

Особенности служб сертификации в Windows Server 2008

Александр Шаповал
Microsoft

Содержание

- Усовершенствования служб сертификации в Windows Server 2008
- Вопросы обновления и миграции
- Мониторинг Active Directory Certificate Services

Содержание

- Усовершенствования служб сертификации в *Windows Server 2008*
- Вопросы обновления и миграции
- Мониторинг Active Directory Certificate Services

Windows Server 2008

Расширения служб сертификации

Active Directory Certificate Services

Certification
Authority

Certification
Authority Web
Enrollment

Online
Responder
(OCSP)

Network Device
Enrollment
Service

Криптография

Отзыв

Управляемость

Криптография

Crypto Next Generation (CNG)

- Поддержка алгоритмов “Группы В”
 - Сервер сертификатов
 - Регистрация клиентов
 - Смарт-карты
 - Online Responder
- Гибкость
 - Настраиваемая реализация
 - Настраиваемые алгоритмы

Реализация

- Криптография эллиптических кривых (ECC)
 - ECDSA_P256, ECDSA_P384, ECDSA_P521
 - ECDH_P256, ECDH_P384, ECDH_P521
- Хэш-алгоритмы: SHA2
 - SHA256, SHA384, SHA512
- Симметричные алгоритмы: AES
 - AES128, AES192, AES256

ОТЗЫВ

Windows Server 2008 Online Responder

- Приложению необходимо проверять статус сертификата
 - Закачка Списка отозванных сертификатов Certificate Revocation List (CRL)
- Проблема
 - Большие файлы CRL
- Решение: Online Responder
 - Реализация протокола OCSP (RFC 2560)
 - Высокоскоростная проверка статуса по http
 - Масштабируемая архитектура

Управляемость

- Упрощенное развертывание
 - Обновленный модуль установки
- Объединенные средства управления
 - Server Manager
- Мониторинг
 - Новые события и счетчики производительности
 - Пакеты управления (Management Packs)
 - System Center Operations Manager 2007
 - Microsoft Operations Manager 2005
 - Набор инструментов Enterprise PKI

Другие усовершенствования

- Отказоустойчивость Центра Сертификации
 - СА поддерживает двухузловую кластеризацию в режиме активный / пассивный
- Ограничиваемые агенты
 - Ограничение по пользователю / группе и / или шаблону
 - Блокировки для смарт-карт
- Network Device Enrollment Service
 - Может быть установлен на СА или отдельную машину
- Изменения на клиентской стороне
 - Новый мастер выдачи сертификатов
 - Изменения в веб-узле выдачи сертификатов

Содержание



- Усовершенствования служб сертификации в Windows Server 2008
- **Вопросы обновления и миграции**
- Мониторинг Active Directory Certificate Services

Планирование обновления

Основные факторы

- Что побуждает к обновлению?
 - Функциональность / новые возможности
 - Жизненный цикл оборудования
 - Жизненный цикл ПО
- Варианты развертывания
 - Обновление «на месте»
 - Обновление и миграция на новое оборудование
 - Сохранение инфраструктуры и добавление новых служб Windows Server 2008
 - Развертывание новой инфраструктуры СА

Поддерживаемые варианты

	Windows Server 2008 Standard Edition	Windows Server 2008 Enterprise Edition	Windows Server 2008 Datacenter Edition
Windows Server 2003 SP1, SP2, R2 Standard Edition			
Windows Server 2003 SP1, SP2, R2 Enterprise Edition			
Windows Server 2003 SP1, SP2, R2 Datacenter Edition			

Миграция

Миграция с одной машины на ...

