

Guia de recursos de verificação de integridade do banco de dados UCSM DME

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Recursos da verificação de integridade do banco de dados UCSM DME](#)

[Verificação de Integridade do Banco de Dados Periódico](#)

[Verificar a configuração padrão](#)

[Alterar o intervalo](#)

[Executar manualmente a verificação de integridade](#)

[Corrupção de banco de dados - Mecanismo de recuperação e falha no nível do usuário](#)

[Mecanismo de recuperação](#)

[Redefinir contagem de corrupção](#)

[Backup periódico](#)

[Alterar intervalo de trabalho de backup](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve os recursos relacionados ao Banco de Dados do Mecanismo de Gerenciamento de Dados (DME - Data Management Engine) (DB - Data Management Engine) introduzido na versão 3.1.3a do Unified Computing System Manager (UCSM).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCSM

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software UCSM versão 3.1.3a
- Fabric Interconnect (FI) série 6200 e modelos 6332

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O DME é o componente central da arquitetura do software UCSM que contém informações de estado do sistema. As informações são armazenadas em o dispositivo FI de armazenamento local na forma de banco de dados incorporado conhecido como DME DB.

A integridade dos dados no banco de dados pode ser corrompida devido à falha do dispositivo de hardware de armazenamento. Com o UCSM 3.1.3a release, muitos recursos novos são adicionados para tornar o UCSM mais resiliente usando a verificação periódica de integridade do banco de dados, recuperação transparente de banco de dados corrompido e proteção de dados por um backup automático do banco de dados de DME.

Recursos da verificação de integridade do banco de dados UCSM DME

Verificação de Integridade do Banco de Dados Periódico

O UCS manager inicia a verificação de integridade do banco de dados em intervalos periódicos para validar a integridade dos dados.

O sistema também permite que os usuários executem manualmente a verificação de integridade e verifiquem a integridade do banco de dados.

Verificar a configuração padrão

Por padrão, a verificação de integridade é realizada a cada 12 horas, para mostrar o status atual, use estes comandos:

```
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 #
```

Alterar o intervalo

Embora você possa modificar o intervalo de tempo ou desabilitar a verificação de integridade, é altamente recomendável não fazer alterações na configuração padrão.

Caution: É altamente recomendável não alterar esses valores do padrão

Neste exemplo, o intervalo é alterado de 12 horas para 48 horas.

```
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
```

Para desativar a verificação de integridade, defina o valor como zero.

Executar manualmente a verificação de integridade

Para verificar a verificação de integridade do DB, você pode executar esses comandos. Se nenhuma mensagem for impressa no terminal, o DB está em bom estado de funcionamento.

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

Além disso, qualquer mensagem de erro será registrada no arquivo de log FI DME principal (parte do pacote de suporte técnico UCSM).

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

Esse comando permite verificar ainda mais o status do DB:

```
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
```

Corrupção de banco de dados - Mecanismo de recuperação e falha no nível do usuário

Se o UCSM detectar corrupção no banco de dados durante a verificação de integridade, ele

gerará mensagens de falha.

Uma falha de nível de INFO é gerada quando há uma única ocorrência e se a corrupção tiver ocorrido mais de uma vez, as falhas de nível MAJOR são registradas e você precisa tomar outras medidas e entrar em contato com o TAC da Cisco. Reúna um pacote de suporte técnico.

```
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
```

Mecanismo de recuperação

O UCSM resolve automaticamente a corrupção sem afetar nenhum tráfego de plano de dados ou serviços, sobrescreve o banco de dados da memória ou copia o banco de dados bom do peer FI.

Evento de corrupção

Mecanismo de recuperação do sistema

| | |
|----------------|--|
| FI primário | O banco de dados é recuperado na árvore de informações de gerenciamento de memória (MIT) |
| Subordinado FI | O arquivo do banco de dados é recuperado do FI primário |

Redefinir contagem de corrupção

A corrupção do banco de dados persiste até que seja removida manualmente. Por exemplo, se o hardware FI foi substituído com base em investigação adicional para resolver a corrupção, você pode executar este comando para redefinir a contagem de falhas de corrupção.

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

Backup periódico

Para maximizar a proteção de dados, o UCSM usa o backup de estado completo da configuração do UCSM (DME DB) a cada duas semanas, que pode ser usado para fins de recuperação. Além disso, a verificação de integridade do banco de dados é validada para que o backup inclua a configuração de um bom estado. O arquivo de backup de estado completo é salvo no diretório /workspace/backup de cada FI.

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

Alterar intervalo de trabalho de backup

A frequência do trabalho de backup pode ser alterada de 1 para 60 dias. Como mostrado neste exemplo, mudamos o valor para 28 dias.

```
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 #
```

Informações Relacionadas

- [Guia do programador de API XMP do Cisco UCS Manager](#)
- [Guia de configuração da CLI do UCSM 3.1](#)