Внедрение шифрования в систему хранения данных высокой производительности

Выполнил:
Овчинников Антон, 345 группа

Научный руководитель:
Ершов П.А., AvroRAID,
инженер по тестированию

Задачи

- Описание требований к шифрованию в СХД
- Исследование специфики шифрования в системах хранения данных
- Описание основных принципов внедрения
- Тестирование в первом приближении

Критерии

- Высокая криптостойкость
- Без ущерба производительности
- Прозрачность для пользователей
- Минимизация накладных расходов
- Без изменения архитектуры

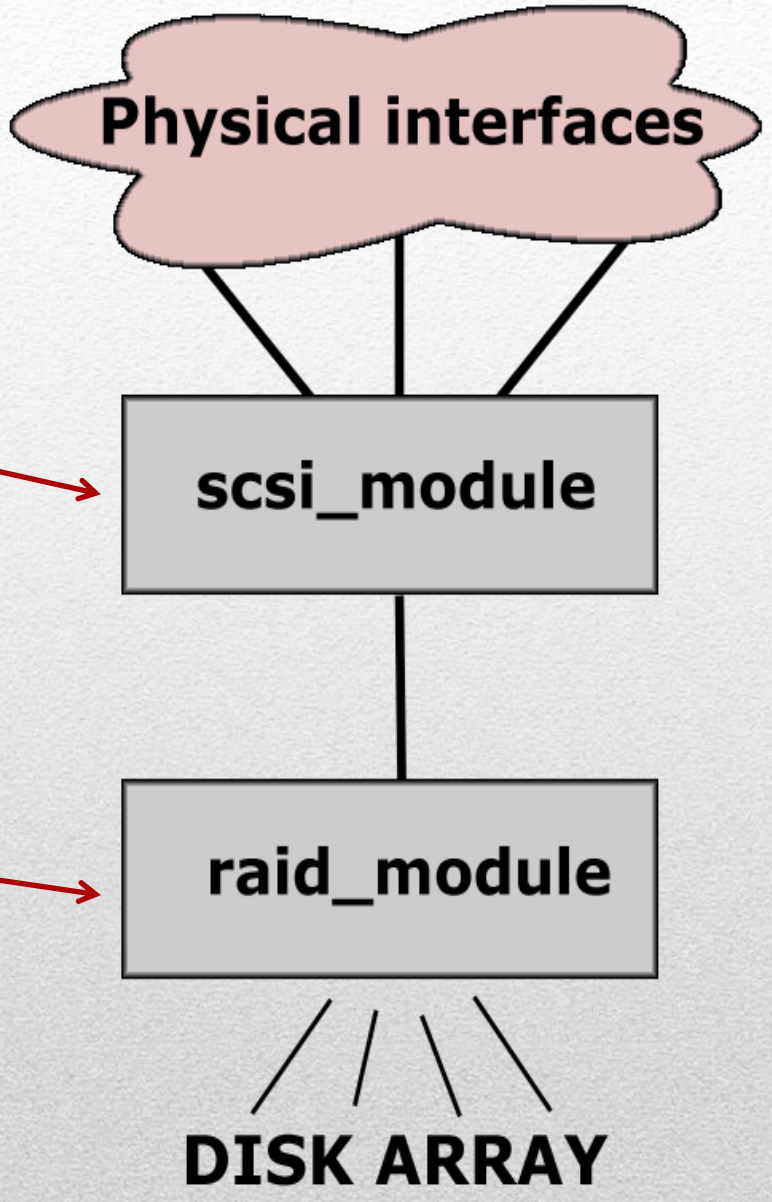
Учет специфики

СХД AVRORA

- Применение алгоритма AES
  - Аппаратная поддержка: AES-NI
- Применение специального режима XTS
- Использование спецификации LUKS (Linux Unified Key Setup)
  - Формат метаданных
  - Управление ключами

