Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Корзина Active Directory: восстановление объекта за 30 секунд

Как мы включаем AD Recycle Bin и настраиваем сроки, делегирование и аудит удалений

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Удаление учётки в AD — это не «пропал логин», а мгновенная потеря членств в десятках групп, прав на файловые шары, доступа к 1С, почте и VPN. Без корзины возврат идёт через authoritative restore из бэкапа в режиме DSRM: часы простоя и остановка контроллера. Мы закрываем это заранее: включаем AD Recycle Bin, задаём msDS-deletedObjectLifetime, делегируем Reanimate Tombstones и с…

Почему это важно бизнесу

- Удалённая учётка = мгновенная потеря доступа к шарам, 1С, почте и VPN, часто сразу у целого отдела
- Восстановление из ночного бэкапа через DSRM — 6–8 часов простоя и остановка контроллера домена
- Ручная пересборка членств в сотнях групп даёт ошибки прав: кто-то получает лишний доступ к финансам
- Массовое удаление скриптом всплывает по жалобам, а не по алерту — теряется рабочий день отдела
- Корзина включается за 5 минут и не требует лицензий: бездействие здесь дороже внедрения

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

180 дней

Дефолт: msDS-deletedObjectLifetime=null → берётся tombstoneLifetime леса (180 дней для лесов о…

Deleted Object Lifetime, AD DS

365 дней

Наш порог msDS-deletedObjectLifetime: перекрывает годовой цикл «уволили — вернули»

стандарт ITfresh

2008 R2

Минимальный функциональный уровень леса (FFL); все домены леса при этом тоже не ниже 2008 R2

AD Recycle Bin, требования

12 ч

Интервал garbage collection на каждом DC; garbageCollPeriod допускает от 1 до 168 часов

AD Schema: garbageCollPeriod

5141 / 5138

События аудита: удаление объекта каталога и его восстановление (undelete), пишутся только на DC

Audit Directory Service Changes

CA + LCRP

Минимум прав делегата: Reanimate Tombstones на NC домена и LCRP на CN=Deleted Objects

стандарт ITfresh

РЕАЛИЗАЦИЯ 1 ИЗ 3

Включение корзины и настройка срока хранения

Что настраиваем

Лес заказчика целиком: DC с ролью Domain Naming Master, RSAT AD PowerShell на рабочем месте инженера

Как мы это делаем

1. Снимаем базу: Get-ADForest / Get-ADDomain (ForestMode ≥ Windows2008R2Forest) и Get-ADOptionalFeature -Filter * — смотрим пустой EnabledScopes у Recycle Bin Feature
2. Под Enterprise Admins: Enable-ADOptionalFeature -Identity 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target corp.example.ru -Server <владелец DNM>. Необ...
3. Поднимаем срок: Set-ADObject -Identity 'CN=Directory Service,CN=Windows NT,CN=Services,<ConfigNC>' -Partition <ConfigNC> -Replace @{'msDS-deletedObjectLifetime'=365}
4. Ждём конвергенцию: repadmin /showrepl и Get-ADReplicationPartnerMetadata -Target <DC> -Scope Server → LastReplicationSuccess по всем партнёрам
5. Фиксируем дату включения в паспорте домена: объекты, удалённые ДО неё, стали recycled и корзиной уже не восстанавливаются

РЕЗУЛЬТАТ

Возврат учётки со всеми link-valued атрибутами (memberOf, managedBy, manager) занимает секунды вместо 6–8 часов восстановления в DSRM, без остановки контроллера, без authoritative restore и без риска рассинхронизировать репликацию.

