Microsoft

Новые возможности Active Directory в Windows Server 2008

Александр Шаповал
Microsoft

Службы каталога

- Службы каталога Windows Server 2008 Directory Services состоят из двух компонент
- **AD DS**
  - Active Directory Domain Services
- **AD LDS**
  - Active Directory Lightweight Directory Services

Active Directory Domain Services

- Изменения в схеме
  - http://msdn2.microsoft.com/en-us/library/ms675085.aspx
- Изменения в политике паролей
- Read Only Domain Controller (RODC)
  - Разделение административных ролей
- Расширение возможностей аудита
- Возможность рестарта AD DS
- Инструмент Database Mounting Tool

Политика паролей

- Может быть задана не только на уровне домена
- Добавлен специальный контейнер Password Settings Container (PSC)
- Объекты политики паролей (Password Settings Objects, PSO)
  - 9 обязательных атрибутов
    - **Enforce password history**
    - **Maximum password age**
    - **Minimum password age**
    - **Minimum password length**
    - **Passwords must meet complexity requirements**
    - **Store passwords using reversible encryption**
    - **Account lockout duration**
    - **Account lockout threshold**
    - **Reset account lockout after**

Политика паролей

- Привязка PSO:
  - msDS-PSOAppliesTo
  - msDS-PSOApplied
- Приоритет PSO
  - msDS-PasswordSettingsPrecedence
- Порядок применения PSO
  - Наименьшее значение Precedence или PSO GUID
  - msDS-ResultantPso
- Определение RSOP
  - Учитывает объекты пользователя и групп

LDIF-файл для создания PSO

```
dn: CN={PSO Object Name},CN=Password Settings
   Container,CN=System,DC=contoso,DC=com
changetype: add
objectClass: msDS-PasswordSettings
msDS-MaximumPasswordAge:-1728000000000
msDS-MinimumPasswordAge:-864000000000
msDS-MinimumPasswordLength:8
msDS-PasswordHistoryLength:24
msDS-PasswordComplexityEnabled:TRUE
msDS-PasswordReversibleEncryptionEnabled:FALSE
msDS-LockoutObservationWindow:-18000000000
msDS-LockoutDuration:-18000000000
msDS-LockoutThreshold:0
msDS-PasswordSettingsPrecedence:10
msDS-PSOAppliesTo:{Add DN of Target Group}
```

demo

Конфигурация политики паролей

Read Only Domain Controllers

- Контроллер домена в удаленном офисе или филиале…

Read Only Domain Controller

- Основные возможности
  - Копия базы AD в режиме «только чтение»
  - DNS в режиме «только чтение»
  - Разделение административных ролей
  - Односторонняя репликация
  - Кэширование параметров учетных записей

База данных RODC

- Содержит все объекты AD
  - Исключение составляют пароли пользователей
  - Можно задать политику репликации паролей
    - msDS-Reveal-OnDemandGroup
    - msDS-NeverRevealGroup
    - msDS-RevealedList
    - msDS-AuthenticatedToAccountList
- Установка атрибута фильтрации
  - schemaFlagsEx = 1 (после Beta3)
  - Не применимо к критическим системным атрибутам
    - LSA & SSPIs (Kerberos)

DNS и администрирование

- Раздел DNS
  - Клиенты могут запрашивать службу DNS на RODC для разрешения имен
  - Запросы на запись перенаправляются
- Делегирование полномочий
  - Можно предоставить определенные права
    - Сопровождение
    - Резервное копирование
    - Установка принтеров
    - Никаких изменений в AD

Кэширование паролей

- Отключено по умолчанию
- Можно настроить политику репликации
  - Для пользователей удаленного офиса
- Каждый RODC имеет свою, отличную от других, запись KRBTGT
- Повышение безопасности
  - Угроза только для кэшированных записей

