СКЗИ «Шифр-X.509»

Масштабирование, резервируемость, диагностика, репликация и резервное хранение данных ЦСК банков

ООО «Сайфер ЛТД», к.т.н. Влад Ковтун

Назначение системы

Система криптографической защиты информации «Шифр-X.509» предназначена для построения ЦСК:

управления персональными ключами и сертификатами для ЭЦП и шифрования информации, согласно стандарту X.509

Содержание

- Требования НБУ к ИТС ЦСК
- Краткая характеристика и архитектура ЦСК
- Масштабирование ЦСК
- Резервирование ЦСК
- Диагностика ЦСК
- Резервное хранение данных ЦСК

Предпосылки

- Постановление НБ Украины от 17.16.2004 г. №265 с изменениями согласно постановления НБ Украины от 05.04.2012 г. № 174 «**Об утверждении Положения об обеспечении непрерывного функционирования информационных систем НБ Украины и банков Украины**»
- Активная интеграция технологий X.509 в системы автоматизации банков и системы дистанционного обслуживания банков

Требования к ЦСК

- Усі вимоги цього Положення стосовно САБ поширюються також на ВМПС у разі її наявності, а також на інші комплекси програмно-апаратних засобів, призначені для розв'язання банками власних завдань у сфері автоматизації, технічної й технологічної підтримки діяльності **ЗЦ НБУ, АЦСК НБУ, ЦСК банку та завдань взаємодії з інформаційною мережею НБУ**

Требования к ЦСК

- Надежность
  - Мониторинг и диагностика
  - Резервируемость сервисов (резервные сервисы, резервный ЦОД)
  - Резервируемость и репликация данных
  - Восстановление после сбоев (резервные сервисы, резервные копии данных, резервный ЦОД)
- Производительность
  - Масштабируемость сервисов
  - Репликация данных

СКЗИ «Шифр-X.509»

ОСОБЕННОСТИ ПОСТРОЕНИЯ

Архитектура

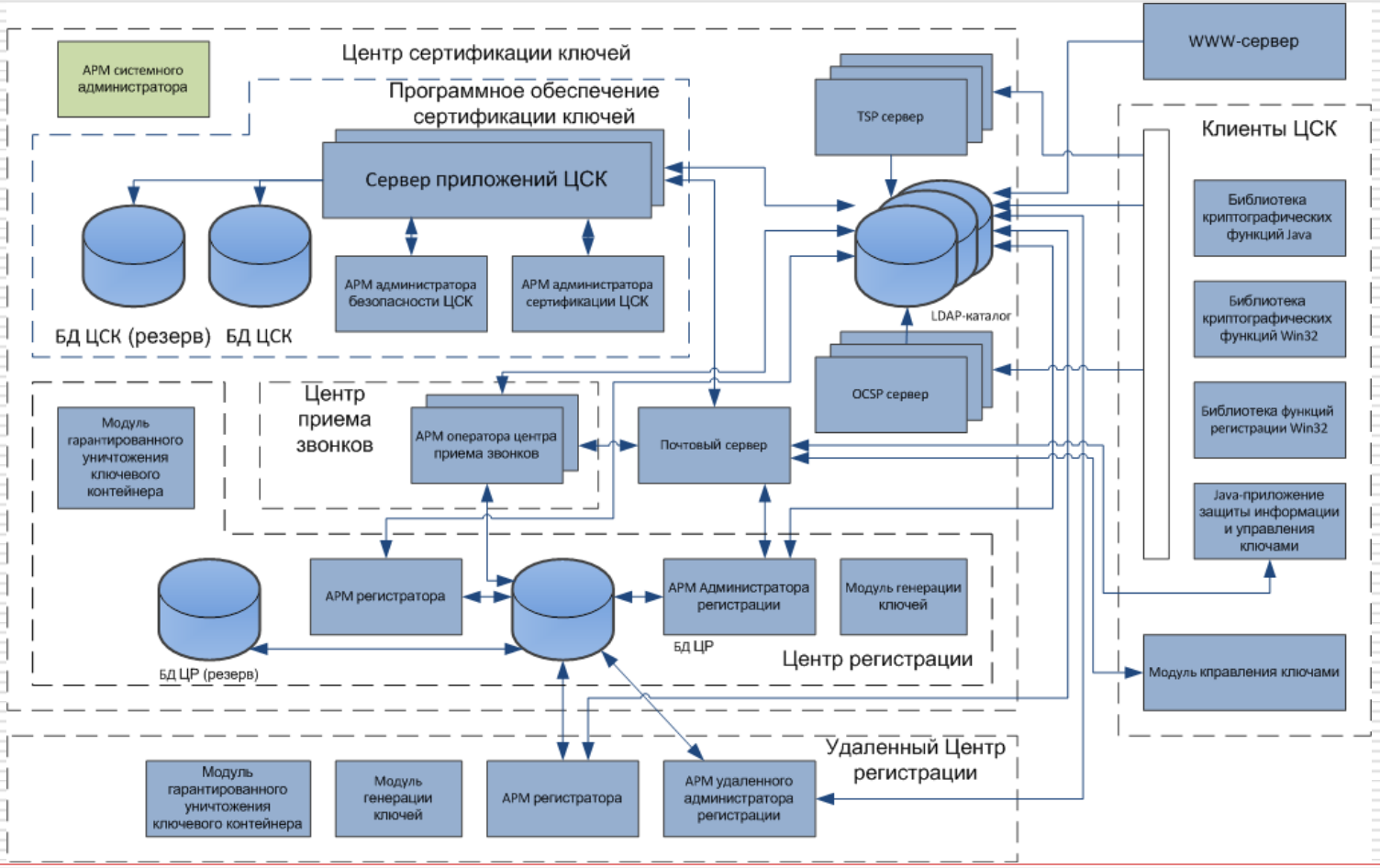


Схема развертывания (1)

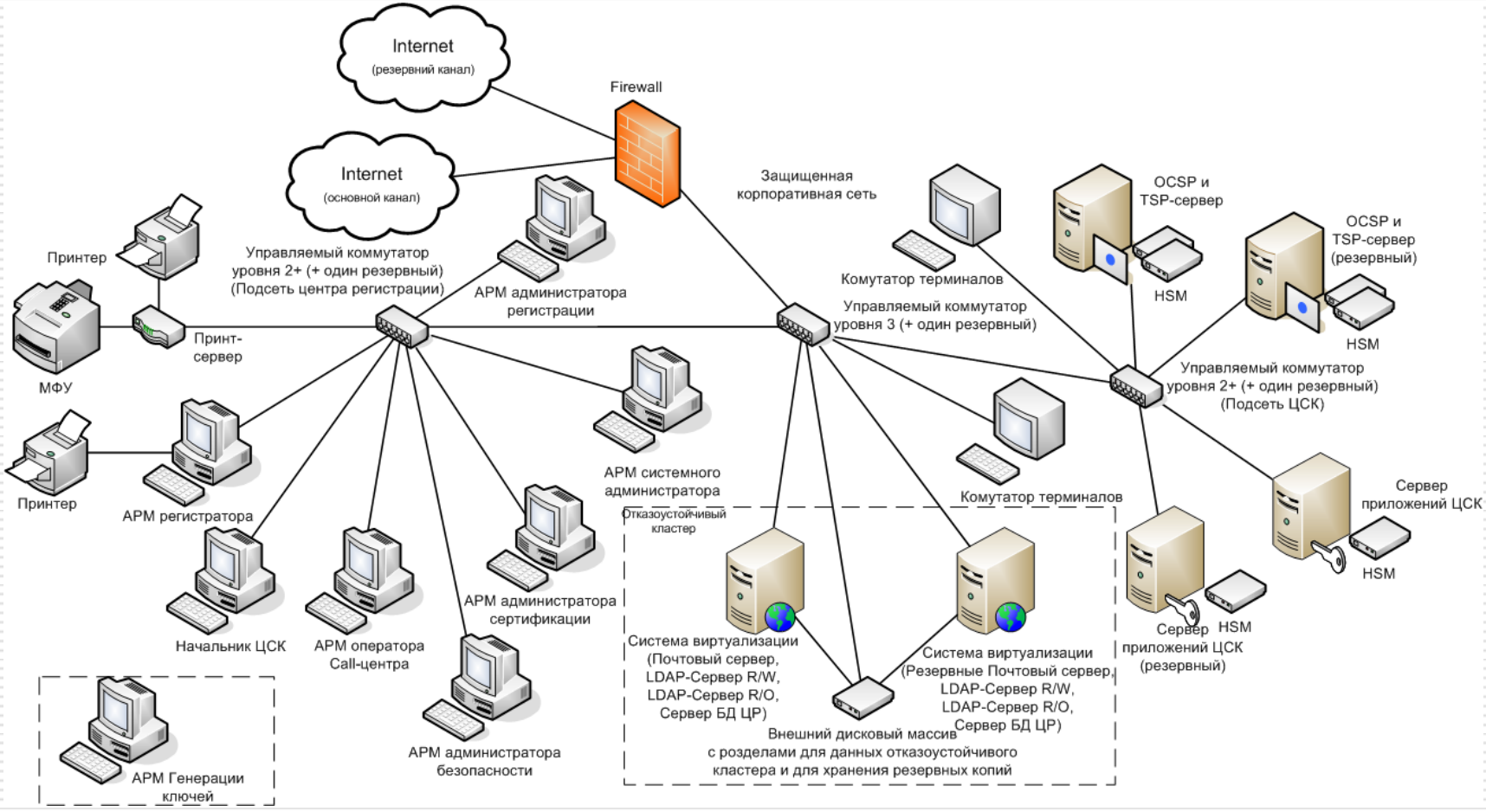
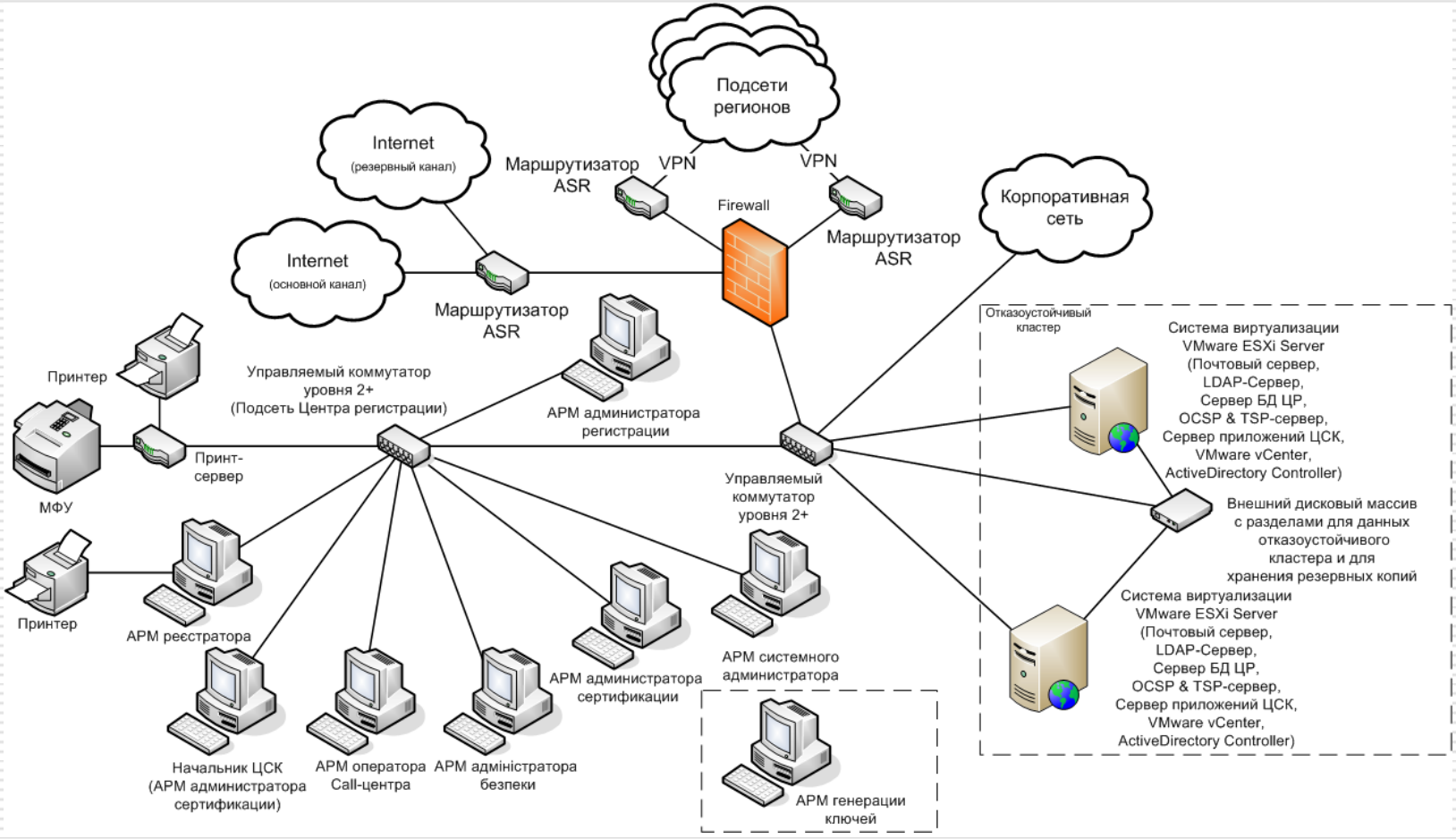


