Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

0xaac при повторном вводе ПК в домен: allowlist владельцев

KB5020276, ms-DS-CreatorSID и GPO trusted owners для делегированного helpdesk

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Мы выдаём helpdesk права на компьютерные объекты в OU, но повторный ввод в домен уже существующей машины падает с 0xaac. Причина не в ACL: join hardening (KB5020276, закрывает CVE-2022-38042) сверяет создателя объекта (mS-DS-CreatorSID) с identity джойнящего, и без allowlist-владельца на DC блокирует reuse даже при полных правах на объект.

Почему это важно бизнесу

- Каждый повторный ввод «зависшего» ПК превращается в эскалацию к администратору домена — SLA на массовые заявки срывается
- Хелпдеск с делегированными правами не может закрыть тикет сам — простой сотрудника на переустановке растягивается с часов до дней
- Ручной обход через реестровый ключ снижает защиту от CVE-2022-38042 и остаётся незамеченным в аудите безопасности
- При массовом re-imaging (десятки-сотни ПК через SCCM/MDT) блокировка 0xaac размножается по всей партии и срывает график миграции
- Незакрытые тикеты копятся в очереди — растёт стоимость эскалаций на 2-3 линию поддержки

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

0xaac

код 2732 NERR_AccountReuseBlockedByPolicy — join блокирован проверкой владельца, а не ACL объе…

KB5020276

14.03.2023

обновления этой даты вводят GPO-параметр allowlist владельцев и расширяют список исключений

по докам KB5020276

12.09.2023

с этой даты проверка reuse выполняется контроллером домена через SAMRPC — политика применяется…

по докам KB5020276

MAQ=10

дефолтная ms-DS-MachineAccountQuota — сколько объектов юзер заводит сам без делегирования

AD DS, наш стандарт

4101

Event ID в журнале System клиента (источник Netjoin) при блокировке reuse; 4100 — reuse разреш…

System, источник Netjoin

13.08.2024

обновления от этой даты убирают поддержку ключа NetJoinLegacyAccountReuse

по докам KB5020276

РЕАЛИЗАЦИЯ 1 ИЗ 3

Allowlist владельцев на контроллерах домена

Что настраиваем

Делегированный helpdesk (группа SG-Helpdesk-Join) на Windows Server 2025, все DC сайта, OU Workstations

Как мы это делаем

1. Открываем GPO, привязанную к OU Domain Controllers, → Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options
2. В «Domain controller: Allow computer account re-use during domain join» через object picker добавляем группу SG-Helpdesk-Join, а не отдельных инженеров
3. gpupdate /force на всех DC сайта, ждём репликации SYSVOL и применения политики на площадке
4. Проверяем на тестовом стенде join/re-join от имени члена SG-Helpdesk-Join — 0xaac должен исчезнуть
5. Фиксируем успешный join по Netsetup.log клиента, событию 4100 (Netjoin) на клиенте и 16995 (Directory-Services-SAM) на DC

РЕЗУЛЬТАТ

Хелпдеск закрывает переустановку и re-imaging сам, без эскалации на администратора домена; массовые волны переустановок проходят без ручного вмешательства в каждую машину.

КЛЮЧЕВОЙ НЮАНС

Allowlist настраивается на контроллерах домена, а не через ACL объекта компьютера — обычные права Create/Delete Computer Objects эту проверку не обходят.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Диагностика по mS-DS-CreatorSID и Netsetup.log

Что настраиваем

Стенд re-imaging через SCCM/MDT, сервисная учётка SVC-MDT-Join, OU Workstations

Как мы это делаем

1. Смотрим C:\Windows\Debug\Netsetup.log на клиенте — ищем строку NetpJoinDomain/NetpValidateName и код 0xaac
2. На клиенте проверяем System-событие 4101 (Netjoin), на DC — 16997/16998 источника Directory-Services-SAM
3. На DC сверяем, чей SID записан создателем объекта: Get-ADComputer -Properties mS-DS-CreatorSID,ntSecurityDescriptor
4. Если объект создавался вручную доменным админом или скриптом без делегирования — CreatorSID не заполнен, reuse блокируется для всех вне allowlist
5. Для одиночных зависших машин удаляем stale-объект и даём SVC-MDT-Join завести объект заново

РЕЗУЛЬТАТ

SCCM/MDT task sequence проходит без ручных правок реестра на образе; повторные волны деплоя не спотыкаются об уже существующие объекты.

