Основы построения отказоустойчивых систем

Мельников В.М., 2011

Отчетность

- ЭКЗАМЕН
- ДОПУСК – сдача практических задач

Литература

- Основная
  - Г. Гарсиа-Молина, Д. Ульман, Д. Уидом. Системы баз данных: полный курс. — Изд. «Вильямс», 2003.
- Вспомогательная
  - J. Gray, A. Reuter. Transaction Processing: Concepts and Techniques. — Morgan Kaufmann, 1993.

Содержание

- Что такое транзакция? Распространение ошибок
- Принципы построения аппаратного обеспечения, устройств хранения, надежных процессов и надежной передачи данных
- Модели транзакций. Блокировки. Оптимистичные и пессимистичные методы. Взаимное блокирование
- Алгоритмы работы с журналом. Восстановление

Введение

- Типовые приложения:
  - Коммуникации
  - Финансы
  - Путешествия
  - Управление процессами
- Появление специализированных средств

Что такое Транзакция

- Группа операций(эффект от выполнения группы операций) со свойствами
  - Атомарность
  - Согласованость(непротиворечивость)
  - Изолированость
  - Устойчивость(прочность)
- ACID
  - atomicity, consistency, isolation, durability

Управление транзакцией

- BEGIN TRANSACTION
- COMMIT
- ROLLBACK

Отказоустойчивость

- Доступность – доля времени работы системы с приемлимым временем ответа, измеряется обычно в %.

Классы доступности

Доступность %	Время простоя в год в	Время простоя месяц*	Время простоя в неделю
90%	36.5 дней	72 часов	16.8 часов
99%	3.65 дней	7.20 часов	1.68 часов
99.9%	8.76 часов	43.2 минут	10.1 минут
99.99%	52.56 минут	4.32 минут	1.01 минут
99.999%	5.26 минут	25.9 секунд	6.05 секунд
99.9999%	31.5 секунд	2.59 секунд	0.605 секунд
99.99999%	3.15 секунд	0.26 секунд	0.06 секунд

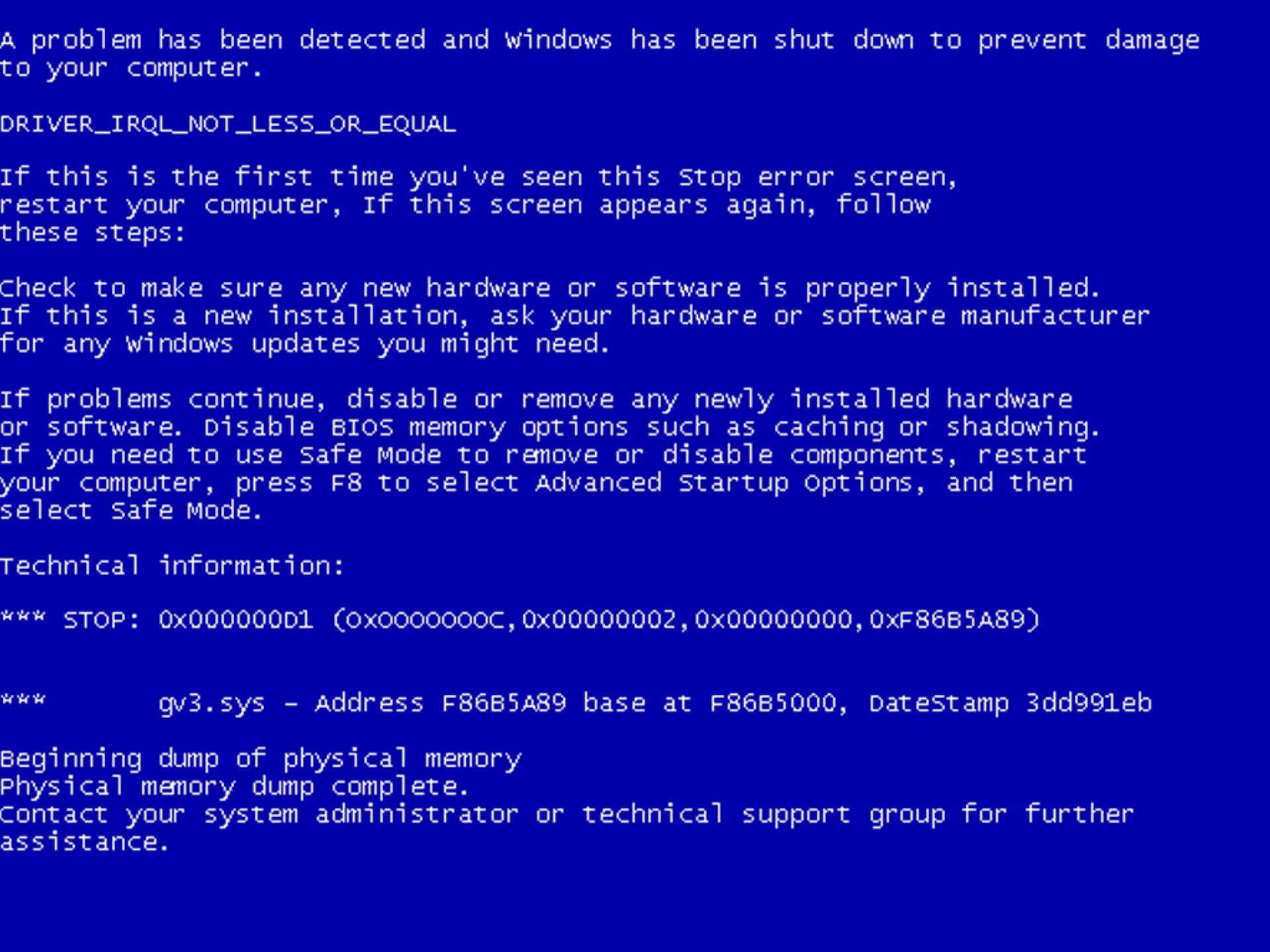
Доступность модуля

- Доступность = MTTF/(MTTF+MTTR)
- MTTF – среднее время наработки на отказ
- MTTR – среднее время восстановления

- Mean Time To Failure(Recovery)

Распространение ошибки

- Опечатка/погрешность
- Ошибка
- С….