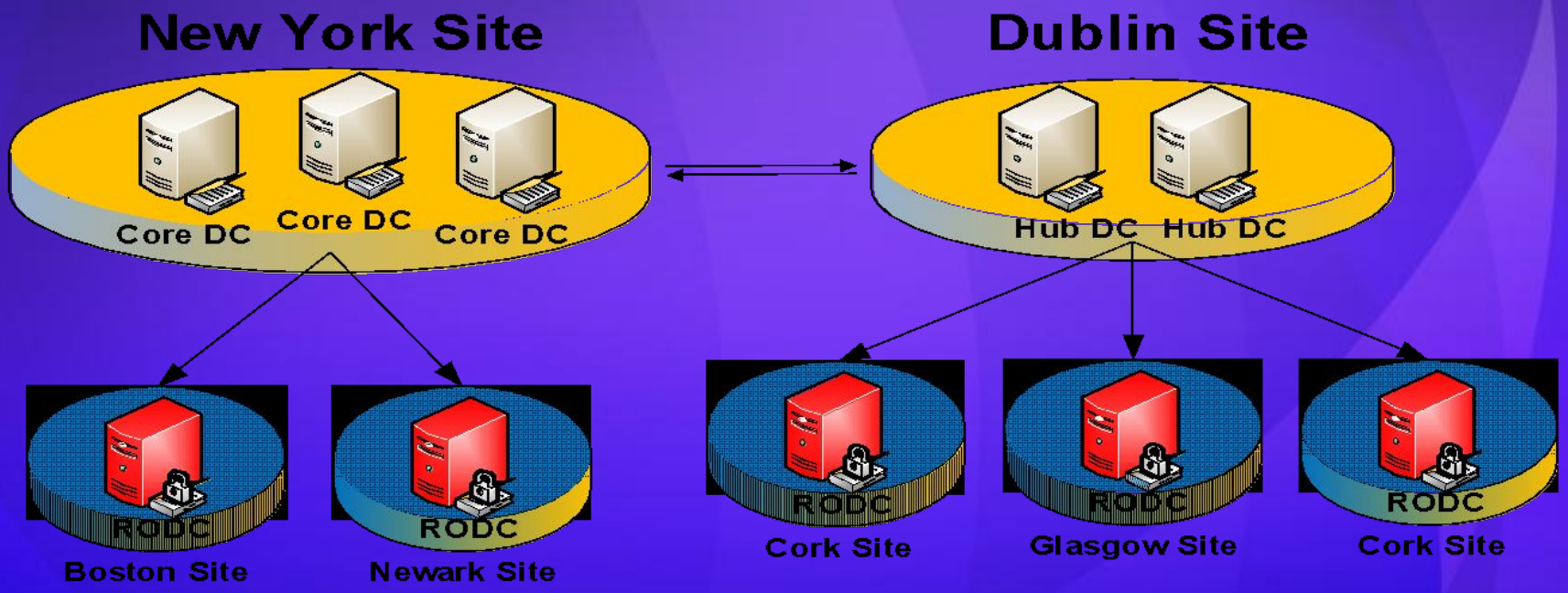
Односторонняя репликация

- Реплицируются
  - База данных Active Directory
  - SYSVOL
- Передаются все изменения
- Ограничения для RODC
  - Не может быть Bridge Head
  - Не может выполнять роли Operations Master
  - Вход по смарт-картам требует специальных полномочий для группы ERODC
- На внедрение RODC могут повлиять используемые приложения

demo

Read Only Domain Controller

Развертывание RODC



Возможности аудита

- Опция Directory Service Access
- Аудит изменений в AD
  - Создание
  - Изменение
  - Восстановление
  - Перенос
- Что протоколируется
  - Предыдущее значение, новое значение, какая учетная запись внесла изменения
- Корреляция событий

Новые события аудита

Event ID	Type of event	Event description
5136	Modify	Произошла успешная модификация атрибута в каталоге
5137	Create	Создан новый объект в каталоге
5138	Undelete	Восстановлен объект в каталоге
5139	Move	Объект перенесен в пределах домена

Перезагрузка служб AD

- Вариант применения
  - Дефрагментация NTDS.DIT
- Возможные режимы
  - AD DS запущена
  - AD DS остановлена
  - Directory Services Restore Mode
- Управление
  - MMC
  - Командная строка

demo

Перезагрузка Directory Services

Database Mounting Tool

- DSAMAIN
  - Совершенствует процесс восстановления
  - Не восстанавливает сами объекты
- Реализуется NTDSUTIL
  - Задействуются теневые копии (VSS)
- Просмотр с помощью DSAMAIN, LDP
- Позволяет администратору сравнивать моментальные снимки

demo

DATA Mining with LDP

Вопросы?

- http://blogs.technet.com/ashapo

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.