- Определение миграции
 - Перенос компонент СА с одного физического компьютера на другой
 - Получаемое окружение не идентично исходному
- Причины
 - Изменение оборудования (например, на 64-битное)
 - Перенос с контроллера домена
 - Перенос на кластер

Стандартная миграция

Наиболее общие шаги

- Резервное копирование и экспорт компонент Центра Сертификации на хосте “А”
 - Сертификат и ключ СА
 - База данных СА
 - Конфигурация (реестр, шаблоны)
- Установка СА на хост “В”
 - Установка роли ADCS с использованием существующего сертификата СА
 - Импорт базы данных
 - Импорт / проверка настроек
- Сценарии с использованием аппаратного модуля безопасности (Hardware security module, HSM)
 - Шаги по миграции дополнительных ключей

Поддерживаемые варианты

Сценарии миграции	2008 - 2008	2003 - 2008	Замечания
Standalone -> Enterprise CA		Не опред.	
Enterprise -> Standalone CA		Не опред.	
x86 -> x64		Не опред.	В процессе тестирования
С машины на машину с изменением имени хоста		Не опред.	Имя CA должно сохраниться
Физическая машина -> виртуальная машина		Не опред.	Для Virtual Server
Домен -> домен (внутри леса)		Не опред.	
Хост -> кластер		Не опред.	Планируется
Лес -> лес		Не опред.	
Изменение языка		Не опред.	

Пример

Миграция CA на машину с другим именем

New Issued Certificates

Issuer:

CN=My Corp CA

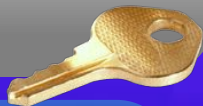
Subject:

CN=Jen Field

...

CRL Distribution Point

URL=ldap:///CN=My Corp
CA,CN=x64corphost,CN=CDP...



CA name "My Corp CA"
on
corphost01



"My Corp CA" on
new host
x64corphost

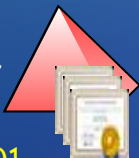


1. Полная резервная копия
2. Первые шаги общей схемы
Экспорт сертификата CA с ключом, копирование БД и конфигурации
3. Установка роли ADCS на сервер с другим именем
Используем сущ. сертификат
Принимаем предупреждение об изменении в AD
4. Импорт базы данных CA
5. Проверка/обновление реестра
CA ServerName – обновление
CRL PublicationURLs – проверка
Проверка других элементов
6. Обновление расширений CA
Новый CA должен сохранить CRL для выданных сертификатов
Добавить CDP для предыдущего имени

Пример

Перенос с контроллера домена

Domain
Controller
on
corphost01



Domain
Controller
on
newDC01



CA "My Corp CA"
on
corphost01



"My Corp CA" on
new host
corphost01



1. Установка нового DC, репликация
2. Полная резервная копия
3. Первые шаги общей схемы
Экспорт сертификата CA с ключом, копирование БД и конфигурации
4. Удаление CA с исходного DC
5. Демонтаж (dcpromo) и выключение старого DC
6. Подготовка нового сервера с таким же именем как старый DC
7. Завершение миграции
Установка CA с сущ. сертификатом
Импорт БД
8. Запуск CA
Модификации расширений CA не требуется

Содержание

- Усовершенствования служб сертификации в Windows Server 2008
- Вопросы обновления и миграции
- Мониторинг Active Directory Certificate Services

Инструменты мониторинга

- System Center Operations Manager 2007
- Microsoft Operations Manager 2005
- Enterprise PKI
- Другие инструменты
 - Выходной модуль SMTP
 - Скрипты

Operations Manager

Мониторинг здоровья Certificate Services

- Пакеты управления

- MOM 2005
- SCOM 2007

- За

- Мониторинг роли Certificate Services
- События в Events Log и счетчики производительности
- Учетная запись агента с низким уровнем привилегий

- Против

- Реактивный мониторинг

Enterprise PKI

Мониторинг элементов, не входящих в

СА

- Критичные ресурсы PKI не ограничиваются машиной со службой Certificate Services
 - CA-сертификаты / AIA-ссылки
 - Certificate Revocation Lists / CDP-ссылки
 - Служба OCSP
- За
 - Проактивный мониторинг
 - Обеспечивает целостную картину состояния PKI
- Против
 - Интерактивность

Вопросы

- <http://blogs.technet.com/ashapo>
- Следите за анонсами
 - <http://www.microsoft.com/rus/technet>

Microsoft[®]

Your potential. Our passion.[™]

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.