NetWrix
#1 for Change Auditing and Compliance™

Восстановление объектов Active Directory

Сборник сценариев

СОДЕРЖАНИЕ

Введение

Несомненно, многие из Вас неоднократно сталкивались с такой проблемой – удалены учетные записи пользователей. Статей по восстановлению учетных записей много, и, наверное, самая лучшая написана Microsoft, однако им всем не хватает наглядности. Мы постараемся преодолеть этот недостаток, сведя процедуру восстановления учетных записей к простым шагам.

Как Вы знаете, восстанавливать объекты можно различными способами, каждый из которых подходит наилучшим образом в той или иной ситуации.

При этом предпочтительным является восстановление из tombstone-объектов. На это есть несколько причин:

- не требуется выведение контроллера домена в автономный режим (все работают, ничего не отключено)
- восстановление объектов-захоронений гораздо лучше, чем простое воссоздание новой версии удаленного объекта

Часть атрибутов удаляется вместе с удалением объекта – их уже не восстановить. Например, членство в группах безопасности.

Если вы вновь создаете объект, он всегда будет иметь новые атрибуты objectGUID и objectSid (если это участник политики безопасности, такой как пользователь). В результате любые внешние ссылки на объект, такие как ACL, необходимо будет обновлять для отражения нового идентификатора объекта. Это может стать очень большой проблемой.

Поэтому в данном сборнике сценариев сначала будут рассмотрены способы, использующие tombstone-объекты, и лишь в конце приведена информация по принудительному восстановлению. Завершать сборник будет обзор возможностей утилиты восстановления NetWrix Active Directory Object Restore Wizard.

Что необходимо восстановить: пример

Дано:

Из домена acme.com удалена OU Finance_Department с входящими в нее учетными записями Oleg и Dmitry и вложенной OU Admins, в которой находится учетная запись Sergey.

Задача:

Восстановить OU во всеми членами (включая и вложенную OU) и атрибутами учетных записей.

И решаться эта задача будет всеми возможными способами.

Авторы сборника хотят заранее извиниться за то, что в приводимых иллюстрациях используются другие значения домена и восстанавливаемых объектов AD. Надеемся, что данная недоработка не сделает материал менее ясным.

1. Восстановление объектов с помощью ldp.exe

Где найти: Выполнить ->Ldp.exe

Суть метода: Восстановление из tombstone-объектов без DSRM-режима (Directory Services Restore Mode)

Недостатки:

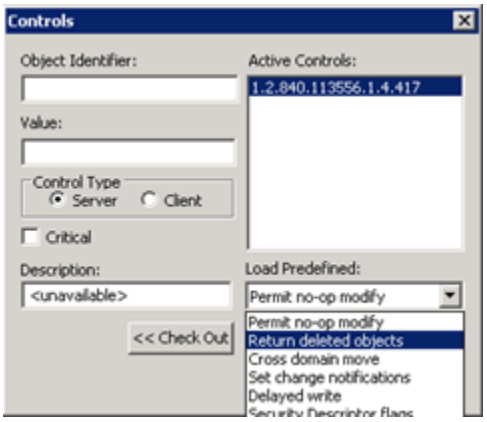
- Объект восстанавливается без атрибутов (подробнее),
- Отсутствует возможность массово восстановить объекты,
- Слишком долгая процедура восстановления

Порядок действий:

1) Включаем отображение в консоли удаленных объектов (CN=Deleted Objects)

Сначала необходимо сделать так, чтобы удаленные объекты отображались (а по умолчанию контейнер CN=Deleted Objects не отображается. Используем ldp.exe в Active Directory (требует членства в Domain Admins).

1. *Запускаем ldp.exe. (Пуск – Выполнить – ldp.exe)*
2. *В меню **Options (Параметры)** выбираем пункт **Controls (Элементы управления)***



3. В появившимся диалоговом окне выбираем меню ***Load Predefined (Предопределенная перезагрузка),*** *в нем выбираем пункт* ***Return deleted objects (Возврат удаленных объектов)*** *и нажимаем* ***Ok***

4. Проверьте, как отображается контейнер удаленных объектов:

a. *Чтобы подключиться и выполнить привязку к серверу, на котором находится корневой домен леса среды Active Directory, в разделе* ***Connections (Подключение)*** *выберите пункт* ***Connect (Подключить)*** *и нажмите* ***Bind (Привязка)****.*

