definitions of the different verdicts are shown in Table 1.

Table 1 Health Check Verdicts

Verdict Sign	Verdict	Description
,	INFO	Information for the user, not checked by the script.
.	OK	Automatic checked passed.
?	VERIFY	Manual verification needed.
!	FAIL	Problem detected by automatic health check.
E	ERROR	An error occurred, script update needed or system broken.

3 Health Check Profiles

This section describes health check profiles content. All health checks are grouped according to importance: Mandatory, Medium and Low priority.

3.1 Mandatory Profile

This profile verifies basic node information.

Table 2 Mandatory Profile Checkers

Checker	Description
Alarms and notifications	Checks if there are any unresolved alarms or notification.
Core MW status	Verifies if there are any AMF entities with questionable health.
DRBD Status	Checks if the DRBD device is in synchronized state.
eVIP status	Verifies status of eVIP.
LDAP connection	Checks if LDAP is configured and responds for requests.
MMAS	Checks MMAS deployment information from MMAS JBOSS application server. This step is not reliable, verdict can be ignored.
NETCONF connection	Verifies if NETCONF is configured on exactly 1 controller.
Network connectivity	Verifies if connectivity between each SC/PL node.
Node outage	Checks node state and verifies ISP logs. Verdict is FAIL if any of the nodes is not started. VERIFY verdict can be ignored.
Operational state	Checks MTAS operational state using COM interfaces.
Processor outage	Checks if there are any unresolved alarms related with node unavailability (based on SAF fault management) This step is not reliable, verdict can be ignored.

SS7 connections	Verifies SS7 stack status. Verdict is FAIL, if SS7 stack is not configured. VERIFY verdict can be ignored.
System status	Verifies system services status. Data gathered by cmw-status.
VirtualDicos process outage	Checks status of virtual machines.
XDMS instance	Verifies XDMS instance status.

3.2 Medium Priority Profile

Medium priority profile contains all steps from mandatory profile and from Table 3.

Table 3 Medium Priority Profile Checkers

Checker	**Description**
All MTAS ports status	Verifies if MTAS ports are open. List of the ports defined in Hardening Guide.
CPU load on PLs	Verifies if CPU load on each PL is below critical value. Thresholds: verdict is OK, if load is less than 30 %, VERIFY, if load is between 30% and 50%, FAIL, load is over 50%.
CpPU load on SCs	Verifies if CPU load on each SC is below critical value. Thresholds: verdict is OK, if load is less than 30 %, VERIFY, if load is between 30% and 50%, FAIL, load is over 50%.
Diameter ports status	Verifies Diameter ports status. Data about diameter port configuration is gathered from COM management objects. This step is not reliable, verdict can be ignored.
Disk use on SCs	Verifies level of available space on SCs disks. Thresholds: verdict is OK, if available space is over 30%, VERIFY, if it is between 30% and 10%, FAIL if less than 10%.
Memory use on PLs	Checks use of memory on each PL. Thresholds: verdict is OK, if memory usage is below 70%, VERIFY, if it is between 70% and 90%, FAIL if over 90%.
Memory use on SCs	Checks use of memory on each controller. Thresholds: verdict is OK, if memory usage is below 70%, VERIFY, if it is between 70% and 90%, FAIL if over 90%.

SIP ports status	Verifies if SIP ports are open. List of the ports defined in Hardening Guide.
XDMS CAI certificate	Checks if the XDMS server certificate is valid.
XDMS rpm	Verifies XDMS package list. This step is not reliable, verdict can be ignored.
XDMS traffic apps	Verifies traffic logs from MMAS server. This step is not reliable, verdict can be ignored.

3.3 Low Profile

Low priority profile contains all steps from medium priority profile and from Table 4.

Table 4 Low Priority Profile Checkers

Checker	**Description**
Backup list	Checks if there is an active backup available to restore.
Security status	Verifies Core MW security package installed on SC/PL nodes.
Software inventory	Collects a list of RPM/SDP files available on SC/PL nodes.
Software versions installed	Collects a list of software installed on node.
Software versions running	Collects a list of software installed and running on node.
System environment variables	Checks vDicos environment variables.
Upgrade list	Based on Core MW repository list verifies if all campaigns are updated.
Vm logs	Inspects vDicos Virtual Machine Logs if any error occurred. This step is for informational purpose only, verdict can be ignored.

4 Problem Reporting

For any abnormal situation, refer to *MTAS Troubleshooting Guideline*.

If the problem still exists, the user can report it to the next level of support.

It is also important to collect the related data. For more information, refer to *Data Collection Guideline for MTAS*.