Схема развертывания (2)



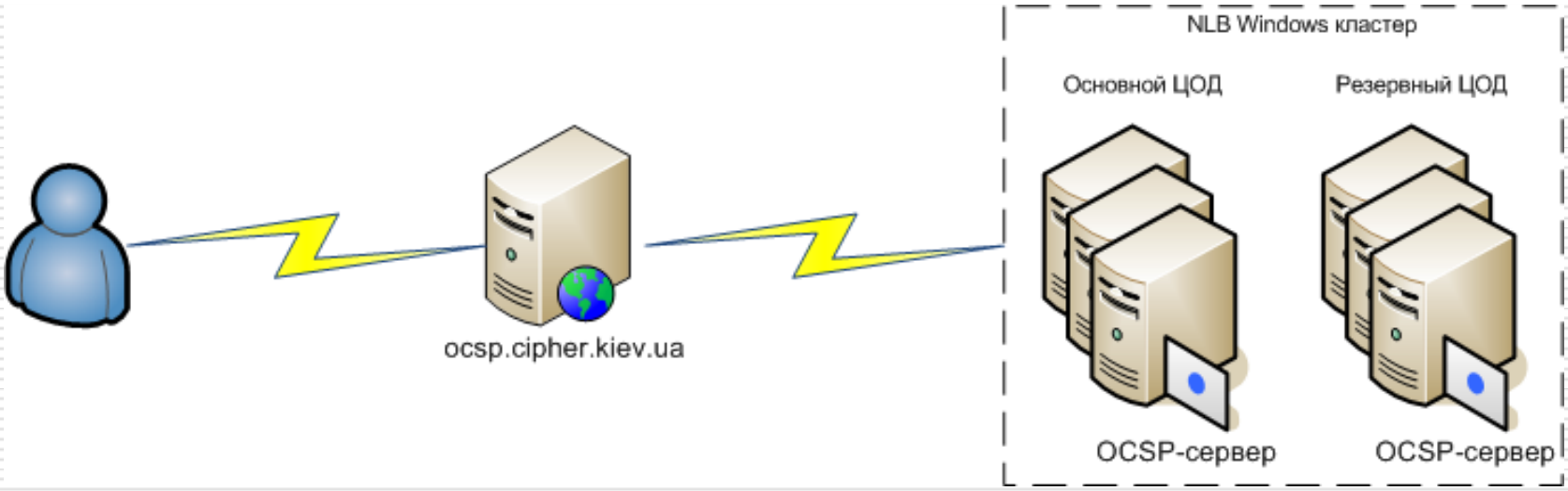
СКЗИ «Шифр-Х.509»

НАДЕЖНОСТЬ И ПРОИЗВОДИТЕЛЬНОСТЬ

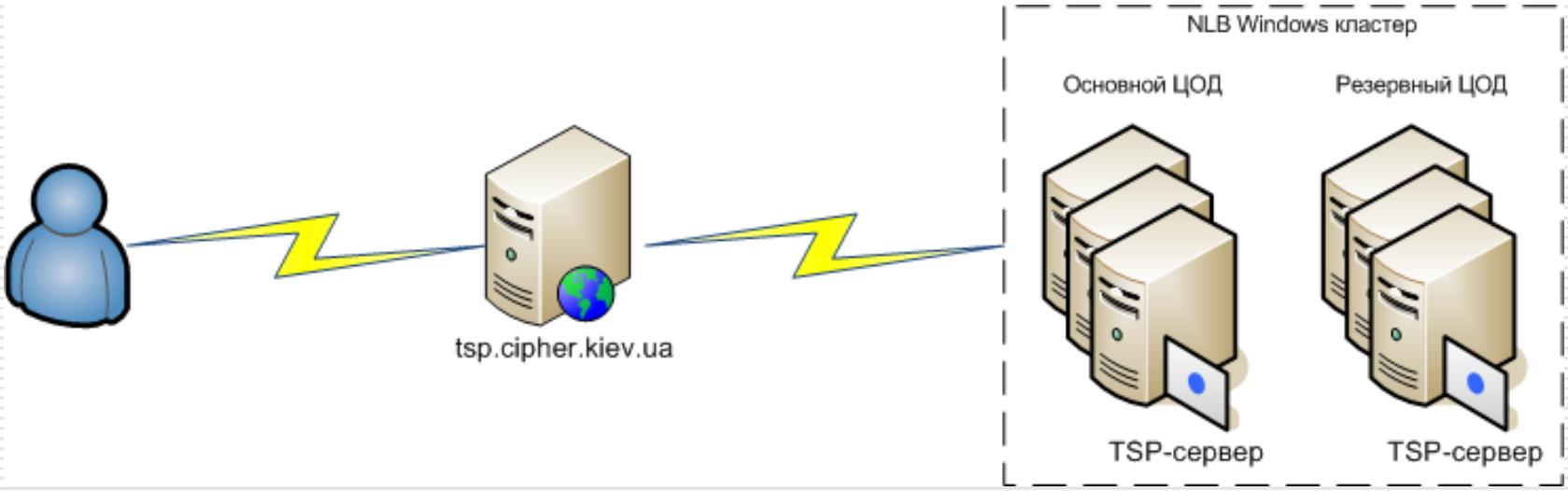
Возможности ЦСК

- Масштабирование сервисов
- Резервирование сервисов
- Мониторинг и диагностика сервисов
- Резервирование данных