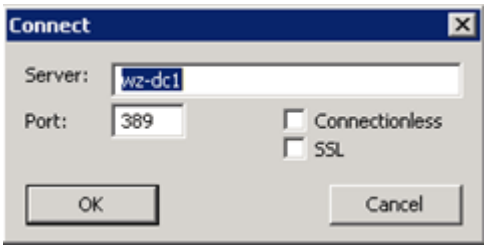
b. *Нажмите кнопку* ***Обзор****, выберите пункт* ***Структура*** *и в поле* ***Distinguished Name (DN)*** *введите* ***DC=<acme>,DC=<com>****.*

c. *В дереве консоли дважды щелкните различающееся имя (DN) корневого домена и найдите контейнер* ***CN=Deleted Objects, DC=<acme>,DC=<com>****.*

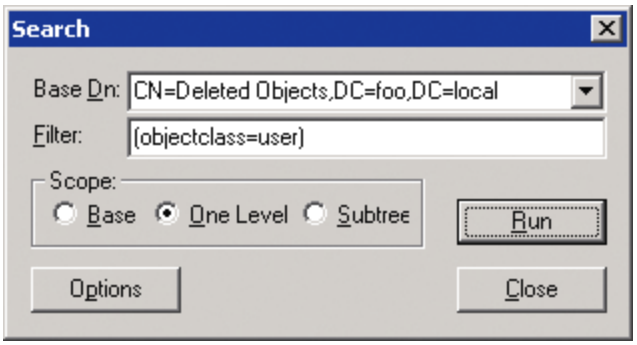
Восстанавливаем объекты:

Рассмотрим восстановление на примере учетной записи Oleg, входящей в OU Finance_Department.

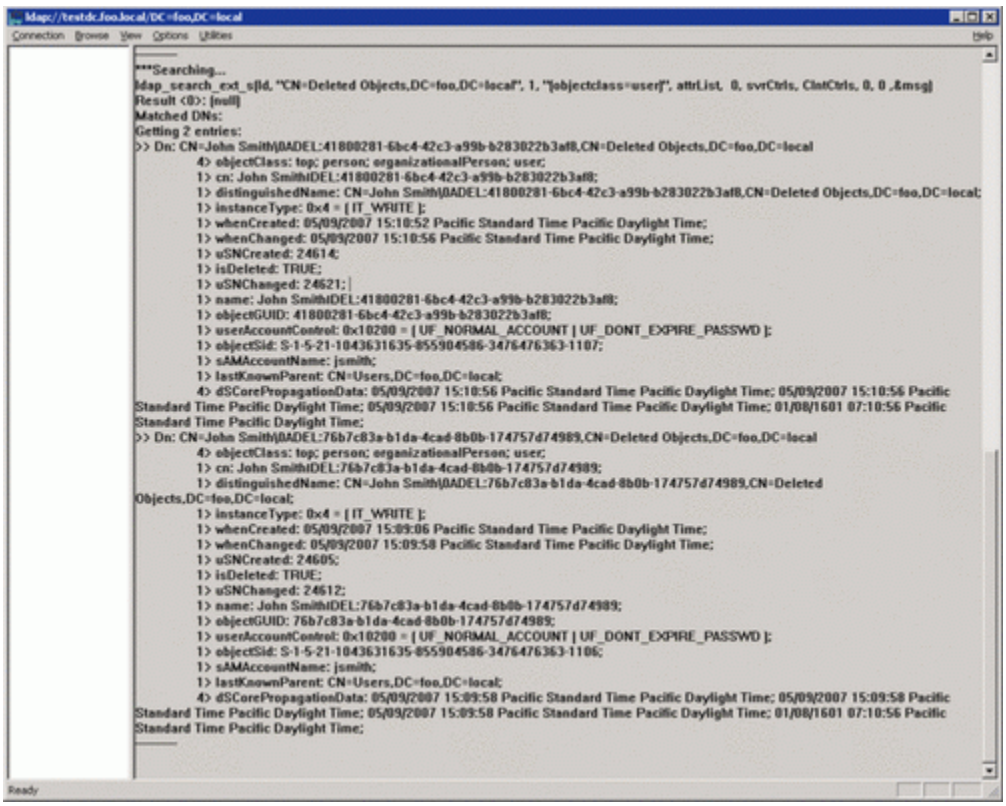
1) Запускаем ldp.exe
2) В разделе **Connections (Подключение)** выбираем пункт **Connect (Подключить)** - **Bind (Привязка)** Подключаемся и осуществляем привязку к серверу, на котором находится корневой домен леса среды Active Directory



3) В дереве консоли переходим в контейнер CN=Deleted Objects (прописываем также DC=acme,DC=com для взятого за пример домена)