КЛЮЧЕВОЙ НЮАНС

По доке операция выполняется на владельце Domain Naming Master: берём (Get-ADForest).DomainNamingMaster в -Server и учётку Enterprise Admins; на RODC командлет не работает.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Массовое восстановление OU и учёток после аварии скрипта

Что настраиваем

Контейнер CN=Deleted Objects домена, все DC; пакетный PowerShell с member-сервера с установленным RSAT

Как мы это делаем

1. Останавливаем источник аварии и снимаем срез: Get-ADObject -IncludeDeletedObjects -Properties whenChanged,lastKnownParent,objectClass → CSV
2. Восстанавливаем сверху вниз: сначала родительская OU, затем вложенные, только потом user/computer — иначе ошибка «the object's parent is either uninstantiated or de…
3. Пакет по родителю: Get-ADObject -SearchBase 'CN=Deleted Objects,DC=corp,DC=ru' -SearchScope OneLevel -IncludeDeletedObjects -Filter {lastKnownParent -eq …} | Restor…
4. Если исходной OU нет — Restore-ADObject -TargetPath 'OU=Restored,DC=corp,DC=ru', далее перенос вручную по согласованной структуре
5. Сверка результата: Get-ADUser -Properties MemberOf,userAccountControl по списку из CSV и дифф против среза, снятого до восстановления

РЕЗУЛЬТАТ

Авария на несколько десятков объектов закрывается за 10–15 минут пакетом с try/catch и логом: членства в группах, пароль, userAccountControl и контактные атрибуты возвращаются без ручной пересборки прав на ресурсы.

КЛЮЧЕВОЙ НЮАНС

ADAC (dsac.exe) не восстанавливает поддерево одним действием — батч сортирует родителей только внутри выделения; разделы Configuration, DomainDNS и ForestDNS он вообще не видит, там только Restore-ADObject.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Делегирование восстановления, аудит и защита OU

Что настраиваем

Домен NC и CN=Deleted Objects, группа AD-Restore-Operators, SACL на OU, пересылка событий с каждого DC

Как мы это делаем

1. Права делегату: dsacls DC=corp,DC=ru /g 'CORP\AD-Restore-Operators:CA;Reanimate Tombstones' — право реанимации выдаётся на весь раздел домена
2. Контейнер удалённых: сначала dsacls 'CN=Deleted Objects,DC=corp,DC=ru' /takeownership, затем /g 'CORP\AD-Restore-Operators:LCRP' — без смены владельца права не выда…
3. Включаем подкатегорию: auditpol /set /subcategory:'Directory Service Changes' /success:enable и вешаем SACL на контейнеры с учётками
4. Собираем 5141 (удаление) и 5138 (undelete) со всех DC, алерт при более чем 10 удалениях объектов класса user за 5 минут
5. Ставим ProtectedFromAccidentalDeletion на все OU и критичные группы — это Deny для Everyone на Delete и Delete Subtree в DACL объекта

РЕЗУЛЬТАТ

Удаление перестаёт быть анонимным: в журнале видно кто, что и когда удалил, массовое удаление ловится алертом за минуты, а не через сутки по жалобам, а восстановление выполняет заранее обученная группа без выдачи Domain Admins.

КЛЮЧЕВОЙ НЮАНС

События 5136–5141 пишутся только при настроенном SACL и только на том DC, где выполнена операция, — журнал обязательно собирать со всех контроллеров, а не с PDC.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

✕ **Корзину включили уже после аварии**
В момент включения все прежние tombstone становятся recycled: атрибуты и членства сброшены. Вариант один — authoritative restore из бэкапа до включен…

✕ **Ждут, что корзина вернёт всё**
Она не возвращает ящики Exchange, профили, содержимое файловых шар и правки схемы. Бэкап system state контроллеров остаётся обязательным.

✕ **Восстановление снизу вверх**
Пользователь не встанет раньше своей родительской OU. Порядок строго: OU → вложенные OU → объекты, ориентир — атрибут lastKnownParent.

✕ **Срок хранения оставили дефолтным**
null в msDS-deletedObjectLifetime = значение tombstoneLifetime леса, обычно 180 дней. Просьбы «верните за прошлый год» упираются в garbage collection.

✕ **Право восстановления у всех админов**
Без делегирования Reanimate Tombstones отдельной группе всё делается под Domain Admins и в логах не видно конкретного исполнителя.