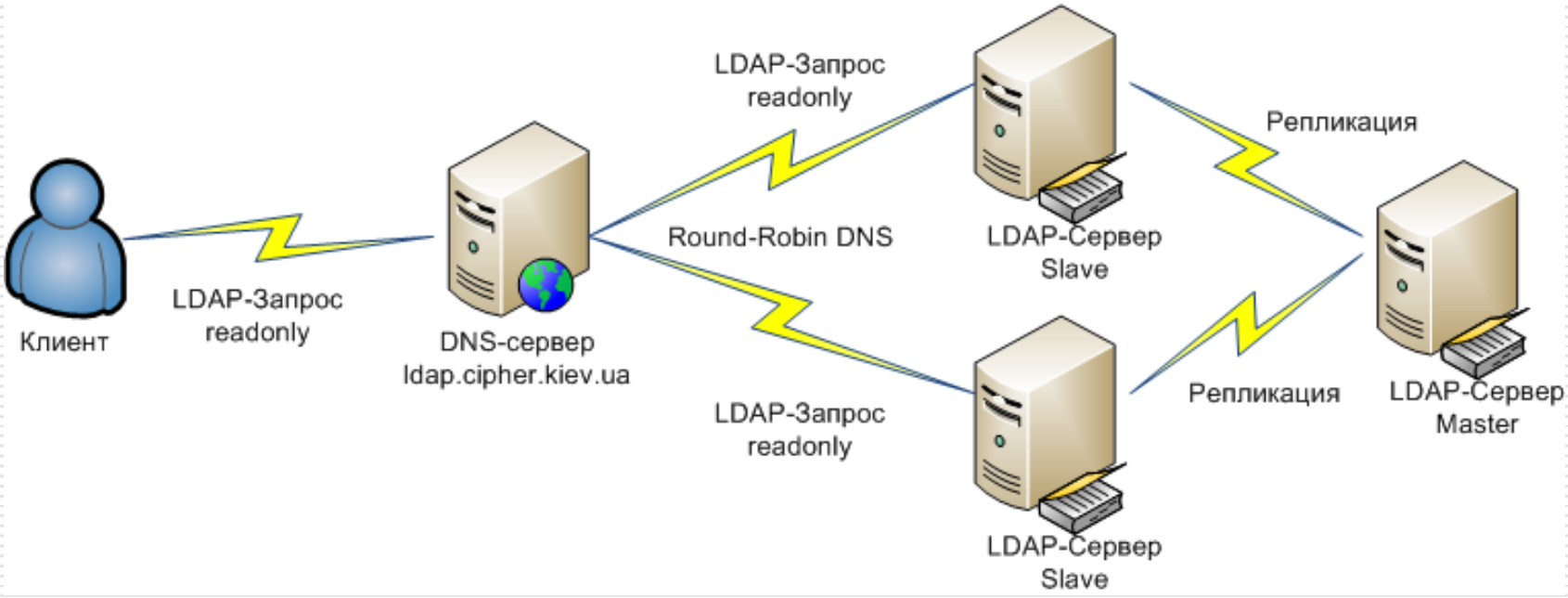
Масштабируемость OCSP



Масштабируемость TSP



Масштабируемость LDAP



Масштабируемость Сервера приложений ЦСК

Схема 1

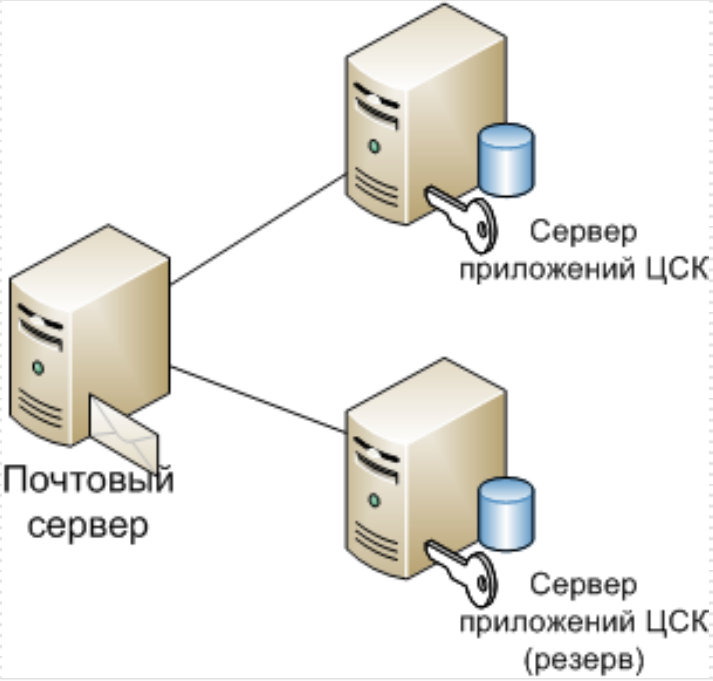
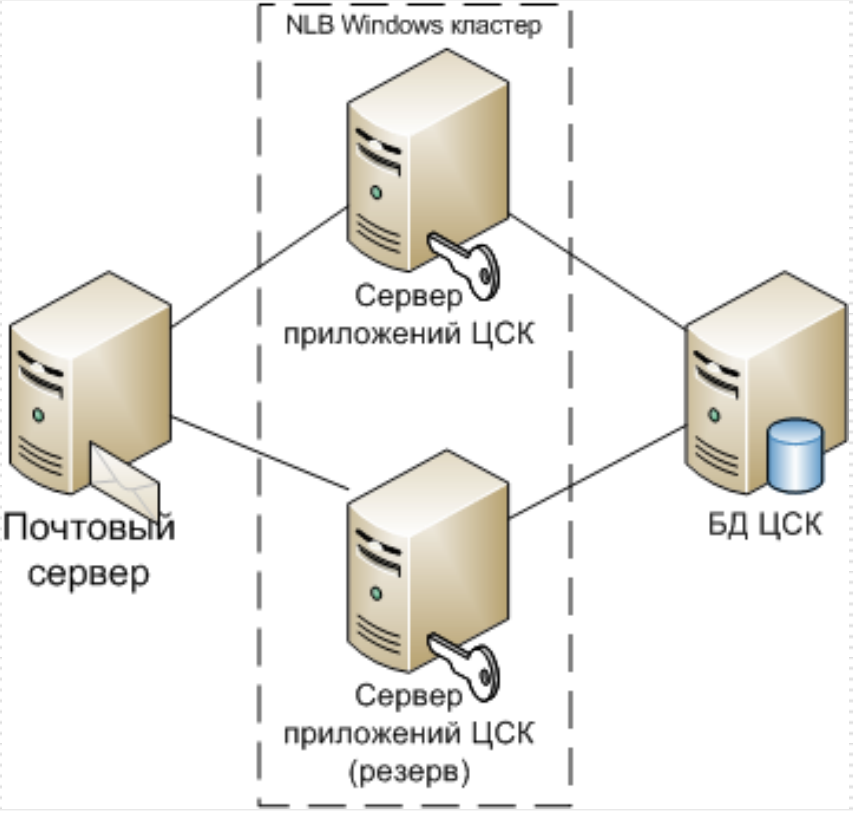
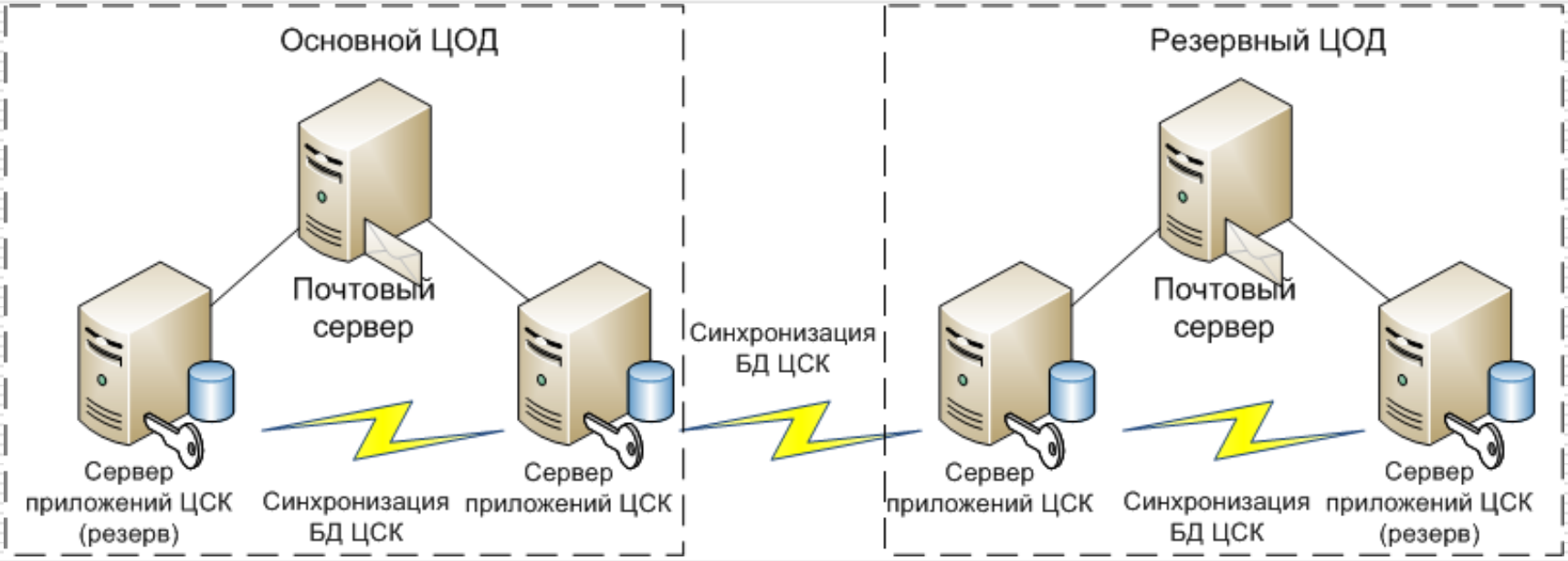


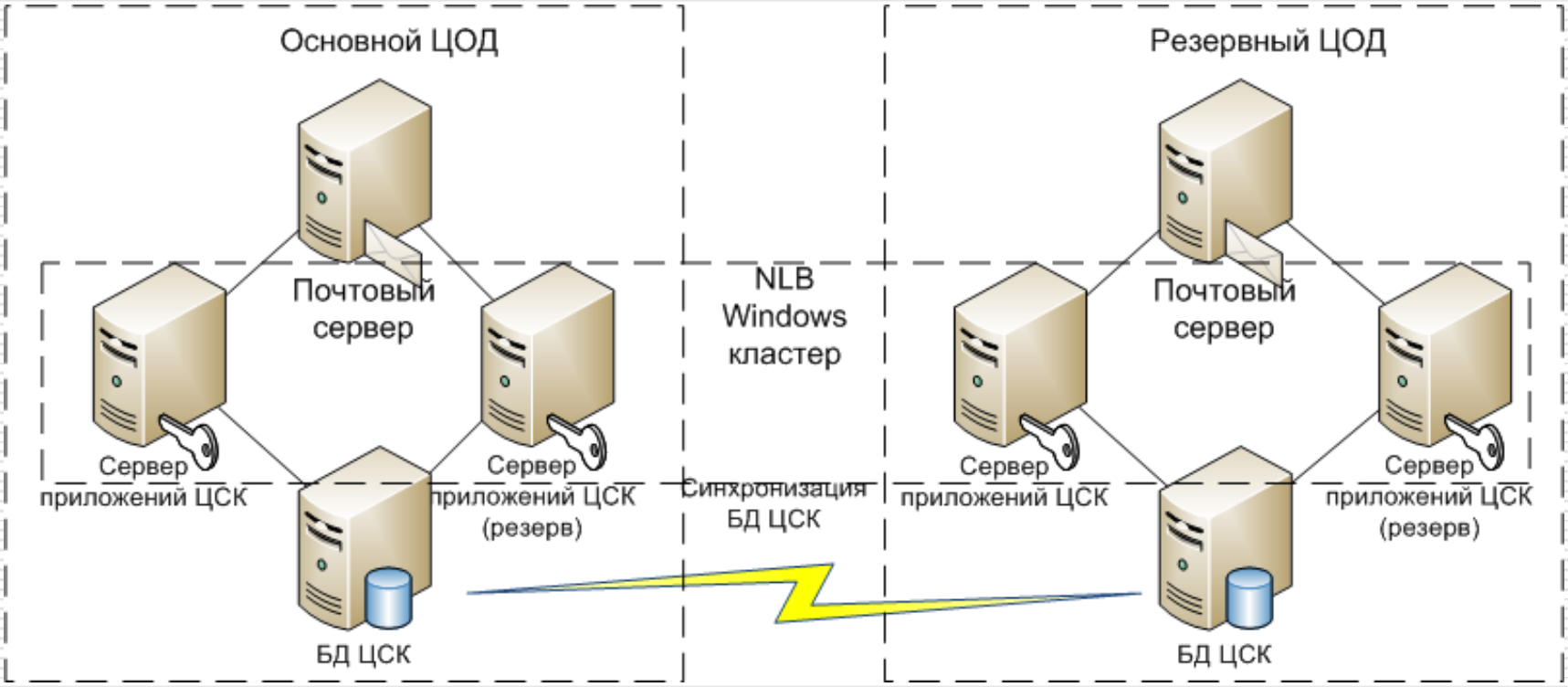
Схема 2



Масштабируемость Сервера приложений ЦСК (схема 1)



Масштабируемость Сервера приложений ЦСК (схема 2)



Мониторинг

Существующие решения:

- Nagios
- Zabbix
- Cacti
- и др.

Требуется существенная переработка:

- Целостность
- Доступность/Разграничение доступа
- Авторство
- Неотказуемость
- Диагностика/Мониторинг специфических сервисов

Мониторинг

Диагностика компонентов ЦСК (АРМ системного администратора):

- для Windows Server
  - SNMP (Informant SNMP Agent, NET-SNMP)
- для Linux Server
  - SNMP (NET-SNMP)
- Сетевое оборудование
  - SNMP

Мониторинг OCSP

- Собственные параметры SNMP
  - Подключений (всего, сейчас)
  - Состояние Listener’ов
  - Статистка успешных запросов
  - Статистика данных
  - Потоков обработки (max, сейчас)
  - Время (запуска, текущее)

Мониторинг TSP

- Собственные параметры SNMP
  - Подключений (всего, сейчас)
  - Состояние Listener’ов
  - Статистка успешных запросов
  - Статистика данных
  - Потоков обработки (max, сейчас)
  - Время (запуска, текущее)

Мониторинг сервера БД TSP

- Firebird Audit & Trace Service
  - Не зависит от платформы
  - Трассировка событий в хронологическом порядке
    - Database-specific
    - Connect, Disconnect
    - Start/Commit/Rollback of transactions
    - Prepare/Start/Finish/Free of SQL statements
    - Start/Finish of stored procedures and triggers
    - и др.