Результаты поиска



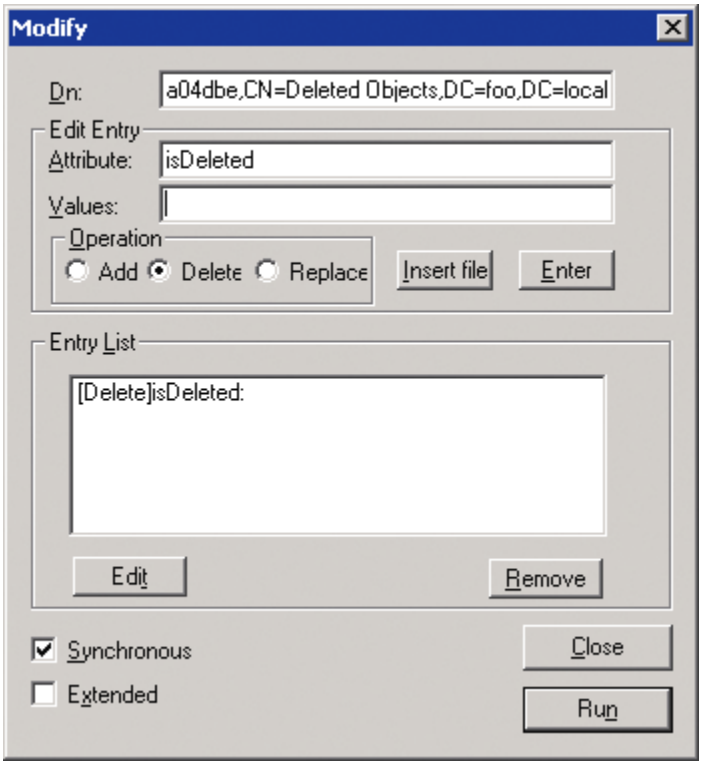
4) Находим в оснастке в контейнере CN=Deleted Objects объект, который хотим восстановить, щелкаем правой кнопкой на него и выбираем пункт **Modify (Изменить).**

5) В окне **Modify (Изменение)** меняем следующие параметры

a. В поле **Edit Entry (Изменить запись)** атрибута вводим *isDeleted*

b. Оставляем поле **Values (Значение)** пустым

c. В разделе **Operation (Операция)** выбираем **Delete (Удалить)** и нажимаем клавишу **Enter (ВВОД)**

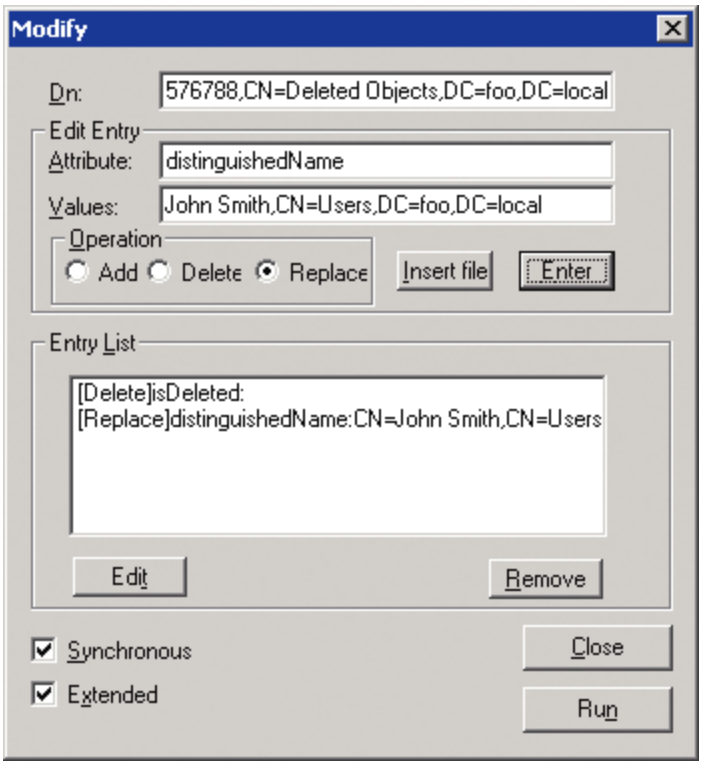


d. В поле **Edit Entry Attribute (Изменить запись Атрибута)** вводим **distinguishedName**

e. В поле **Values (Значения)** вводим первоначальное различающееся имя (DN) этого объекта Active Directory.

f. В разделе **Operation (Операция)** выбираем **Replace (Заменить)**

g. Устанавливаем флажок **Extended (Расширенный)**, нажимаем клавишу **Enter (ВВОД)**, а затем **Run (Выполнить)**



Учетная запись восстановлена, но деактивирована. Включить ее необходимо будет вручную. Также вручную необходимо восстановить членство в группах и сбросить пароль.

