【MVS】Windows日志分析基础

性能分析和调优 **吴成井** 2023-07-04 发表

问题描述

Windows日志分析基础介绍

解决方法

1. Windows日志分析基础

1.1. Windows常见日志分类

1) Enent log
2) Performance log
3) Event tracing log
4) Dump file
5) App-related log files

1.2. 日志作用介绍

1.2.1. Event log

Windows常用排错手段。

日志内容涉及：应用安装、安全管理、系统设置、问题或报错等。

默认存储位置： %SystemRoot%\system32\winevt\logs\

1.2.2. Performance log

日志涵盖的范围：

1) 操作系统基础组件：存储，内存，网络，处理器，系统组件；
2) 应用组件：SQL，Exchange，第三方应用等….

1.2.3. Event tracing log

ETW：Event tracing for Windows

ETW tracing作用：

1) 提供对操作系统或用户、内核模式运行的更深解读。
2) 显示特定驱动的延迟和行为。
3) 无需重启系统或安装调试工具，可通过接口实时访问。
4) 常见格式ETL（Event tracing log format)

Events和Performance counters区别；

1) Performance 记录以ms为单位，常用于总体性能诊断；
2) ETL记录以us为单位，每分钟产生数GB的数据，记录了详细的系统信息

1.2.4. Dump file

1.2.4.1. 系统DUMP文件：

Dump文件是系统出错一瞬间的系统内存静态拷贝。

系统保存DUMP的流程：

1) 系统调用基本磁盘驱动，把内存数据写入到系统盘的pagefile中；
2) 启动时，系统检查注册表值，确定是否要转换DUMP文件；
3) 当需要转换时，系统将page文件写道memory.dmp中；

Dump file类型设置方法：系统属性》高级》启动和故障恢复》写入调试信息

Dump file常见类型：

1) Complete memory dump(完全内存转储）：内存中所有用户态和内核态数据。
2) Kernel memory dump（核心内存转储）：内存中内核态数据，为完全转储文件的1/3。
3) Smal memory dump(minidump)：基本调试信息，文件较小，一般64KB-256KB。

1.2.4.2. 应用程序dump文件

收集应用程序的userdump文件

目的：在应用程序失去响应或占用高CPU时，手动收集应用程序的User Dump文件。

方法：在“任务管理器”中右击程序，创建转储文件。

1.2.4.3. Symbol文件

Symbol file是以pdb为扩展名一个数据信息文件，包含应用程序二进制文件调试信息，专门用于调试时解释可执行文件中的变量信息。

Symbol 分为public symbol（定位到函数）和private symbols（定义到变量和源代码）,大部分信息需要配合源代码才可方便分析。

1.2.5. 其他应用日志

常见应用日志：

1) Setup log
2) Cluster log
3) IIS log
4) DHCP log
5) DNS log
6) Windows update log
7) ……

1.3. 日志的常规分析工具和方法

1.3.1. Event View

启动：Event Viewr(事件查看器)

常见日志分类：

1) 系统日志，10天内无重复性故障报告。
2) 应用日志：应用相关日志
3) 安全日志：默认关闭
4) Forwarded Events：远程收集日志，方便监控；