



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Корзина Active Directory: восстановление удалённых объектов

Как мы включаем AD Recycle Bin, делегируем Reanimate Tombstones и держим RTO 15 минут

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Удаление OU в AD — мгновенная потеря доступа у целого подразделения: рвутся членства в группах, перестают работать NTFS-ACL на шарах и публикациях 1С, слетают gPLink. Без включённой корзины остаётся tombstone без атрибутов либо authoritative restore из system state с загрузкой DC в DSRM. Мы закрываем это заранее: включаем Recycle Bin, пишем рантбук, делегируем восстановление.

Почему это важно бизнесу

- Удалённая OU на 90 человек — стоп отдела: нет входа в домен, 1С, почту и файловые шары до полного восстановления.
- Без корзины единственный путь — authoritative restore из системного стеита с загрузкой DC в DSRM и простым каталогом.
- Потеря членств в группах ломает разграничение доступа: часть людей теряет права, часть получает лишние.
- Инцидент вечером пятницы без рантбука превращается в выходные на восстановление и оплату сверхурочных.
- Проверяющим нужно показать, кто и когда удалил учётную запись, — без аудита каталога ответа нет.



Ключевые параметры реализации

180 дней

tombstoneLifetime лесов на WS2003 SP1 и новее; пустой msDS-DeletedObjectLifetime берёт это зна...

MS-ADTS, разд. 6.1.1.2.4.1.1

2 дня

Минимум msDS-DeletedObjectLifetime: значение меньше трактуется как 2 дня; мы не опускаем ниже...

MS-ADTS, Deleted-Object Lifetime

12 ч

garbageCollPeriod по умолчанию; tombstoneLifetime обязан быть больше 3х интервала, иначе откат...

AD Schema, Garbage-Coll-Period

2008 R2

Минимальные FFL и DFL для включения корзины; на WS2025 доступен уровень 10

AD DS Functional Levels

365 дней

Наше значение lifetime для клиник и бухгалтерий с длинным циклом разбора удалений

стандарт ITfresh

10-15 мин

RTO рантбука на возврат OU со 100+ объектами двумя проходами Restore-ADObject

стандарт ITfresh



Включение Recycle Bin в лесу заказчика

Что настраиваем

Лес corp.*.ru, 1-3 DC на WS2019/2022; работаем на контроллере с ролями Schema Master и Domain Naming Master корневого домена

Как мы это делаем

- 1 Снимаем Get-ADForest | Select ForestMode и Get-ADDomain | Select DomainMode: нужен уровень не ниже Windows2008R2Forest/Domain, иначе сначала поднимаем FFL и DFL.
- 2 Делаем system state всех DC через wbadmin start systemstatebackup и проверяем repadmin /replsummary — включение необратимо, отключить фичу нельзя.
- 3 Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=...' -Scope Fores...
- 4 Проверяем Get-ADOptionalFeature: в EnabledScopes появляются DN Partitions и DN домена; ждём сходимости Configuration NC на всех DC.
- 5 Правим msDS-DeletedObjectLifetime на CN=Directory Service,CN=Windows NT,CN=Services: 180 дней штатно, 365 для регулируемых отраслей.

РЕЗУЛЬТАТ

Удалённый объект хранится целиком: objectSid, objectGUID, link-valued атрибуты member и memberOf. Восстановление возвращает пользователя в ту же OU с теми же правами на шары, базы 1С и почтовый ящик — прикладные сервисы инцидента не замечают.

КЛЮЧЕВОЙ НЮАНС

По документации AD DS хватает Domain Admins того домена, где включаем фичу. Если командлет падает — сводим Schema Master и Domain Naming Master на один DC корневого домена и запускаем именно там.



Рантбук: возврат удалённой OU за два прохода

Что настраиваем

Доменный раздел и контейнер CN=Deleted Objects; работаем на владельце PDC Emulator под Tier-0 учёткой — на RODC и снапшоте Restor...