Те же самые действия повторяем для оставшихся объектов:

OU Finance_Department

OU Admins

Учетной записи Dmitry

Учетной записи Sergey

Итог:

Необходимо проделать много действий, прежде чем объект будет восстановлен.

Все действия придется повторить для каждого из удаленных объектов.

2. Используем ADRESTORE

Что это такое: Утилита для восстановления объектов Active Directory

Где найти: www.microsoft.com/technet/sysinternals/utilities/AdRestore.mspx

Суть метода: Извлечение объектов с последующим восстановлением объектов без DSRM-режима (Directory Services Restore Mode)

Недостатки:

- Объект восстанавливается без атрибутов
- Невозможность восстановления объектов, удаленных из контекста именования конфигурации
- Сложность массового восстановления вложенных объектов (OU внутри OU)

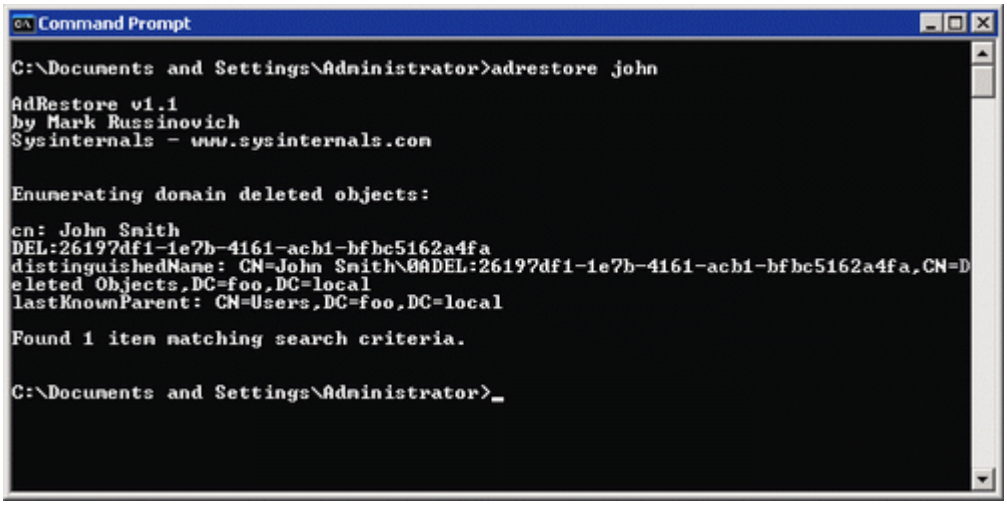
Восстановление объектов-захоронений с помощью LDP дело несложное. Однако неудобное и долгое. Для этих целей есть ADRESTORE, которая предназначена специально для восстановления объектов AD.

Утилита работает в двух режимах:

- **Запуск без параметров**. Она ***выведет список всех объектов-захоронений в контейнере CN=Deleted Objects*** домена по умолчанию. Можно добавить строку для поиска в командной строке, чтобы выбрать объекты для показа:

C:\> adrestore Finance_Department

Выводятся все объекты в контейнере CN=Deleted Objects, которые содержат строку «Finance_Department» в атрибуте CN или OU — используется поисковый фильтр LDAP cn=*Finance_Department* и ou=*Finance_Department*. На рисунке ниже показаны результаты поиска, возвращенного программой ADRESTORE.



- **Восстановление объектов**

Если нужно восстановить объект-захоронение, а не только найти его, необходимо указать параметр –r вместе с дополнительной строкой, например, вот так:

C:\> adrestore –r Finance_Department

Для восстановления учетных записей используем команды:

C:\> adrestore –r Oleg

C:\> adrestore –r Dmitry

C:\> adrestore –r Admins

C:\> adrestore –r Sergey

Команда предложит восстановить каждый удовлетворяющий условию объект-захоронение. Объект восстанавливается в контейнер, указанный атрибутом lastKnownParent объекта-захоронения (и никакой другой).

Эта команда предложит восстановить каждый подходящий объект-захоронение. ADRESTORE всегда восстанавливает объект в контейнер, указанный атрибутом lastKnownParent объекта-захоронения, нет никакого способа указать другой контейнер.

Итог:

ADRESTORE легче использовать, чем LDP.

Утилита позволяет относительно быстро восстановить объекты, но опять-таки без необходимых атрибутов - членство в группах и пароли придется восстановить вручную.

Один из самых популярных способов восстановления объектов.