Мониторинг LDAP

- OpenLDAP Monitoring interface
  - Подключений (всего, сейчас)
  - Состояние Listener’ов
  - Статистка операций (Bind, Unbind, Add, Delete, Modify, …)
  - Статистика данных (Bytes, PDU, Entries, Referrals)
  - Потоков обработки (max, сейчас)
  - Время (запуска, текущее)

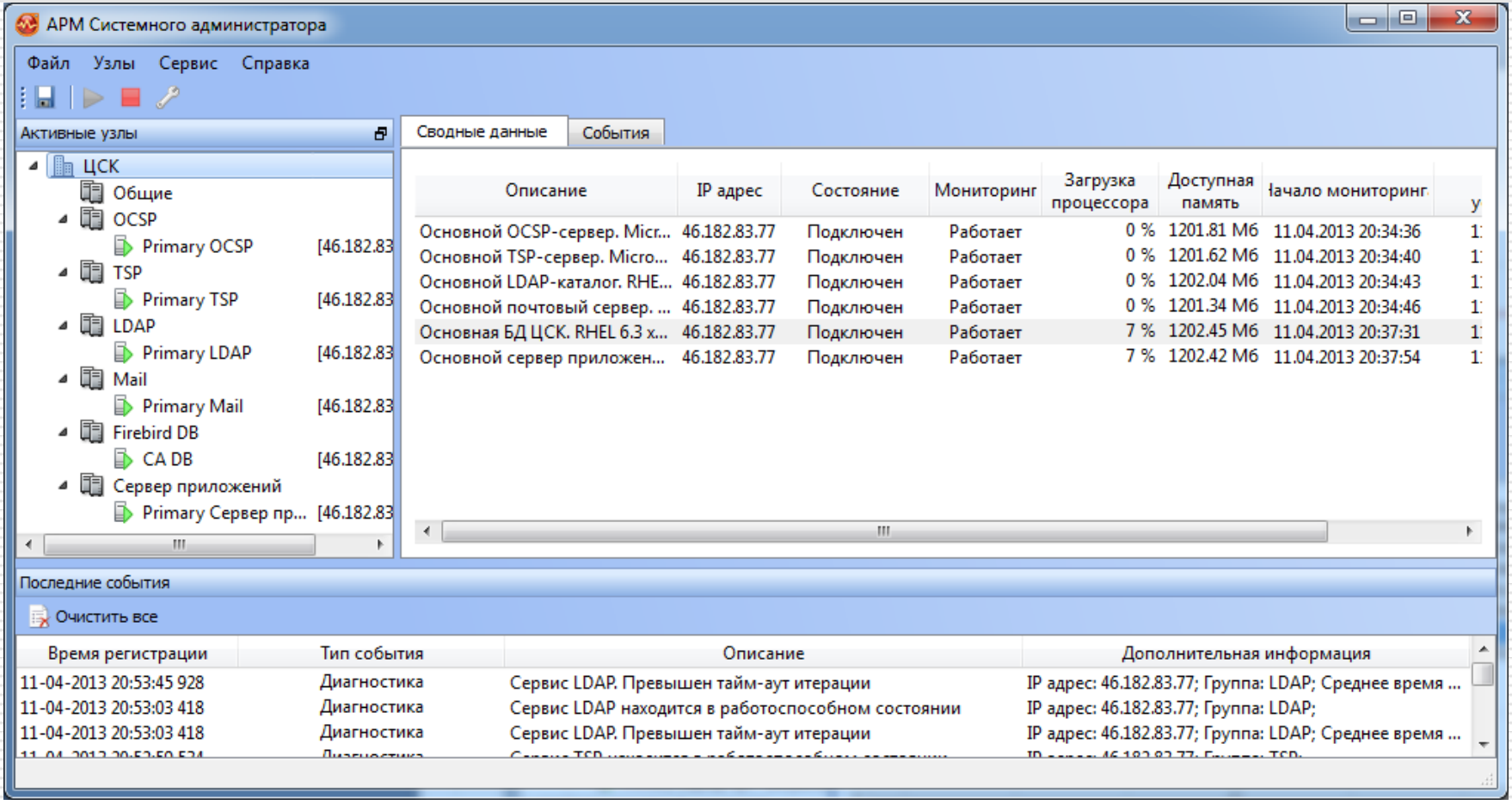
Мониторинг сервера БД ЦСК

- Firebird Audit & Trace Service
  - Не зависит от платформы
  - Трассировка событий в хронологическом порядке
    - Database-specific
    - Connect, Disconnect
    - Start/Commit/Rollback of transactions
    - Prepare/Start/Finish/Free of SQL statements
    - Start/Finish of stored procedures and triggers
    - и др.

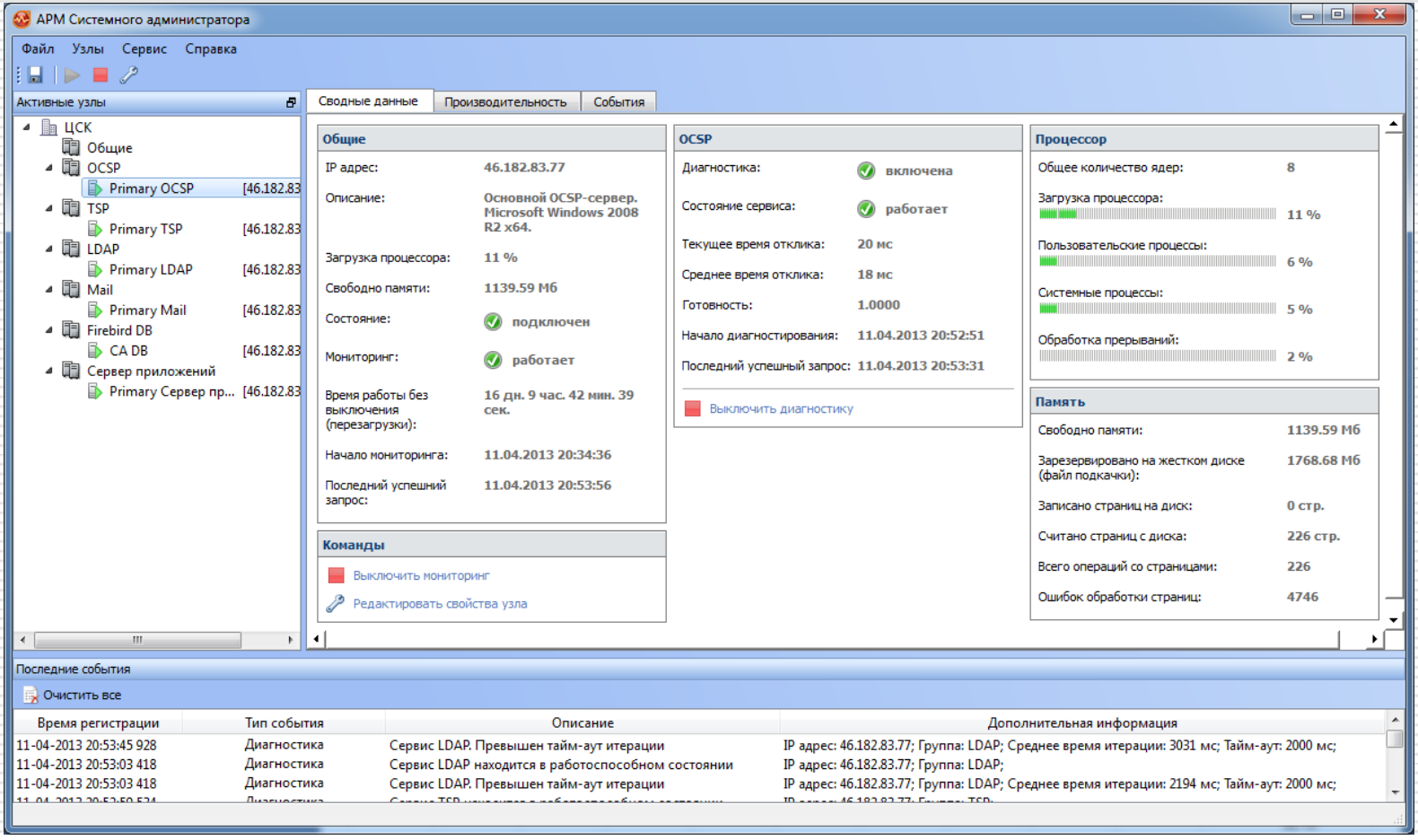
Мониторинг сервера БД ЦР

- Firebird Audit & Trace Service
  - Не зависит от платформы
  - Трассировка событий в хронологическом порядке
    - Database-specific
    - Connect, Disconnect
    - Start/Commit/Rollback of transactions
    - Prepare/Start/Finish/Free of SQL statements
    - Start/Finish of stored procedures and triggers
    - и др.

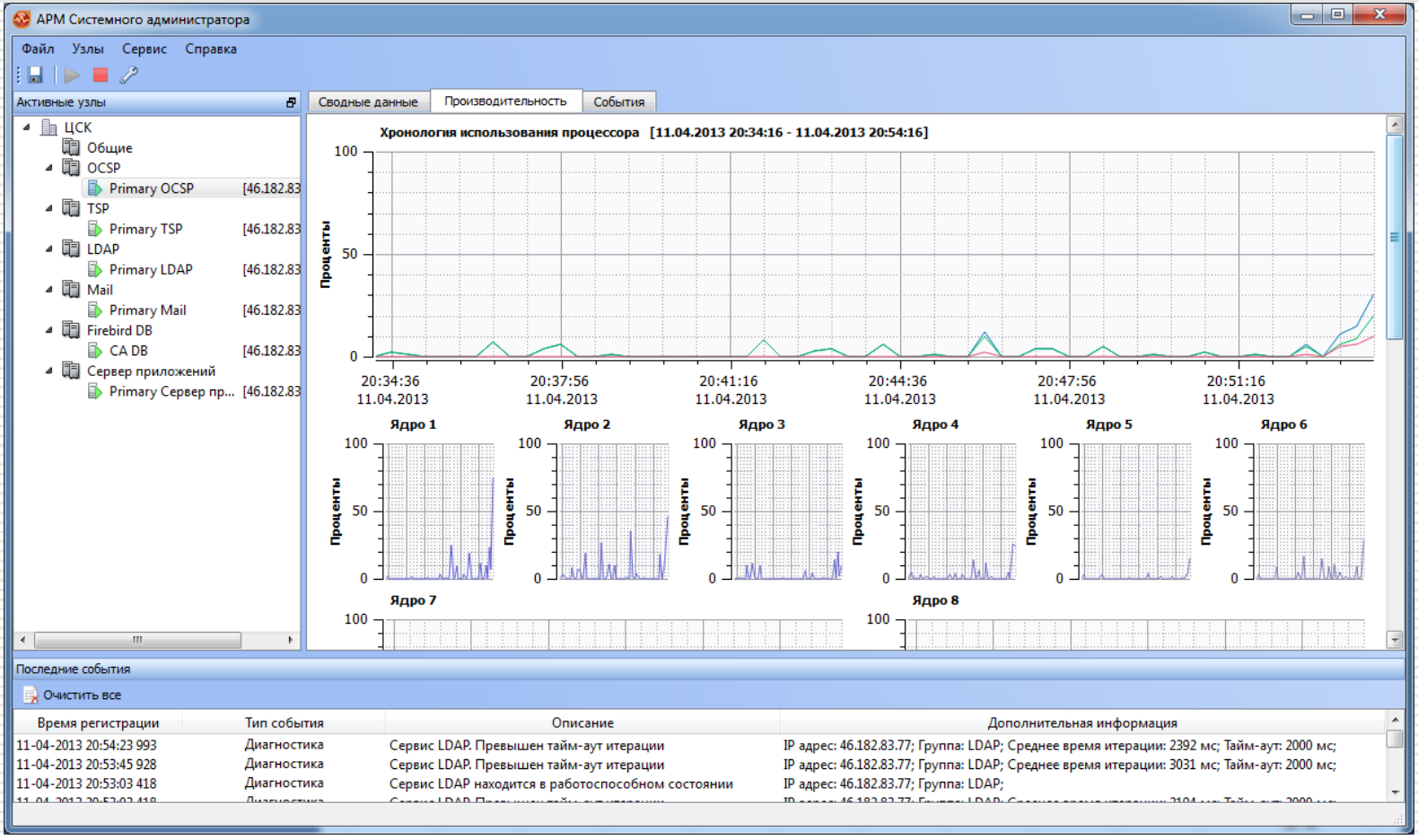
Мониторинг


АРМ Системного администратора
Файл
Узлы
Сервис
Справка
Активные узлы
ЦСК
Общие
OCSP
Primary OCSP [46.182.83
TSP
Primary TSP [46.182.83
LDAP
Primary LDAP [46.182.83
Mail
Primary Mail [46.182.83
Firebird DB
CA DB [46.182.83
Сервер приложений
Primary Сервер пр... [46.182.83
Сводные данные
События
Описание
IP адрес
Состояние
Мониторинг
Загрузка процессора
Доступная память
Начало мониторинг
Основной OCSP-сервер. Micr... 46.182.83.77 Подключен Работает 0 % 1201.81 Мб 11.04.2013 20:34:36
Основной TSP-сервер. Micro... 46.182.83.77 Подключен Работает 0 % 1201.62 Мб 11.04.2013 20:34:40
Основной LDAP-каталог. RHE... 46.182.83.77 Подключен Работает 0 % 1202.04 Мб 11.04.2013 20:34:43
Основной почтовый сервер. ... 46.182.83.77 Подключен Работает 0 % 1201.34 Мб 11.04.2013 20:34:46
Основная БД ЦСК. RHEL 6.3 x... 46.182.83.77 Подключен Работает 7 % 1202.45 Мб 11.04.2013 20:37:31
Основной сервер приложен... 46.182.83.77 Подключен Работает 7 % 1202.42 Мб 11.04.2013 20:37:54
Последние события
Очистить все
Время регистрации
Тип события
Описание
Дополнительная информация
11-04-2013 20:53:45 928 Диагностика Сервис LDAP. Превышен тайм-аут итерации IP адрес: 46.182.83.77; Группа: LDAP; Среднее время ...
11-04-2013 20:53:03 418 Диагностика Сервис LDAP находится в работоспособном состоянии IP адрес: 46.182.83.77; Группа: LDAP;
11-04-2013 20:53:03 418 Диагностика Сервис LDAP. Превышен тайм-аут итерации IP адрес: 46.182.83.77; Группа: LDAP; Среднее время ...