A problem has been detected and Windows has been shut down to prevent damage
to your computer.
DRIVER_IRQL_NOT_LESS_OR_EQUAL
If this is the first time you've seen this Stop error screen,
restart your computer, If this screen appears again, follow
these steps:
Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.
If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.
Technical information:
*** STOP: 0x000000D1 (0x0000000C,0x00000002,0x00000000,0xF86B5A89)
*** gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb
Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.

Распространение ошибки

- Опечатка/погрешность
- Ошибка
- Сбой

Причины ошибок

- Ошибки в программах
- Сбой аппаратного обеспечения
- Сбой программного обеспечения
- Проблема окружения(электропитание, охлаждение)

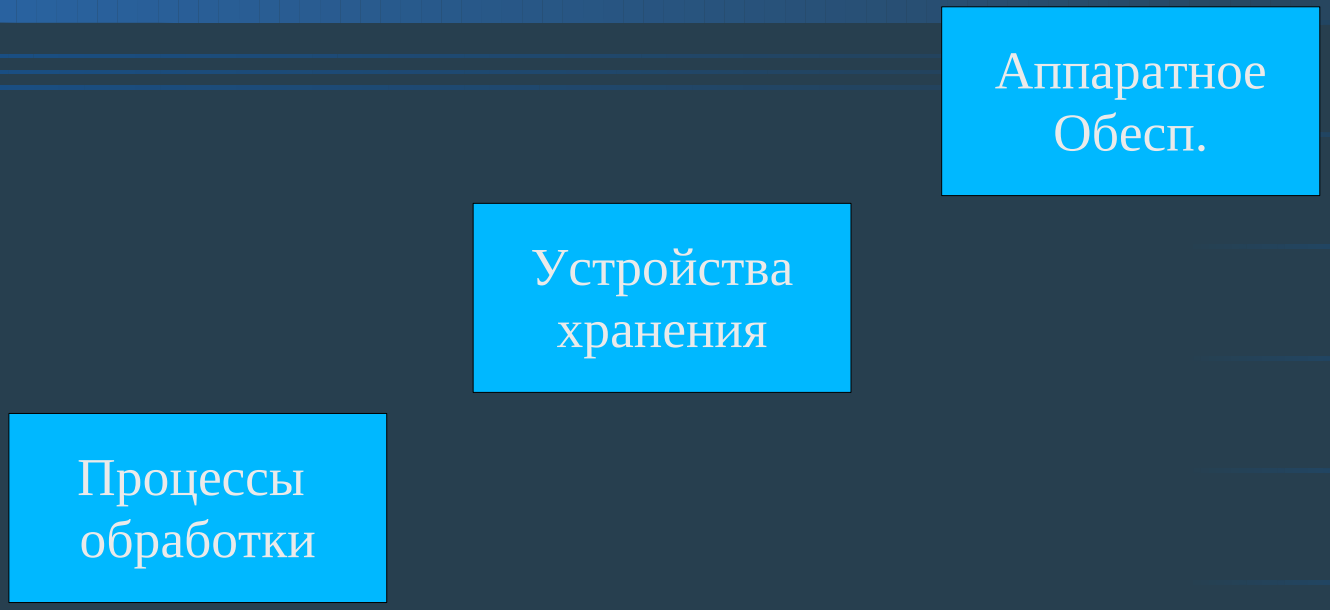
Предотвращение ошибок

- Правильное кодирование
  - Парное программирование
  - Тестирование
- Коррекция ошибок
  - Постоянное выявление и коррекция
  - Восставновление после ошибки
    - Маскирование + восстановление за счет избыточного кода
    - Восстановление корректного состояния
      - Новое
      - Возврат к предыдушему корректному

Обработка ошибок в программах

- Глобальная переменная
  - errno, _errno
- Глобальная функция
  - GetLastError()
- Код завершения
  - int dataLoad(string fileName) { .... }
- Исключения
  - throw new IncorrectParamException();

Иерархия информационной системы



Некоторые факты

- F0 0F C7 C8 — последовательность байтов, формирующих недействительную машинную команду процессоров семейства x86. В процессорах Pentium MMX и Pentium OverDrive, вследствие аппаратной недоработки, команда, будучи выполненной на любом уровне привилегий, приводила к мёртвому зависанию процессора, что отрицательно сказывалось на надёжности системы в целом.
- Маринер-1 должен был направиться к Венере, но был уничтожен во время аварии на старте в 09:26:16 UT 22 июля 1962 года через 293 секунды после старта. Антенна аппарата потеряла связь с наводящей системой на Земле, в результате управление взял на себя бортовой компьютер, программа которого содержала ошибку.
- Первый запуск новой ракеты-носителя Ариан 5 разработанного Европейским космическим агентством был произведён 4 июня 1996 года. Запуск окончился неудачей — ракета разрушилась на 39-й секунде полёта из-за неверной работы бортового программного обеспечения. Этот неудачный запуск стал одним из самых дорогостоящих компьютерных багов в истории.

Вопросы?