3. Использование AD Recycle Bin (Windows Server 2008 R2)

Что это такое: специальная опция, позволяющая восстанавливать удаленные объекты с атрибутами

Где найти: только в Windows Server 2008 R2. Корзину необходимо включить

Суть метода: Восстановление объектов со всеми атрибутами

Недостатки:

- Отсутствие графического интерфейса – Вам придется работать с Powershell.
- Необходимы множественные операции по восстановлению
- Невозможно гранулярное восстановление
- Все сервера в лесу должны быть Windows 2008 R2

В Windows Server 2008 R2 появилась корзина Active Directory Recycle Bin (AD RB), Чтобы ее активировать, необходимо, чтобы уровень леса был Windows Server 2008 R2. AD RB напоминает обыкновенную корзину Windows - случайно удаленный объект может быть быстро и со всеми атрибутами восстановлен. Причем восстановленный из AD RB объект сразу же получает и все свои атрибуты. По умолчанию время «жизни» удаленного объекта в AD RB составляет 180 дней, после этого переходит в состояние Recycle Bin Lifetime, теряет атрибуты и через некоторое время полностью удаляется.

В самом простом случае восстановление объекта происходит с помощью Powershell командлетов **Get-ADObject и Restore-ADObject** (в том случае, если Вы точно знаете, что именно Вам необходимо восстановить). Командлет Get-ADObject используется для извлечения удаленного объекта, который затем передается с помощью конвейера в командлет Restore-ADObject:

1. Запускаем от имени администратора **Модуль Active Directory для Windows PowerShell**.
2. В командной строке Active Directory module for Windows PowerShell введите следующую команду:

PS C:\> Get-ADObject -Filter {displayName -eq "user"} -IncludeDeletedObjects | Restore-ADObject

В данном примере

-Filter {displayName -eq "user"} указывает, что какую информацию об объекте AD необходимо получить (в примере – об объекте с отображаемым именем пользователя “user),

-IncludeDeletedObjects означает, что поиск осуществляется по удаленным объектам

Restore-ADObject непосредственно осуществляет восстановление объекта AD.

Недостаток очевиден – отсутствует наглядность, нужно помнить информацию об имени, ошибки кода опять-таки. Однако если удаление одного объектов произошло только что, то можно использовать данный метод.

Однако не всегда нужно восстановить только один объект, да и имена удаленных объектов могут быть неизвестны администратору.

Поиск удаленных объектов

1. Запускаем от имени администратора **Модуль Active Directory для Windows PowerShell**.
2. В командной строке Active Directory module for Windows PowerShell вводим следующие команды для получения необходимой информации:

Вывод информации об удаленных объектах в домене acme.com

Get-ADObject -SearchBase "CN=Deleted Objects,DC=acme,DC=com" –IncludeDeletedObjects

Получаем информацию о том, в какой OU состоял удаленный пользователь

Get-ADObject -SearchBase "CN=Deleted Objects,DC=acme,DC=com" -ldapFilter:"(msDs-lastKnownRDN=User)" –IncludeDeletedObjects –Properties lastKnownParent

Где User – отображаемое имя пользователя

В итоге получаем информацию о принадлежности к OU указанного пользователя (с помощью -Properties lastKnownParent)

Поиск всех удаленных объектов, которые входили в данную OU

В качестве примера берем различающееся имя OU Finance_Department, которое было получено после запуска предыдущего командлета (Finance_Department\\0ADEL:e954edda-db8c-41be-bbbd-599bef5a5f2a).

Get-ADObject –SearchBase "CN=Deleted Objects,DC=acme,DC=com" -Filter {lastKnownParent -eq 'OU=Finance_Department\\0ADEL:e954edda-db8c-41be-bbbd-599bef5a5f2a,CN=Deleted Objects,DC=acme,DC=com'} -IncludeDeletedObjects -Properties lastKnownParent | ft

Внимание! Если у Вас имеется вложенная OU, восстановление осуществляется начиная с наивысшего уровня иерархии. В данном случае таковым является OU=Finance_Department.

Восстановление объектов

1. Запускаем **Модуль Active Directory для Windows PowerShell**
2. Восстанавливаем подразделение Finance_Department, выполнив в командной строке следующую команду:

Get-ADObject -ldapFilter:"(msDS-LastKnownRDN=Finance_Department)" –IncludeDeletedObjects | Restore-ADObject

3. Восстанавливаем учетные записи и OU, которые являются непосредственными дочерними объектами OU Finance_Department (помните, что на этом этапе различающееся имя Finance_Department уже восстановлено в значение OU=Finance_Department,DC=acme,DC=com)

Get-ADObject -SearchBase "CN=Deleted Objects,DC=acme,DC=com" -Filter {lastKnownParent -eq "OU=Finance_Department,DC=acme,DC=com"} -IncludeDeletedObjects | Restore-ADObject

