目次

概要

資料はユニファイド コンピューティング システム ファブリック相互接続（FI）クラッシュか予想外再度ブートする失敗を調査するためにステップを提供したものです。

高レベルで、次の問題は FI の再度ブートするという結果に終る可能性があります

- カーネル領域プロセスはクラッシュしました（別名カーネル パニック）
- カーネルはメモリを使い果たしました（メモリから-メモリを開拓するためにユーザ プロセスを強制終了する OOM）
- クラッシュするユーザ領域プロセス（前。 - netstack、fcoe_mgr、callhome 等）
- FI ファームウェア問題（まれなシナリオ、例- CSCuq46105）またはハードウエアコンポーネント失敗（ストレージに使用する SSD のように）

前提条件

要件

次の項目に関する知識があることが推奨されます。

Cisco Unified Computing System（UCS）マネージャ

Cisco Unified Computing System（UCS）マネージャ Command Line Interface（CLI）

必須ログファイル

FI が予想に反してリブートするとき、続くログを集め、TAC サービス リクエストにそれをアップロードして下さい。

- UCSM techsupport ログ バンドル

- コアダンプ ファイルが再度ブートする イベントの時のまわりに作成されるかどうか確認して下さい。
  CLI か GUI によってコア・ダンプ ファイルがあるように確認できます

  UCS-FI #スコープ モニタリング

  UCS-FI /monitoring #スコープ sysdebug

  UCS-FI /monitoring/sysdebug は#コア詳細を示します

- syslog サーバにログをエクスポートするために FI が設定される場合再度ブートする タイムスタンプ前に 7 日の履歴を提供するデバイスのための syslog サーバからのログメッセージを収集して下さい。

- (再度ブートするがカーネル パニックが原因なら) カーネル スタック トレース

最初の糸口のためのログを分析する方法

1) Nexus オペレーティング システム (NX-OS) " show version " コマンド出力からの再度ブートする理由およびタイムスタンプがあるように確認して下さい

2) 再度ブートする タイムスタンプ前にログメッセージがあるように「**show logging nvram**」コマンド 出力を確認して下さい

3) syslog サーバで保存される追加糸口があるようにログメッセージを確認して下さい

4) 再度ブートするがユーザ領域プロセス クラッシュによって引き起こされた場合、プロセス名および再度ブートする タイムスタンプと一致するコアダンプをチェックして下さい。

6) それがカーネル パニックである場合、確認して下さいあるように「**sw_kernel_trace_log**」と名付けられるファイルのカーネル スタック トレース出力が

UCSM 2.2.1b から、このファイルは含まれた UCSM 示します techsupport バンドルをです。

2.2.1b 以前の UCSM バージョンに関しては次のコマンドの出力を集めて下さい

7) 「**topout.log** 上」コマンド」**は** 2 秒毎にの「出力が含まれています。 再度ブートするの前に、UCSM は /opt/sam_logs.tgz ファイルがそれメモリ、利用またはプロセスについての情報を提供できると同時にログの古いセットを保存します。

8) 注意すればメモリ (OOM) からののようなメッセージはプロセスおよびプロセス クラッシュを FI の再度ブートするを引き起こす可能性があり、リセット理由として isted 止めました。そのようなシナリオでは、それは可能性が高いですプロセスで、メモリが低い状態の対象クラッシュまたはメモリリークの後ろの原因ではないかもしれません。

UCS セットアップについての収集する 情報

返事以下はよりよくシステム セットアップおよびそれが再度ブートする以前状態であることを理解するためにヘルプに質問します。

1) ずっとこの問題は前に起こっていますか。

2) 再度ブートするの時のまわりにあらゆる特定のユーザー操作がありましたか。

3) FI に行う最近のソフトウェア/ハードウェア/コンフィギュレーション変更をか。

4) Fi はあらゆる外部アプリケーションによって監察されています (SNMP に

5) Yes の場合は、アプリケーションはどのように頻繁にデータのための FI をポーリングしますか。 これらのアプリケーションによってどんな情報が一定の間隔でポーリングされますか。 (前 SNMP クエリ)

6) FI マネージメントポートの方のトラフィック嵐がずっとありますか。

7) このスケールは設定されますか。 (シャーシ、ブレード、仮想インターフェイスの数)

予防的に FI のモニタための提案

1) syslog サーバにログをエクスポートするために UCSM を設定して下さい

2) CPU およびメモリの傾向を監視するために口ーカルmgmt から「show processes」の出力を一定の間隔で集めて下さい

プロセスの使用方法。 外部アプリケーションによって監察される FI が arleady である場合この必要な tis。

関連情報

Cisco UCS Manager コンフィギュレーション ガイド