Как мы это делаем

- 1 Фиксируем окно инцидента: `Get-ADObject -Filter 'isDeleted -eq $true -and -not (isRecycled -eq $true)' -IncludeDeletedObjects -Properties *` с выгрузкой в CSV.
- 2 Проход 1 — сами OU: `Restore-ADObject` берёт имя из `msDS-lastKnownRDN` и место из `lastKnownParent`; без родительского контейнера дочерние объекты не лягут.
- 3 Проход 2 — фильтр по `lastKnownParent = DN` восстановленной OU, затем `Restore-ADObject`; при конфликте `sAMAccountName` или `UPN` добавляем `-TargetPath` и `-NewName`.
- 4 Контроль: `repadmin /showobjmeta` по объекту-образцу, тестовый вход 3-4 пользователей, сверка `gPLink` на OU и членств в критичных группах.
- 5 Если снесён и GPO — из корзины вернётся только `groupPolicyContainer`, содержимое GPT в `SYSVOL` накатываем `Restore-GPO` из еженедельного Backup-GPO.

РЕЗУЛЬТАТ

Возврат OU со 100+ объектами укладывается в 10-15 минут без остановки контроллеров и без DSRM. SID и членства сохраняются, поэтому NTFS-ACL, доступы к базам 1С и почтовые права не требуют ручной перевыдачи.

КЛЮЧЕВОЙ НЮАНС

ADAC (`dsac.exe`) показывает Deleted Objects только доменного раздела. Объекты из `Configuration`, `DomainDnsZones` и `ForestDnsZones` достаём `Get-ADObject -SearchBase 'CN=Deleted Objects,CN=Configuration,DC=...'` и во...



Аудит удалений и восстановление без прав Domain Admins

Что настраиваем

GPO на Default Domain Controllers Policy и SACL на корне раздела; группа AD-Restore-Operators вместо Tier-0 у сервисдеска

Как мы это делаем

- 1 Включаем подкатегории Audit Directory Service Changes и Audit Directory Service Access, вешаем SACL на Delete и Delete Subtree для корня NC и критичных OU — без SAC...
- 2 Собираем 5141 (Directory Service Changes), 4726 и 4743 (Audit User и Computer Account Management) в Zabbix; порог 5 удалений за 10 минут от одного SID — алерт в Tel...
- 3 Делегируем: dscls на корне NC даёт право Reanimate Tombstones; на CN=Deleted Objects сначала /takeOwnership, затем LCRP; на целевых OU — WPCC для записи и создания...
- 4 Массовая защита: Get-ADOrganizationalUnit -Filter * | Set-ADOrganizationalUnit -ProtectedFromAccidentalDeletion \$true, включая вновь создаваемые OU.
- 5 Раз в полгода поднимаем клон леса из system state в изолированной сети и прогоняем рантбук с замером времени обоих проходов.

РЕЗУЛЬТАТ

Массовое удаление видно в течение минут, а не после звонков пользователей. Восстановление выполняет дежурный инженер без выдачи Domain Admins, что снимает постоянный Tier-0 доступ у первой линии поддержки.

КЛЮЧЕВОЙ НЮАНС

Одного права Reanimate Tombstones мало: нужны LCRP на CN=Deleted Objects (только после dscls /takeOwnership) и права CC и WP на целевой OU, иначе Restore-ADObject падает с Access denied.



Подводные камни

✗ Ждут от корзины старых удалений

Recycle Bin работает только с момента включения. Объекты, удалённые раньше, становятся recycled и в контейнере Deleted Objects больше не видны.

✗ Восстанавливают содержимое раньше OU

Restore-ADObject кладёт объект по lastKnownParent. Нет родительской OU — команда падает. Всегда два прохода: сначала контейнеры, потом их содержимое.

✗ Снижают msDS-DeletedObjectLifetime

Минимум 2 дня, и значение реально применяется. Ставим 180-365 и держим tombstoneLifetime больше 3х garbageCollPeriod, иначе значение откатится к дефо...

✗ Считают корзину заменой бэкапу

Она не спасает от повреждения NTDS.dit, отката схемы и потери SYSVOL. System state контроллеров и Backup-GPO остаются обязательными.

✗ Забывают про SYSVOL при удалении GPO

Из корзины вернётся только groupPolicyContainer в каталоге; файлы GPT в SYSVOL восстанавливаются командой Restore-GPO из бэкапа GPMC.