Опционально (восстановление вложенных OU)

4. Восстанавливаем учетные записи, входящие во вложенную OU (например, OU Admins, которая входит в состав OU Finance Department. Различающееся имя в нашем примере было восстановлено в значение OU=Admins,OU=Finance_Department,DC=acme,DC=com)

Get-ADObject -SearchBase "CN=Deleted Objects,DC=acme,DC=com" -Filter {lastKnownParent -eq "OU=Admins,OU=Finance_Department,DC=acme,DC=com"} -IncludeDeletedObjects | Restore-ADObject

Подробную справку о командлетах и их параметрах вызвав командлет Get-Help, например Get-Help Get-ADObject

Итог:

Объекты будут восстановлены в первоначальный вид – со всеми атрибутами.

Однако, как мы можем видеть, данный метод довольно сложен, когда приходится работать с большим количеством объектов.

Также требуется, все сервера в лесу должны быть Windows 2008 R2.

Для восстановления объектов с атрибутами при включенной корзине AD можно использовать описанные выше инструменты LDP и AdRestore.

4. Принудительное восстановление с помощью NTDSUTIL

Что это такое: утилита командной строки, позволяющая восстанавливать удаленные объекты из мгновенных снимков AD

Где найти: Работает в режиме DSRM (F8)

Суть метода: Восстановление объектов со всеми атрибутами из снимков Active Directory

Недостатки:

- Режим DSRM требует вывода домена в режим перезагрузки.
- Объект может быть перезаписан процессом репликации

Стандартным способом (но, однако, не самым подходящим) является принудительное восстановление из резервной копии в режиме Directory Service Restore Mode. Он обладает серьезными недостатками: нужно перезагружать сервер, а во-вторых, восстанавливать из резервной копии состояние системы и помечать, какие объекты не будут перезаписаны процессом репликации.

Восстановление осуществляется с помощью утилиты командной строки NTDSUTIL. Утилита становится доступной после установки роли AD DS. Используя ее, можно восстановить как OU со всем содержимым, так и отдельный объект.

Работа утилиты основана на мгновенных снимках (снапшотах) Active Directory, которые делаются при помощи службы VSS.

Внимание! В ходе принудительного восстановления AD внутренний номер версии восстанавливаемых объектов увеличивается. После подключения контроллера домена к сети эти объекты будут реплицированы по всему домену, а восстановленная версия становится глобально действующей.

Порядок действий:

1. Нам необходимо восстановить OU Finance_Department из домена acme.com
2. Загружаемся в режиме DSRM (в загрузочном меню вызывается нажатием клавиши F8) и выполните регистрацию с паролем, DSRM, заданным во время работы Dcpromo. AD не загружается, база данных переводится в автономный режим.

Внимание! Невозможно выполнить восстановление, если на контроллерах домена Server 2008 и выше остановлена служба NTDS AD.

3. Восстановите системное состояние из резервной копии, созданной до аварии.

Внимание! Не перезагружайте компьютер.

В снимке, полученном при помощи ntdsutil, присутствует как сам объект, так и его атрибуты. Образ можно монтировать и подключать в качестве виртуального LDAP-сервера, экспортирующего объекты. Запускаем ntdsutil:

> ntdsutil

ntdsutil: snapshot

Просматриваем список доступных снимков:

снимок: list all

```
 1: 2009/04/22:23:18 {8378f4fe-94c2-4479-b0e6-ab46b2d88225}

2:              C:              {732fdf7f-9133-4e62-a7e2-2362227a8c8e}



3: 2009/04/23:00:19 {6f7aca49-8959-4bdf-a668-6172d28ddde6}

4: C: {cd17412a-387b-47d1-9d67-1972f49d6706}
```

Монтируем командой mount с указанием номера или {ID}:

снимок: mount 4

```
Снимок {cd17412a-387b-47d1-9d67-1972f49d6706} установлен как C:\$SNAP_200904230019_VOLUMEC$\
```

Снимок смонтирован.