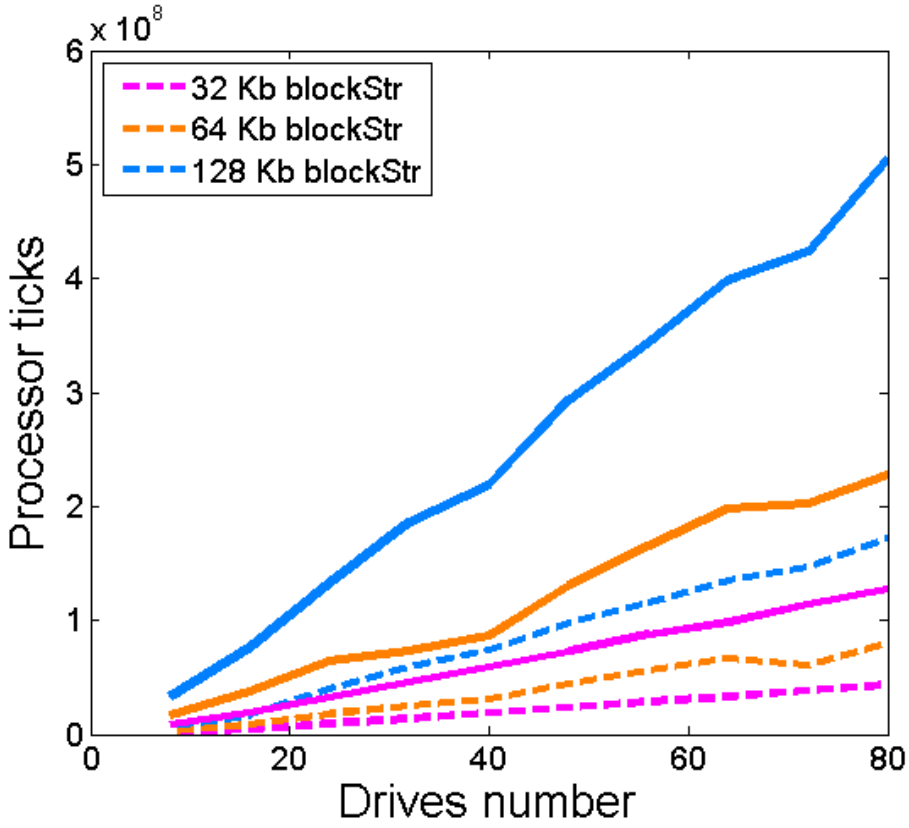
Как встраивать?

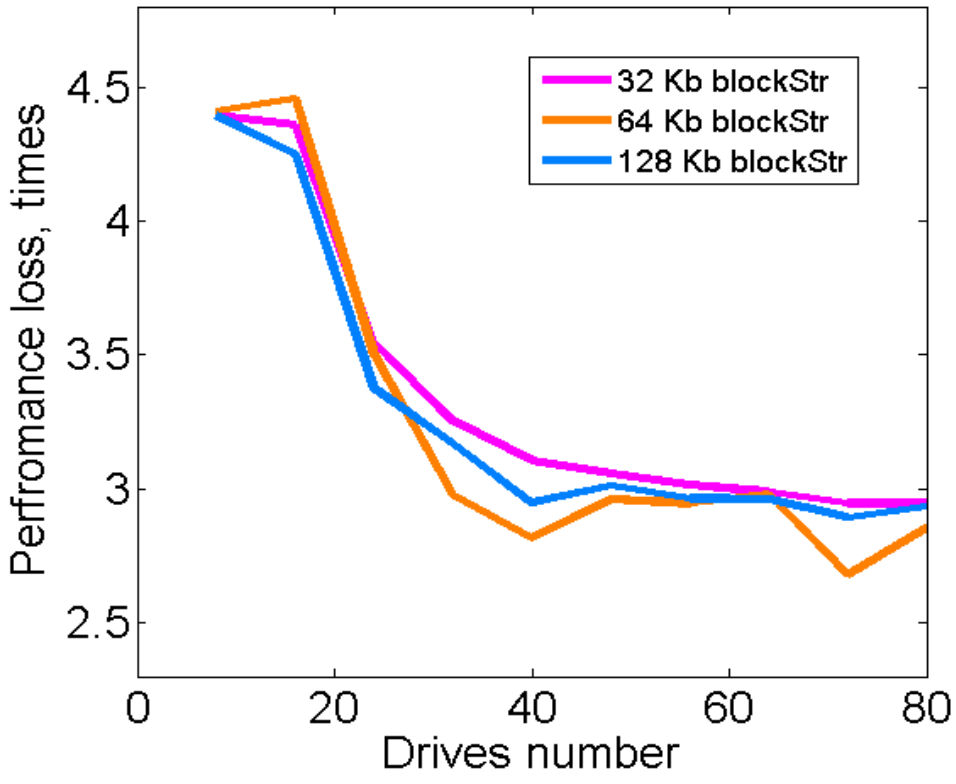
- SCSI-уровень
  - Проще: одинаково для всех типов RAID
- RAID-уровень
  - Эффективнее: не нужно пробегать по данным несколько раз



Результаты тестирования

- Отсутствие большой разницы между двумя подходами
- Нет зависимости от размера страйпа
- Максимальное падение – до 4.5 раз





Результаты и выводы

- Исследована специфика шифрования в СХД
- Реализовано шифрование AES-XTS с применением AES-NI
- Проведено тестирование в контексте RAID-6
- Шифрование теоретически не создает серьезной деградации производительности
- Достигаются поставленные требования