✕ **Не следят за ростом NTDS.dit**
Корзина хранит объекты со всеми атрибутами на каждом DC леса; контролируем свободное место на томе базы и планируем offline defrag.

✕ **Одноимённые удалённые объекты**
При повторных удалениях одного sAMAccountName нужен фильтр по whenChanged или ObjectGUID, иначе вернётся не та версия объекта.

✕ **Снят флаг защиты OU от удаления**
Без ProtectedFromAccidentalDeletion подразделение сносится одним действием вместе с содержимым; ставим Deny Delete/Delete Subtree на все OU.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Включить AD Recycle Bin, функциональный уровень леса поднять минимум до Windows Serv…
- Проверить EnabledScopes у Recycle Bin Feature (Get-ADOptionalFeature) и зафиксироват…
- Включить ProtectedFromAccidentalDeletion на всех OU и критичных группах

НОРМАЛЬНО

- msDS-deletedObjectLifetime = 365 дней плюс контроль свободного места на томе NTDS.dit
- Делегировать Reanimate Tombstones отдельной группе, а не всем админам
- Аудит Directory Service Changes + SACL, сбор событий 5141/5138 со всех DC
- Ежедневный бэкап system state DC (Windows Server Backup или Veeam)

ХОРОШО

- Алерт в Telegram при более чем 10 удалениях объектов user за 5 минут
- Готовый скрипт пакетного восстановления по lastKnownParent с логом
- Квартальный тест восстановления с протоколом сверки атрибутов и memberOf
- Ежемесячный отчёт по содержимому CN=Deleted Objects и срокам истечения

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Включена ли корзина AD во всех лесах и зафиксирована ли дата включения в паспорте домена?
- [ ] Функциональный уровень леса не ниже Windows Server 2008 R2 (ForestMode = Windows2008R2Forest и выше)?
- [ ] Задан ли msDS-deletedObjectLifetime явно (365 дней) или он всё ещё null и равен tombstoneLifetime?
- [ ] Есть ли отдельная группа с правом Reanimate Tombstones и LCRP на CN=Deleted Objects?
- [ ] Включена ли подкатегория аудита Directory Service Changes и настроены ли SACL на контейнерах?
- [ ] Уходят ли события 5141 и 5138 со всех DC в общий журнал с алертом на массовое удаление?
- [ ] Стоит ли защита от случайного удаления на всех OU и критичных группах безопасности?
- [ ] Проводился ли тест восстановления пользователя за последние три месяца?
- [ ] Есть ли ежедневный бэкап system state контроллеров домена помимо корзины?
- [ ] Известно ли, кто и по какой процедуре восстанавливает объекты вне рабочих часов?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Включаем корзину AD, поднимаем функциональный уровень леса и задаём срок хранения 365 дней
- Делегируем восстановление отдельной группе, настраиваем аудит удалений и алерты в Telegram
- Передаём скрипт пакетного восстановления OU и учёток по lastKnownParent с логированием
- Настраиваем бэкап system state контроллеров и проводим учебное восстановление раз в квартал
- Делаем аудит домена: FSMO, репликация, защита OU от удаления, отчёт с планом работ

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Advanced AD DS Management Using ADAC (Level 200): Recycle Bin (learn.microsoft.com — 2025)

02 Enable-ADOptionalFeature (модуль ActiveDirectory) (learn.microsoft.com — WS2025)

03 Restore-ADObject: TargetPath, IncludeDeletedObjects (learn.microsoft.com — WS2025)

04 Appendix A: Additional AD Recycle Bin Tasks — DOL и делегирование (learn.microsoft.com — WS2008R2)

05 Garbage-Coll-Period attribute, AD Schema (1–168 ч) (learn.microsoft.com — 2025)

06 Audit Directory Service Changes: события 5136–5141 (learn.microsoft.com — 2025)

07 Чек-лист ITfresh «AD Recycle Bin: включение, делегирование, аудит» (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.