4. Запустите команду

Для восстановления подразделения Finance_Department

> ntdsutil "authoritative restore" "restore subtree ou=Finance_Department,dc=acme,dc=com" q q

В итоге будет восстановлена OU Finance_Department с входящими в нее учетными записями и вложенной OU Admins

Для восстановления отдельной учетной записи, например, с отображаемым именем Oleg

> ntdsutil "authoritative restore" "restore object cn=Oleg,ou=Finance_Department,dc=acme,dc=com" q q

5. Необходимо подтвердить предупреждения безопасности. Затем будет выдано сообщение, подобное показанному на рисунке 3. Обратите внимание на сформированные текстовые и LDIF-файлы.

```
Successfully updated 72 records.

The following text file with a list of authoritatively restored
objects has been created in the current working directory:
     ar_20110221-151131_links_contoso.com.txt

One or more specified objects have back-links in this domain. The
following LDIF files with link restore operations have been
created in the current working directory:
     ar_20110221-151131_links_contoso.com.ldf

Authoritative Restore completed successfully.
```

6. Перезагрузите DC в нормальном режиме запуска операционной системы.

7. Зарегистрируйтесь на DC и откройте командную строку. Импортируйте LDIF-файл, экспортированный на шаге 5, выполнив команду

ldifde -i -f

ar_20110221-151131_links_contoso.com.ldf,

где **ar_20110221-151131_links_contoso.com.ldf** – имя созданного LDIF-файла.

8. В результате будут импортированы значения связанных атрибутов (такие, как членство в группах) для восстановленных объектов

Внимание! Если в лесу содержится несколько доменов, необходимо использовать текстовый файл, экспортированный на шаге 6 для восстановления членства в локальных группах других доменов.

Итог:

Учетные записи и объекты восстановлены, однако база Active Directory была недоступна в течение определенного периода времени. Вы также зависите от наличия актуальных баз данных AD, полагаясь на данный метод восстановления.

5. NetWrix Active Directory Object Restore Wizard

Что такое: утилита гранулярного восстановления объектов AD

Как работает: программа анализирует снапшоты и позволяет восстановить объекты с атрибутами

Где найти: www.netwrix.com/ru/active_directory_object_restore_wizard_freeware.html

Недостатки метода:

- Для полного восстановления объектов с атрибутами программа должна быть заранее установлена в домене

Процесс восстановления объектов можно очень сильно упростить, если воспользоваться утилитой NetWrix Active Directory Object Restore Wizard.

Сразу хочется отметить, что в нашу компанию постоянно обращаются администраторы, которые удалили объекты AD и теперь хотят их восстановить. Предлагаемое нами решение – NetWrix Active Directory Object Restore Wizard - хоть и позволяет упростить процесс восстановления объектов (например, восстановить OU со всеми объектами и их атрибутами за пару кликов), однако все равно не творит чудеса – программа должна быть установлена в домене и периодически делать снимки AD. Поэтому рекомендуем после прочтения статьи все-таки поставить программу работать (есть бесплатная версия с периодом восстановления за последние 4 дня), чтобы в следующий раз не испытывать таких проблем с восстановлением объектов.

Утилита позволяет восстанавливаться удаленные объекты за пару кликов, а в том случае, если программа работала до удаления объектов в домене, то восстановление происходит со всеми атрибутами. В итоге Вы получаете возвращенные учетные записи за пару минут

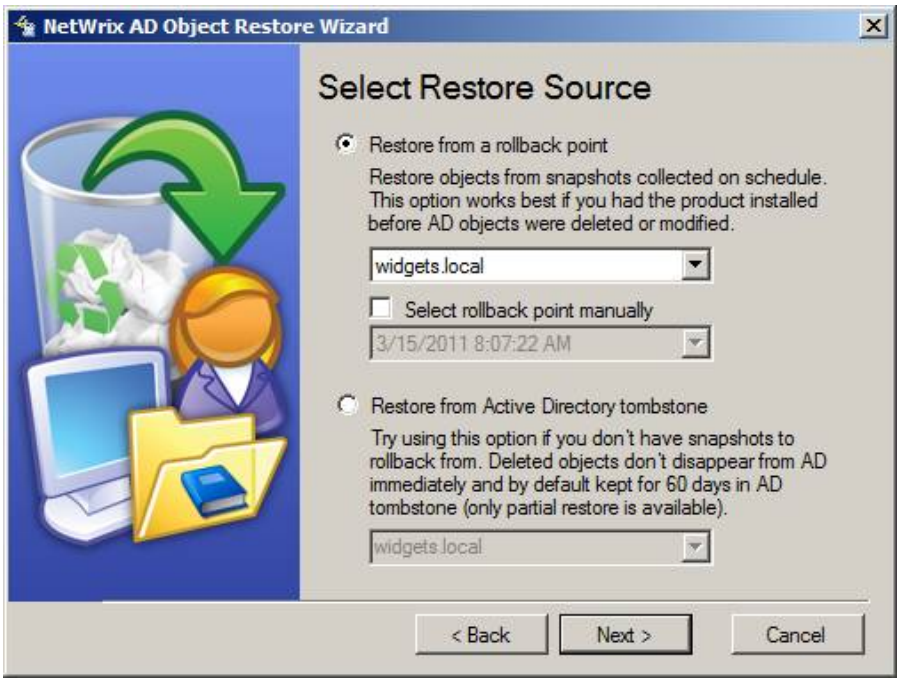
без серьезных сбоев в работе организации. Также следует отметить то, что программа позволяет восстанавливать удаленные почтовые ящики.