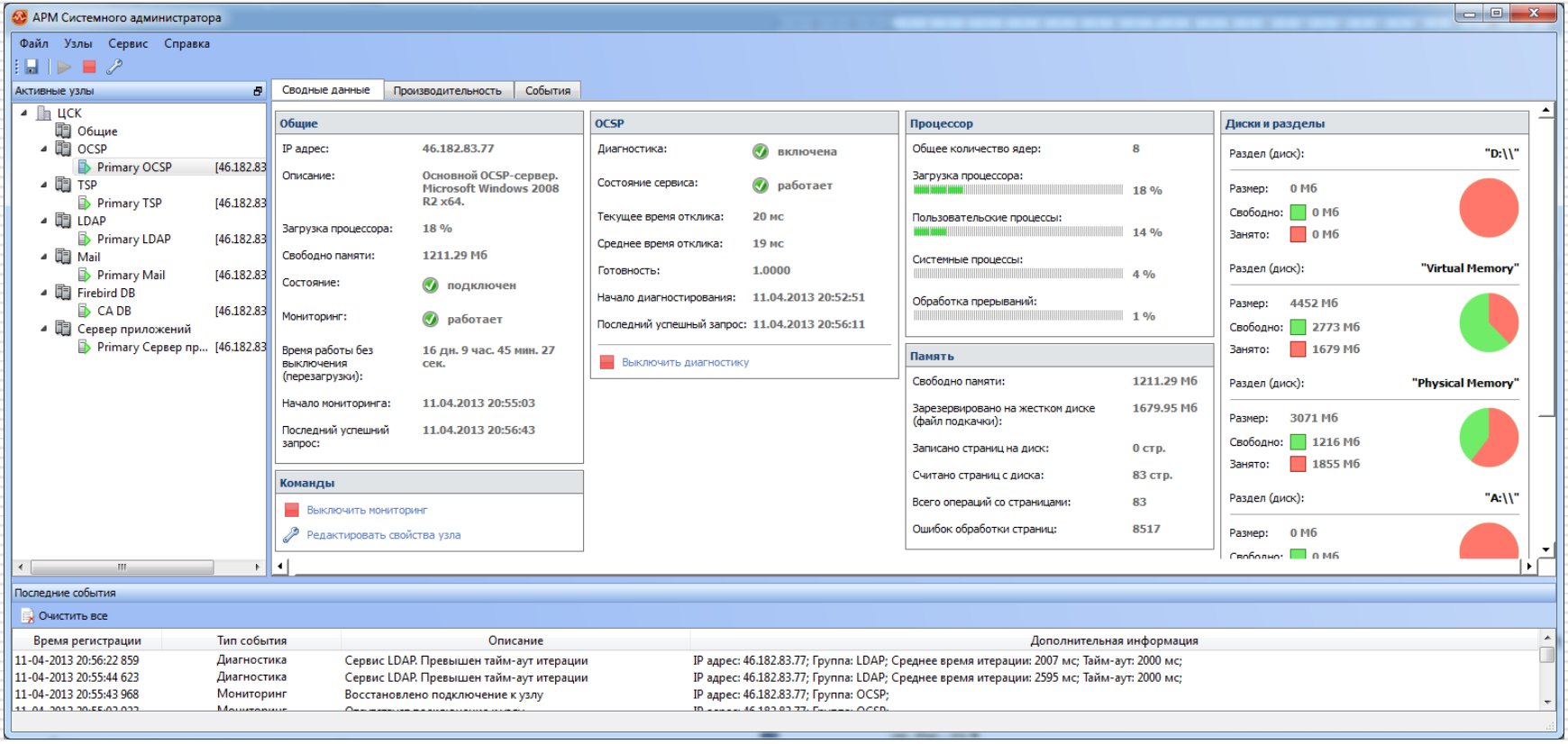
Мониторинг


АРМ Системного администратора
Файл Узлы Сервис Справка
Активные узлы
ЦСК
Общие
OCSP
Primary OCSP [46.182.83
TSP
Primary TSP [46.182.83
LDAP
Primary LDAP [46.182.83
Mail
Primary Mail [46.182.83
Firebird DB
CA DB [46.182.83
Сервер приложений
Primary Сервер пр... [46.182.83
Сводные данные
Производительность
События
Общие
IP адрес: 46.182.83.77
Описание: Основной OCSP-сервер. Microsoft Windows 2008 R2 x64.
Загрузка процессора: 11 %
Свободно памяти: 1139.59 Мб
Состояние: подключен
Мониторинг: работает
Время работы без выключения (перезагрузки): 16 дн. 9 час. 42 мин. 39 сек.
Начало мониторинга: 11.04.2013 20:34:36
Последний успешний запрос: 11.04.2013 20:53:56
Команды
Выключить мониторинг
Редактировать свойства узла
OCSP
Диагностика: включена
Состояние сервиса: работает
Текущее время отклика: 20 мс
Среднее время отклика: 18 мс
Готовность: 1.0000
Начало диагностирования: 11.04.2013 20:52:51
Последний успешный запрос: 11.04.2013 20:53:31
Выключить диагностику
Процессор
Общее количество ядер: 8
Загрузка процессора: 11 %
Пользовательские процессы: 6 %
Системные процессы: 5 %
Обработка прерываний: 2 %
Память
Свободно памяти: 1139.59 Мб
Зарезервировано на жестком диске (файл подкачки): 1768.68 Мб
Записано страниц на диск: 0 стр.
Считано страниц с диска: 226 стр.
Всего операций со страницами: 226
Ошибок обработки страниц: 4746
Последние события
Очистить все
Время регистрации
Тип события
Описание
Дополнительная информация
11-04-2013 20:53:45 928 Диагностика Сервис LDAP. Превышен тайм-аут итерации IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 3031 мс; Тайм-аут: 2000 мс;
11-04-2013 20:53:03 418 Диагностика Сервис LDAP находится в работоспособном состоянии IP адрес: 46.182.83.77; Группа: LDAP;
11-04-2013 20:53:03 418 Диагностика Сервис LDAP. Превышен тайм-аут итерации IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 2194 мс; Тайм-аут: 2000 мс;

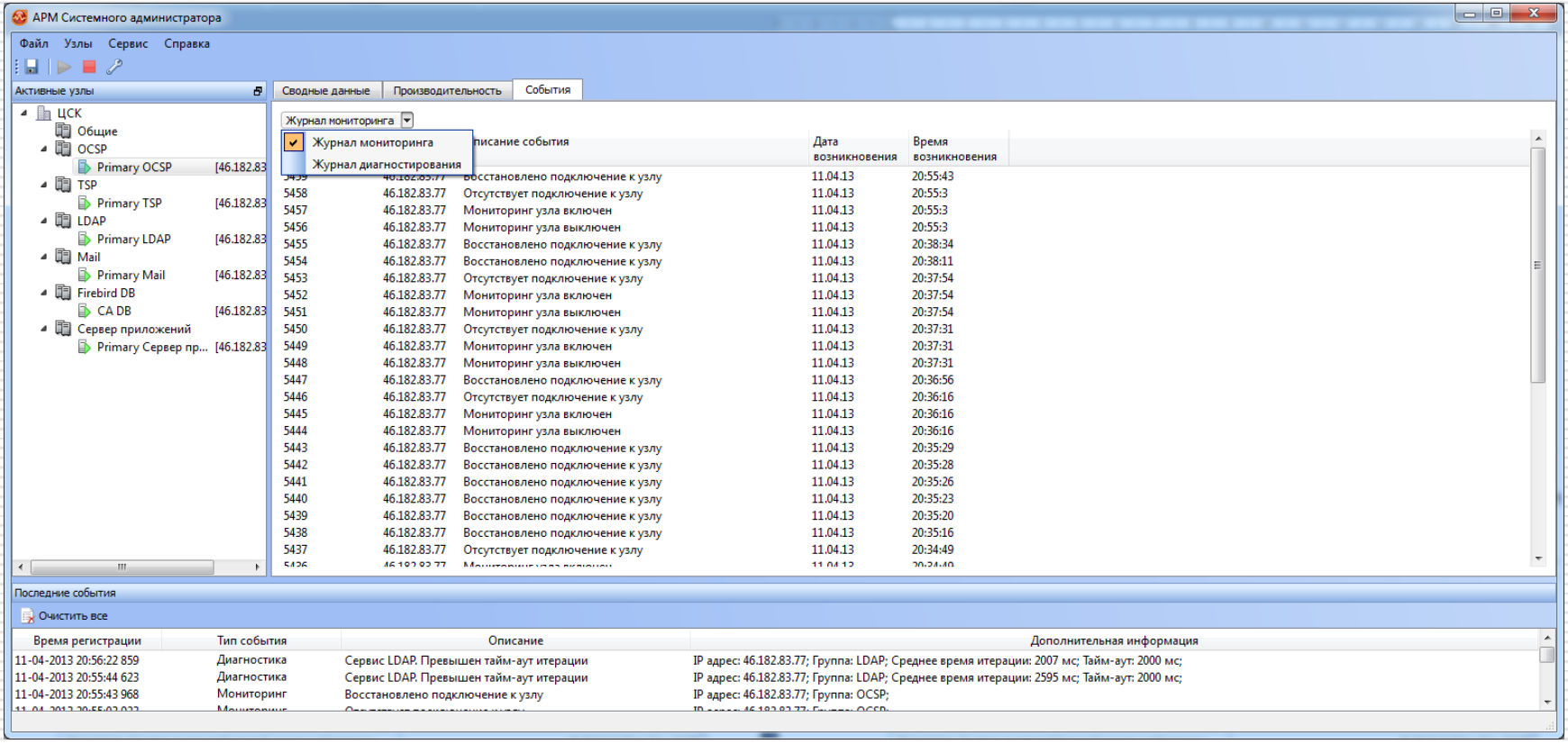
Мониторинг


АРМ Системного администратора
Файл Узлы Сервис Справка
Активные узлы
ЦСК
Общие
OCSP
Primary OCSP [46.182.83
TSP
Primary TSP [46.182.83
LDAP
Primary LDAP [46.182.83
Mail
Primary Mail [46.182.83
Firebird DB
CA DB [46.182.83
Сервер приложений
Primary Сервер пр... [46.182.83
Сводные данные
Производительность
События
Хронология использования процессора [11.04.2013 20:34:16 - 11.04.2013 20:54:16]
Проценты
100
50
0
20:34:36 11.04.2013
20:37:56 11.04.2013
20:41:16 11.04.2013
20:44:36 11.04.2013
20:47:56 11.04.2013
20:51:16 11.04.2013
Ядро 1
Ядро 2
Ядро 3
Ядро 4
Ядро 5
Ядро 6
Ядро 7
Ядро 8
Последние события
Очистить все
Время регистрации
Тип события
Описание
Дополнительная информация
11-04-2013 20:54:23 993
Диагностика
Сервис LDAP. Превышен тайм-аут итерации
IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 2392 мс; Тайм-аут: 2000 мс;
11-04-2013 20:53:45 928
Диагностика
Сервис LDAP. Превышен тайм-аут итерации
IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 3031 мс; Тайм-аут: 2000 мс;
11-04-2013 20:53:03 418
Диагностика
Сервис LDAP находится в работоспособном состоянии
IP адрес: 46.182.83.77; Группа: LDAP;