✗ Включают фичу без учёта FSMO

Командлету нужны доступные Schema Master и Domain Naming Master. При ошибке роли сводим на один DC корневого домена и запускаем оттуда.

✗ Не проверяют репликацию до включения

Операция меняет Configuration NC всего леса. При лагах часть DC уходит в рассинхрон, поэтому сначала добиваемся чистого repadmin /replsummary.

✗ Запускают restore на RODC

Restore-ADObject не работает ни на read-only DC, ни на снапшоте AD. Рантбук всегда исполняем на RW-DC, у нас — на владельце PDC Emulator.



Как правильно

МИНИМУМ

- FFL и DFL не ниже Windows2008R2, корзина включена во всём лесу
- ProtectedFromAccidentalDeletion на всех OU и критичных группах
- System state двух DC раз в неделю; копия старше tombstoneLifetime непригодна

НОРМАЛЬНО

- msDS-DeletedObjectLifetime 180-365, garbageCollPeriod оставляем 12 ч
- Аудит 5141, 4726 и 4743 с алертом в Telegram при всплеске удалений
- Письменный рантбук: два прохода Restore-ADObject и контрольный вход
- Еженедельный Backup-GPO и выгрузка структуры OU, групп, членств

ХОРОШО

- Reanimate Tombstones делегирован отдельной группе, а не Domain Admins
- Полугодовая тренировка восстановления на клоне леса из system state
- Счётчик Get-ADObject -IncludeDeletedObjects в Zabbix: триггер на +50 за час
- Снятие ProtectedFromAccidentalDeletion ловим аудитом 5136 по nTSecurityDescriptor



Чек-лист самопроверки

☐ Включена ли корзина: Get-ADOptionalFeature показывает EnabledScopes для леса?

☐ Проверены ли уровни леса и домена — не ниже Windows2008R2Forest/Domain?

☐ Известно ли текущее значение msDS-DeletedObjectLifetime и кто его менял?

☐ Стоит ли ProtectedFromAccidentalDeletion на всех OU, включая созданные вчера?

☐ Есть ли system state двух DC свежее tombstoneLifetime и проверялось ли восстановление?

☐ Настроен ли аудит 5141, 4726 и 4743 и есть ли SACL на Delete у критичных OU?

☐ Делегировано ли восстановление без постоянной выдачи прав Domain Admins?

☐ Есть ли письменный рантбук с двумя проходами Restore-ADObject?

☐ Делается ли Backup-GPO еженедельно — GPT в SYSVOL корзина не вернёт?

☐ Проводилась ли учебная тревога по возврату OU за последние полгода?

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



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).

- Аудит леса: функциональные уровни, репликация, наличие корзины и защиты OU от удаления
- Включение AD Recycle Bin под ключ с бэкапом DC и контролем сходимости Configuration NC
- Настройка SACL, подкатегорий аудита и алертов в Telegram по событиям 5141, 4726 и 4743
- Делегирование Reanimate Tombstones и рантбук восстановления для вашей ИТ-службы
- Учебное восстановление OU на клоне леса и обучение дежурных инженеров заказчика

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



Техническая база

- 01** Enable Active Directory Recycle Bin in Windows Server (learn.microsoft.com — 2025)
- 02** [MS-ADTS] Tombstone Lifetime и Deleted-Object Lifetime, 6.1.1.2.4.1.1 (learn.microsoft.com — 2026)
- 03** Restore-ADObject и Get-ADObject, модуль ActiveDirectory (WS2025) (learn.microsoft.com — 2025)
- 04** Garbage-Coll-Period attribute, AD Schema (learn.microsoft.com — 2020)
- 05** Restoring Deleted Objects, AD SDK: права Reanimate Tombstones (learn.microsoft.com — 2021)
- 06** Event 5141(S): A directory service object was deleted (learn.microsoft.com — 2026)
- 07** AD DS Functional Levels, включая WS2025 (уровень 10) (learn.microsoft.com — 2025)
- 08** Рантбук ITfresh: возврат OU за два прохода (itfresh.ru — 2026)