Работа с программой сводится к следующим шагам:

1. Запускается мастер **NetWrix Active Directory Object Restore Wizard**.

2. Выбирается режим восстановления:

- Только из tombstone-объектов (если программа не была установлена до этого в домене)
- Восстановление с использованием снапшотов (если программа была установлена и был сделан хотя бы один снапшот)



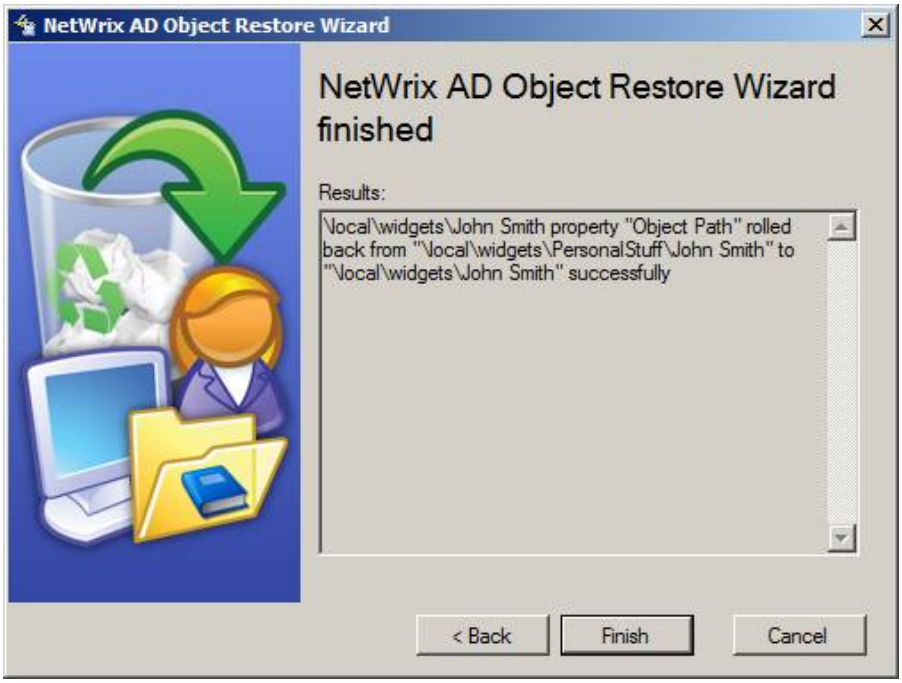
3. По результатам анализа выводится список удаленных объектов с их первоначальной иерархией и объектами

4. Выберите те OU или объекты, которые необходимо восстановить, и нажмите далее

5. В зависимости от того, была ли установлена программа раньше или нет:

- Если не была, то необходимо вручную восстановить членство в группах и пароли пользователей

- Если программа была установлена, то восстановление на этом закончено и все будет работать так, как будто ничего не произошло.



Как Вы можете видеть, восстановление объектов занимает гораздо меньше времени, нежели с использованием штатных инструментов восстановления объектов Active Directory.

Но восстановление объектов – это только одна из сторон программы. Вы также можете откатывать изменения объектов – вплоть до значения одного атрибута – программа предназначена и для этого.

Итог:

Восстановление объектов с атрибутами сводится к паре простых шагов. Возможно не только восстановить объекты, но и откатить лишь их некоторые значения.

Заключение

В данном руководстве было рассмотрены основные способы восстановления удаленных объектов Active Directory. То, какой способ использовать зависит от того, сколько объектов необходимо восстановить и версии серверной операционной системы. В любом случае по мере увеличения количестве учетных записей, подлежащих восстановлению, предпочтение отдается специализированным решениям, которые позволяют не только быстро и с минимальными потерями восстанавливать удаленные объекты, но и своевременно оповещать обо всех изменениях в Active Directory.

Дополнительные ресурсы:

- Полное руководство по аудиту Active Directory в Windows Server 2008/R2: http://www.netwrix.com/ru/active_directory_audit_guide.html
- NetWrix Active Directory Change Reporter – программа для аудита AD http://www.netwrix.com/ru/landing.html?product=adcr
- Все решения NetWrix для аудита изменений и управления доступом http://www.netwrix.com/ru/products.html