Мониторинг


АРМ Системного администратора
Файл Узлы Сервис Справка
Активные узлы
ЦСК
Общие
OCSP
Primary OCSP [46.182.83
TSP
Primary TSP [46.182.83
LDAP
Primary LDAP [46.182.83
Mail
Primary Mail [46.182.83
Firebird DB
CA DB [46.182.83
Сервер приложений
Primary Сервер пр... [46.182.83
Сводные данные
Производительность
События
Общие
IP адрес: 46.182.83.77
Описание: Основной OCSP-сервер. Microsoft Windows 2008 R2 x64.
Загрузка процессора: 18 %
Свободно памяти: 1211.29 Мб
Состояние: подключен
Мониторинг: работает
Время работы без выключения (перезагрузки): 16 дн. 9 час. 45 мин. 27 сек.
Начало мониторинга: 11.04.2013 20:55:03
Последний успешный запрос: 11.04.2013 20:56:43
Команды
Выключить мониторинг
Редактировать свойства узла
OCSP
Диагностика: включена
Состояние сервиса: работает
Текущее время отклика: 20 мс
Среднее время отклика: 19 мс
Готовность: 1.0000
Начало диагностирования: 11.04.2013 20:52:51
Последний успешный запрос: 11.04.2013 20:56:11
Выключить диагностику
Процессор
Общее количество ядер: 8
Загрузка процессора: 18 %
Пользовательские процессы: 14 %
Системные процессы: 4 %
Обработка прерываний: 1 %
Память
Свободно памяти: 1211.29 Мб
Зарезервировано на жестком диске (файл подкачки): 1679.95 Мб
Записано страниц на диск: 0 стр.
Считано страниц с диска: 83 стр.
Всего операций со страницами: 83
Ошибок обработки страниц: 8517
Диски и разделы
Раздел (диск): "D:\\"
Размер: 0 Мб
Свободно: 0 Мб
Занято: 0 Мб
Раздел (диск): "Virtual Memory"
Размер: 4452 Мб
Свободно: 2773 Мб
Занято: 1679 Мб
Раздел (диск): "Physical Memory"
Размер: 3071 Мб
Свободно: 1216 Мб
Занято: 1855 Мб
Раздел (диск): "A:\\"
Размер: 0 Мб
Последние события
Очистить все
Время регистрации
Тип события
Описание
Дополнительная информация
11-04-2013 20:56:22 859 Диагностика Сервис LDAP. Превышен тайм-аут итерации IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 2007 мс; Тайм-аут: 2000 мс;
11-04-2013 20:55:44 623 Диагностика Сервис LDAP. Превышен тайм-аут итерации IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 2595 мс; Тайм-аут: 2000 мс;
11-04-2013 20:55:43 968 Мониторинг Восстановлено подключение к узлу IP адрес: 46.182.83.77; Группа: OCSP;

Мониторинг


АРМ Системного администратора
Файл Узлы Сервис Справка
Активные узлы
ЦСК
Общие
OCSP
Primary OCSP [46.182.83
TSP
Primary TSP [46.182.83
LDAP
Primary LDAP [46.182.83
Mail
Primary Mail [46.182.83
Firebird DB
CA DB [46.182.83
Сервер приложений
Primary Сервер пр... [46.182.83
Сводные данные
Производительность
События
Журнал мониторинга
Журнал мониторинга
Журнал диагностирования
Описание события
Дата возникновения
Время возникновения
5458 46.182.83.77 Отсутствует подключение к узлу 11.04.13 20:55:3
5457 46.182.83.77 Мониторинг узла включен 11.04.13 20:55:3
5456 46.182.83.77 Мониторинг узла выключен 11.04.13 20:55:3
5455 46.182.83.77 Восстановлено подключение к узлу 11.04.13 20:38:34
5454 46.182.83.77 Восстановлено подключение к узлу 11.04.13 20:38:11
5453 46.182.83.77 Отсутствует подключение к узлу 11.04.13 20:37:54
5452 46.182.83.77 Мониторинг узла включен 11.04.13 20:37:54
5451 46.182.83.77 Мониторинг узла выключен 11.04.13 20:37:54
5450 46.182.83.77 Отсутствует подключение к узлу 11.04.13 20:37:31
5449 46.182.83.77 Мониторинг узла включен 11.04.13 20:37:31
5448 46.182.83.77 Мониторинг узла выключен 11.04.13 20:37:31
5447 46.182.83.77 Восстановлено подключение к узлу 11.04.13 20:36:56
5446 46.182.83.77 Отсутствует подключение к узлу 11.04.13 20:36:16
5445 46.182.83.77 Мониторинг узла включен 11.04.13 20:36:16
5444 46.182.83.77 Мониторинг узла выключен 11.04.13 20:36:16
5443 46.182.83.77 Восстановлено подключение к узлу 11.04.13 20:35:29
5442 46.182.83.77 Восстановлено подключение к узлу 11.04.13 20:35:28
5441 46.182.83.77 Восстановлено подключение к узлу 11.04.13 20:35:26
5440 46.182.83.77 Восстановлено подключение к узлу 11.04.13 20:35:23
5439 46.182.83.77 Восстановлено подключение к узлу 11.04.13 20:35:20
5438 46.182.83.77 Восстановлено подключение к узлу 11.04.13 20:35:16
5437 46.182.83.77 Отсутствует подключение к узлу 11.04.13 20:34:49
Последние события
Очистить все
Время регистрации
Тип события
Описание
Дополнительная информация
11-04-2013 20:56:22 859 Диагностика Сервис LDAP. Превышен тайм-аут итерации IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 2007 мс; Тайм-аут: 2000 мс;
11-04-2013 20:55:44 623 Диагностика Сервис LDAP. Превышен тайм-аут итерации IP адрес: 46.182.83.77; Группа: LDAP; Среднее время итерации: 2595 мс; Тайм-аут: 2000 мс;
11-04-2013 20:55:43 968 Мониторинг Восстановлено подключение к узлу IP адрес: 46.182.83.77; Группа: OCSP;

Диагностика

Диагностика служб ЦСК (АРМ системного администратора):

- LDAP-сервер
- OCSP-сервер
- TSP-сервер
- Сервер приложений ЦСК
- Почтовый сервер
- WWW-сервер

Диагностика OCSP

- Диагностические запросы - время отклика
  - Подключение
  - Запрос на статус одного сертификата
  - Запрос на статус пакета сертификатов

Диагностика TSP

- Диагностические запросы - время отклика
  - Подключение
  - Запрос на метку времени
  - Запрос на пакет меток времени

Диагностика LDAP

- Диагностические запросы - время отклика
  - Master (чтение, запись, поиск)
  - Slave (чтение, поиск)

Диагностика сервера приложений ЦСК

- Диагностические запросы - время отклика
  - Подключение
  - Передача тестового запроса на сертификат (тестовый профиль)
  - Прием тестового сертификата* (тестовый профиль)

*Не сохраняются в БД ЦСК и LDAP

Диагностика сервера БД ЦСК

- Диагностические запросы - время отклика
  - Подключение
  - Тестовый поисковый запрос

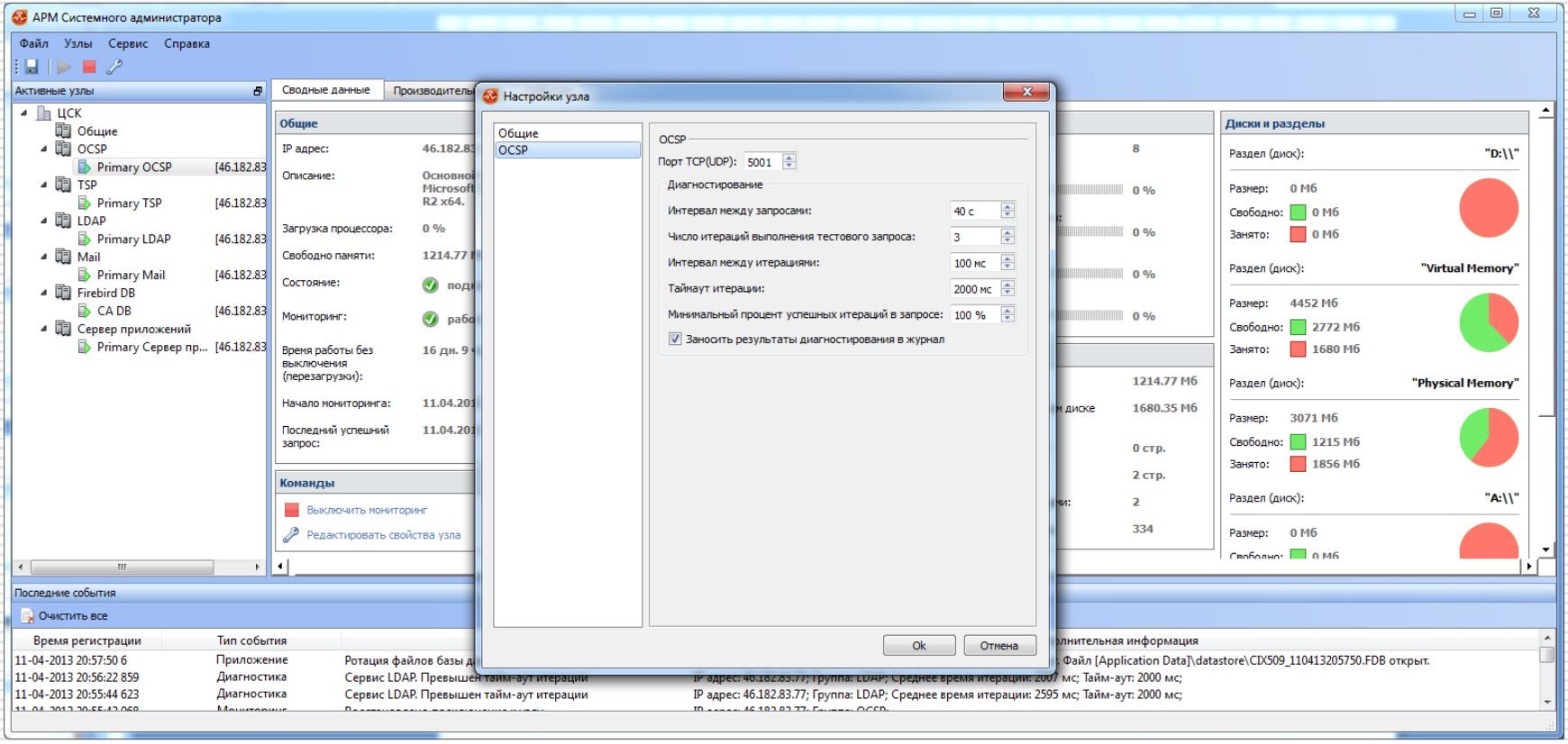
Диагностика сервера БД ЦР

- Диагностические запросы - время отклика
  - Подключение
  - Тестовый поисковый запрос

