UCSM DME Database Health Check Feature Guide

Contents

Introduction

This document describes features related to Data Management Engine (DME) Database (DB) introduced in Unified Computing System Manager (UCSM) 3.1.3a release.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- UCSM

Components Used

The information in this document is based on these software and hardware versions:

- UCSM software version 3.1.3a
- Fabric Interconnect (FI) 6200 series and 6332 models

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, ensure that you understand the potential impact of any command.

Background Information

DME is the central component of UCSM software architecture that holds system state information. The information is stored on
the local storage FI device in the form of embedded database known as DME DB.

The data integrity in the database can get corrupted due to storage hardware device failure. With UCSM 3.1.3a release, many new features
are added to make UCSM more resilient using periodic DB health check, seamlessly recovery of corrupted DB and data protection by an automatic backup of the DME DB.

UCSM DME Database Health Check Features

Periodic Database Health Check

UCS manager initiates health check of DB at periodic intervals to validate the integrity of the data.

The system also allows users to manually run health check and verify the DB integrity.

Verify default configuration

By default, the health check is performed every 12 hours, to show the current status use these commands:

```
UCS # scope system
UCS /system # show mgmt-db-check-policy detail

Management Database Integrity Check Policy:
Health Check Interval (hours): 12
Last Integrity Check Time: 2017-05-07T14:42:47.019
Internal Backup Interval (days): 14
Last Internal Backup Time: 2017-04-28T14:52:12.648
UCS /system #
```

Change the interval

While you can modify the time interval or disable health check, it is strongly recommended to not make changes to the default configuration.

> **Caution**: It is strongly recommended to not change these values from the default

In this example, the interval is changed from 12 hours to 48 hours.

```
UCS /system # set mgmt-db-check-policy health-check-interval 48
UCS /system* # commit-buffer
UCS /system # show mgmt-db-check-policy detail

Management Database Integrity Check Policy:
Health Check Interval (hours): 48
Last Integrity Check Time: 2017-05-07T14:42:47.019
Internal Backup Interval (days): 14
Last Internal Backup Time: 2017-04-28T14:52:12.648
```

To disable the health check, set the value to zero.

Manually run the health check

To verify the DB health check, you can execute these commands. If no message is printed on the terminal, then DB is in good health.

```
UCS # scope system
UCS /system # start-db-check
UCS /system* # commit-buffer
```

In addition, any error message will be logged in the primary FI DME log file (part of UCSM techsupport bundle).

```
[prt:executeHealthCheck] Health Check complete with no corruption
```

This command allows you to further verify the DB status:

```
UCS # scope system
UCS /system # show mgmt-db

Management Database Status:
Fabric Id Corrupted Count Last Occurrence Time
--------- ---------------------- --------------------
A 0 1970-01-01T00:00:00.000
B 0 1970-01-01T00:00:00.000
```

DB Corruption - User level fault and Recovery mechanism

If UCSM detects corruption in DB during health check, it generates fault messages.

An INFO level fault is generated when there is a single occurrence and if corruption has happened more than once, MAJOR level faults are logged and you need to take further action and contact Cisco TAC. Gather a techsupport bundle.

```
ucs /system # show fault
Severity Code Last Transition Time ID Description
```

```
--------- -------- ------------------------ -------- -----------
Info F1899 2017-04-28T01:09:23.332 263649 Management database corruption detected and recovered
on Fabric Interconnect B. Number of corruption events: 1. Last corruption event timestamp: 2017-
04-28T01:09:23.332

Major F1900 2017-05-02T00:52:07.846 263651 High number of management database corruption events
on Fabric Interconnect A. Number of corruption events: 3. Last corruption event timestamp: 2017-
05-02T01:06:06.387
```

Recovery mechanism

UCSM automatically resolves the corruption without any affect to any services or data plane traffic, it overwrites the DB from memory or copies the good DB from peer FI.

Corruption Event	System Recovery mechanism
Primary FI	Database is recovered from in memory Management Information Tree (MIT)
Subordinate FI	Database file is retrieved from Primary FI

Reset corruption count

The DB corruption persists until it is manually cleared out. For example, if FI hardware was replaced based on further investigation to resolve the corruption, you can execute this command to reset the corruption fault count.

```
ucs-A # scope system
ucs-A /system # set mgmt-db-check-policy reset-corruption-count yes
ucs-A /system* # commit-buffer
```

Periodic Backup

To maximize the data protection, UCSM takes full state backup of UCSM configuration (DME DB) every two weeks which can be used for recovery purposes.
Further, DB integrity check is validated so that backup includes configuration from a good state.
Full state backup file is saved on each FI's /workspace/backup directory.

```
UCS # connect local-mgmt
UCS(local-mgmt)# dir backup/
1 1823454 Apr 28 14:53:23 2017 internalBackup.1493391132.tgz
```

Change backup job interval

The frequency of the backup job can be changed from 1 to 60 days. As shown in this example, we changed the value to 28 days.

```
UCS # scope system
UCS /system # set mgmt-db-check-policy internal-backup-interval 28
UCS /system* # commit-buffer
```

```
UCS /system # show mgmt-db-check-policy detail
```

```
Management Database Integrity Check Policy:
Health Check Interval (hours): 24
Last Integrity Check Time: 2017-05-10T10:35:24.909
Internal Backup Interval (days): 28
Last Internal Backup Time: 2017-04-28T14:52:12.648
UCS /system #
```

Related Information

- Cisco UCS Manager XMP API Programmer's Guide
- UCSM 3.1 CLI configuration guide