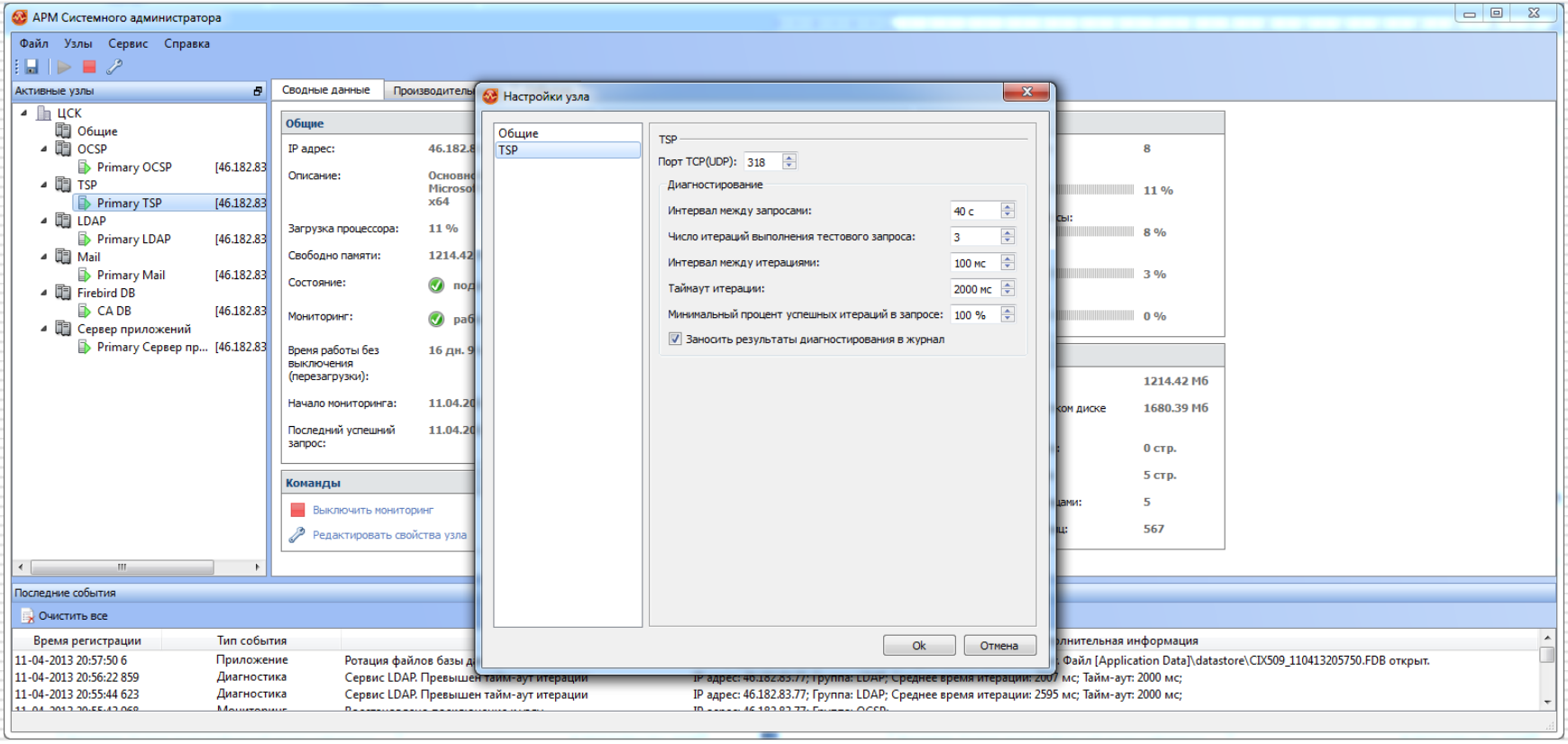
Диагностика почтового сервера

- Диагностические запросы - время отклика
  - Отправка тестового почтового сообщения «сам на себя»
  - Прием тестового почтового сообщения «сам на себя»

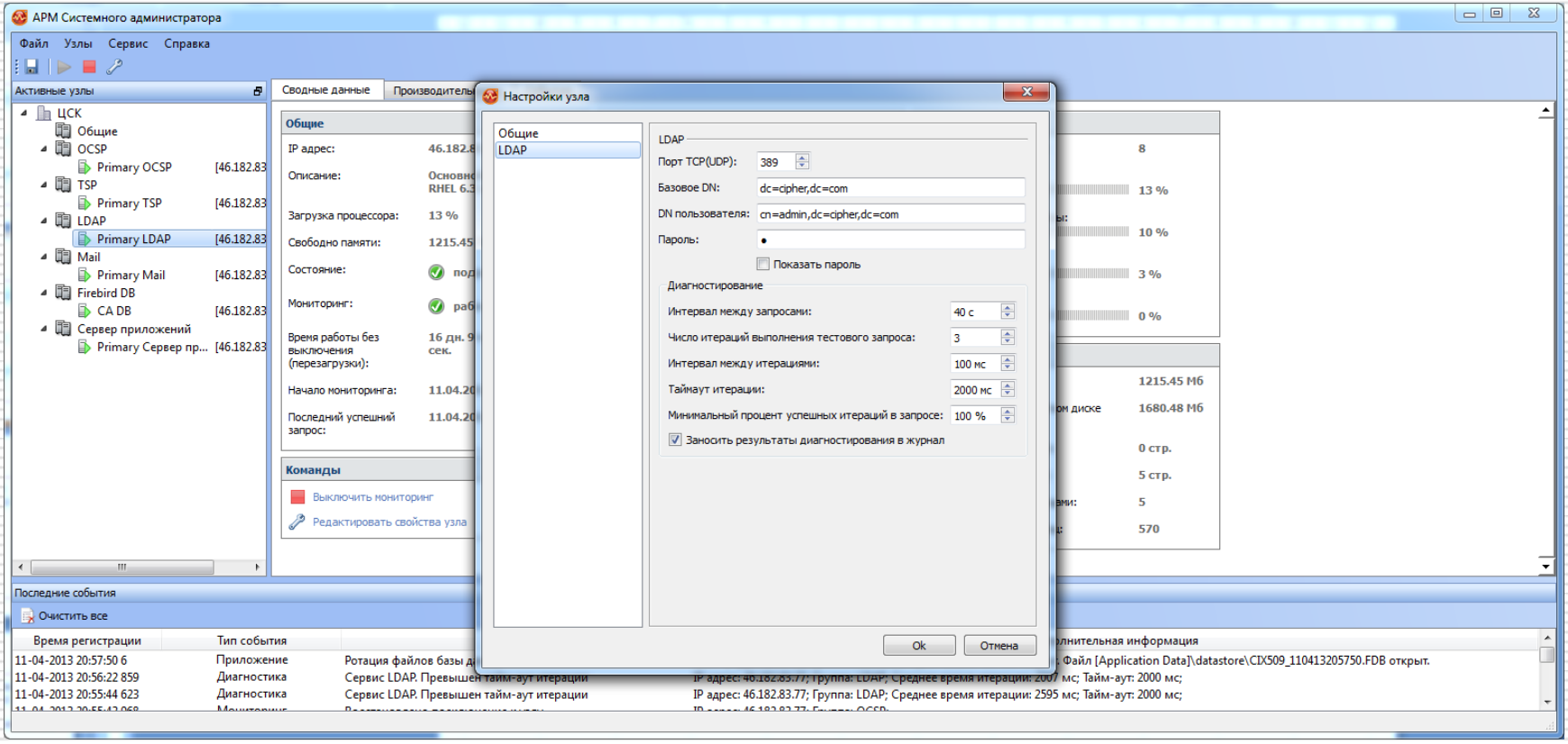
Диагностика OCSP



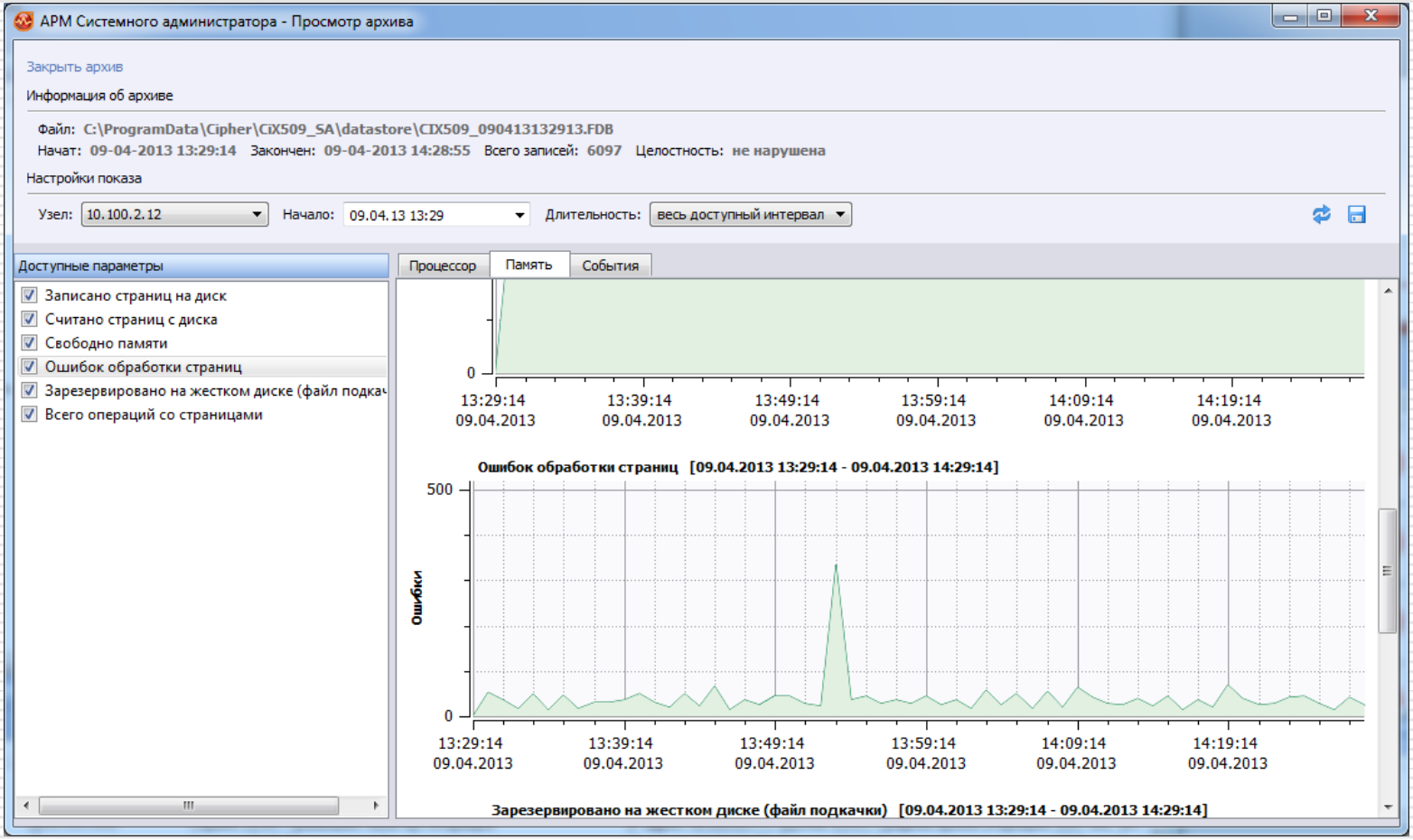
Диагностика TSP



Диагностика LDAP



Работа с архивом



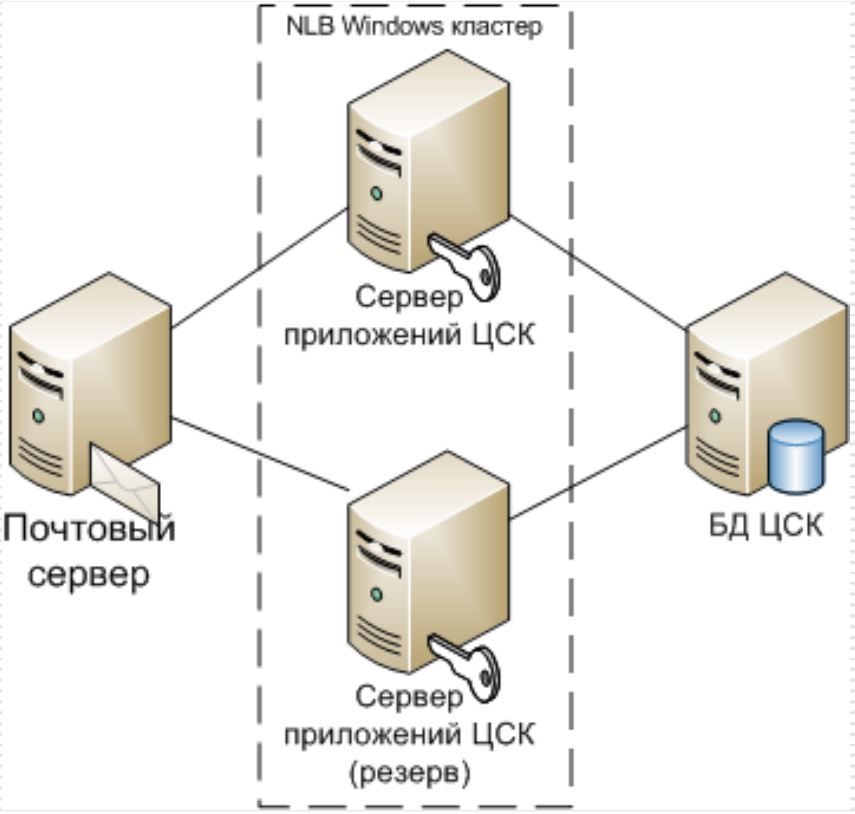
Резервируемость сервисов

- OCSP-сервер, решается в рамках масштабируемости
- TSP-сервер, решается в рамках масштабируемости
- LDAP-сервер, решается в рамках масштабируемости
- Сервер приложений ЦСК, решается в рамках масштабируемости

Резервируемость сервера приложений ЦСК

Схема 1

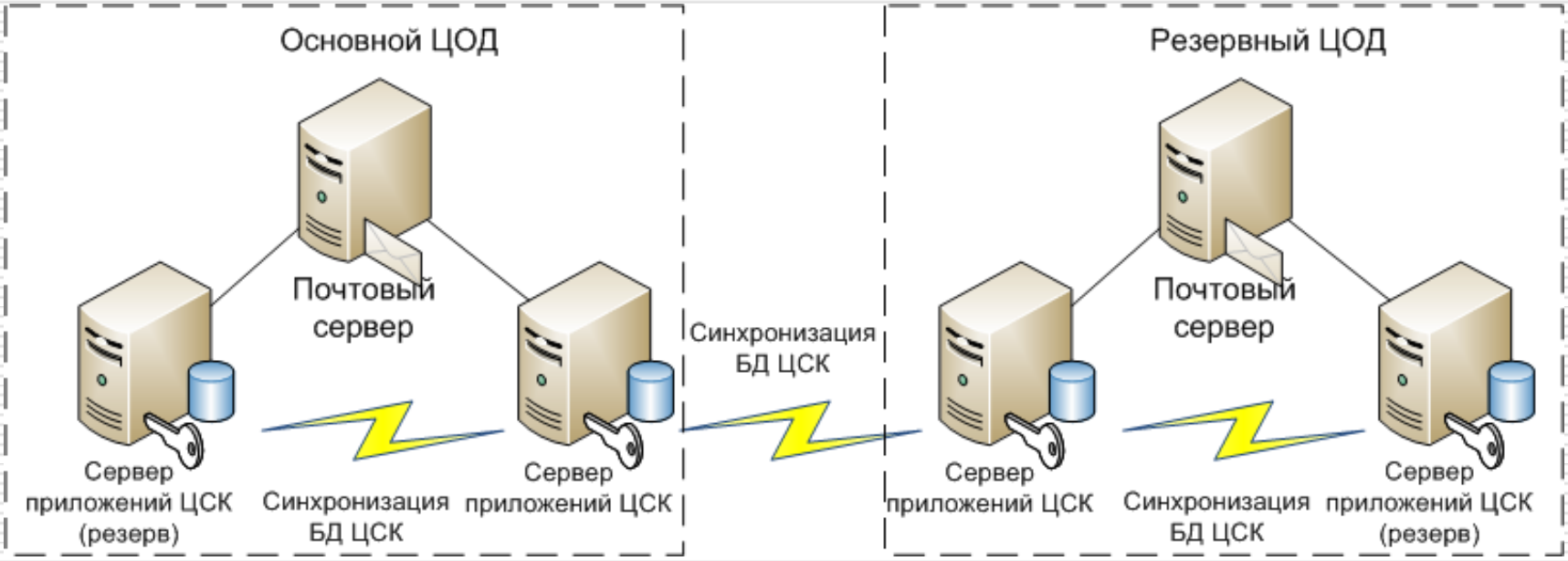
Схема 2



Резервируемость сервера приложений ЦСК (1)

- Сервера приложений ЦСК организуются в NLB Windows кластер
- БД ЦСК выносится на отдельный сервер с общим доступом узлов кластера

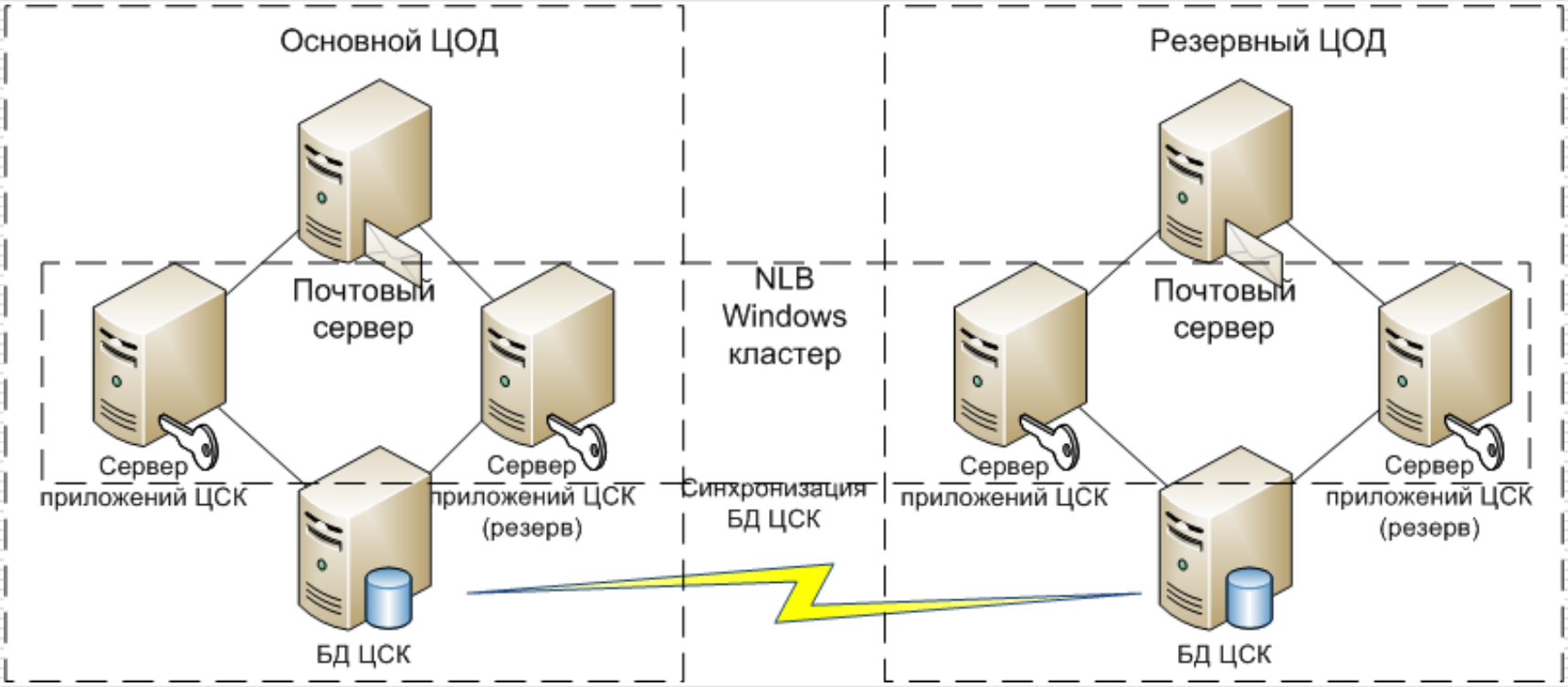
Резервируемость сервера приложений ЦСК (1)



Резервируемость сервера приложений ЦСК (2)

- Сервера приложений ЦСК достигается за счет полного клонирования
- Основной ведет запись в свою БД и в БД резервного Сервера приложений ЦСК
- Периодическая синхронизации БД ЦСК

Резервируемость сервера приложений ЦСК (2)



Репликация БД

- Базы данных FireBird

Существуют различные утилиты для организации репликации:

- **FiBRE** - open source, cross-platform.
- FBReplicator - open source.
- **ReplicadorBR** - open source.
- Replicador Firebird – freeware.
- **DBRE** - open source.
- и т.д.

Резервное хранение данных

Базы данных FireBird

Существуют различные утилиты для организации резервирования и восстановления:

- Nbackup, входит в поставку FireBird для различных операционных систем.
- GBAK, бесплатная утилита поддерживаемая официально FireBird, которая, в отличие от nbackup, позволяет работать с многофайловыми БД под управлением FireBird.

Для эффективного резервирования используют различные подходы:

- Полное резервирование.
- Инкрементное резервирование.

Резервное хранение данных

- Базы данных OpenLDAP

Существуют встроенные утилиты для организации резервирования* и восстановления данных:

- slapcat, полностью копирует содержимое БД при работающем сервере;
- slapadd, восстанавливает содержимое БД при остановленном сервере.

*Каждые сутки создается резервная копия БД в LDIF файл.

Вопросы?

Спасибо за внимание!

ООО «САЙФЕР ЛТД»

Владислав Ковтун

email: vlad.kovtun@cipher.kiev.ua
www: http://www.cipher.kiev.ua

СУБД FireBird

- Максимальный размер таблицы:
  - 2.5 ТБ для страницы в 4 КБ;
- Максимальная длинна записи:
  - суммарно все поля: 64 кБ;
- Размер базы: 131 ТБ;
- Максимальное число одновременных подключений:
  - Windows SuperClassic: 1024;
  - Linux: без перекомпиляции ядра - до 600.
- Поддержка многоядерных CPU