КЛЮЧЕВОЙ НЮАНС

Смотрим не только на ACL, а на то, кто фактически СОЗДАЛ объект — hardening сверяет identity создателя, а не текущие права на объект.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Контролируемый временный обход на переходный период

Что настраиваем

Пилотная группа из нескольких ПК до согласования постоянной GPO-политики на DC

Как мы это делаем

1. HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters, REG_DWORD NetJoinLegacyAccountReuse=1 — работает только на клиентах с обновлениями ДО 13.08.2024
2. Выполняем join/re-join, сразу после успеха удаляем ключ — не оставляем его постоянно на образе или в GPO
3. Фиксируем факт временного обхода в тикете как technical debt на закрытие через нормальный allowlist
4. Переносим машину в постоянный сценарий (allowlist-группа SG-Helpdesk-Join) при следующем плановом обслуживании

РЕЗУЛЬТАТ

Закрываем единичные горящие тикеты без ожидания согласования GPO-изменения на DC, не оставляя защиту от CVE-2022-38042 снятой навсегда.

КЛЮЧЕВОЙ НЮАНС

Реестровый обход — не конфигурация, а костыль: с обновлений от 13.08.2024 hardening работает независимо от ключа, и обход перестаёт действовать.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Путаем ACL и allowlist reuse**
  Create/Delete Computer Objects управляют тем, кто МОЖЕТ создать объект, но не снимают проверку CreatorSID при повторном join — это разные механизмы.

- ✕ **Добавляем людей, а не группу**
  Персональные учётки в allowlist ломаются при ротации helpdesk-состава; заводим группу SG-Helpdesk-Join и меняем членство, а не саму GPO.

- ✕ **Забываем про репликацию GPO на DC**
  Политика на OU Domain Controllers применяется только после репликации SYSVOL и gpupdate — тестируем join не раньше чем через 15-20 минут.

- ✕ **Оставляем реестровый обход навсегда**
  NetJoinLegacyAccountReuse снимает защиту от CVE-2022-38042, а с обновлений от 13.08.2024 hardening действует независимо от ключа — это временный кост…

- ✕ **Пре-стейджим объект не той учёткой**
  Если объект создаёт администратор, а джойнит сервисная учётка деплоя — CreatorSID не совпадает, и без allowlist всё равно заблокировано.

- ✕ **Не проверяем Netsetup.log**
  Без C:\Windows\Debug\Netsetup.log и события 4101 (Netjoin) в System клиента не видно, что блокировка — именно hardening-политика, а не занятое имя ил…

- ✕ **Держим MachineAccountQuota=10**
  Дефолтные 10 объектов на любого аутентифицированного пользователя позволяют создавать «ничьи» компьютерные объекты без делегирования.

- ✕ **Настраиваем политику на клиенте, не на DC**
  С обновлений от 12.09.2023 проверка reuse выполняется контроллером домена по SAMRPC — локальная политика на рабочей станции на неё не влияет.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Задокументировать, кто и какой учёткой создаёт компьютерные объекты в OU
- Проверять Netsetup.log и событие 4101 (Netjoin) в System клиента перед эскалацией лю…
- Не использовать реестровый обход дольше одного join-сеанса

НОРМАЛЬНО

- Завести группу SG-Helpdesk-Join и внести её в allowlist на всех DC
- Пре-стейджить объекты той же сервисной учёткой, что джойнит при деплое
- Настроить MachineAccountQuota=0 и делегировать Create/Delete Computer Objects явно

ХОРОШО

- Автоматизировать проверку mS-DS-CreatorSID перед массовым re-imaging скриптом
- Собирать в центральный лог события 16995-16998 (Directory-Services-SAM) с DC и 4100/…
- Вести регламент ротации allowlist-группы синхронно с оргштатом helpdesk
- Раз в квартал сверять GPO allowlist с фактическим составом делегированных прав в OU

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть отдельная GPO «Allow computer account re-use during domain join» на OU Domain Controllers?
- [ ] В allowlist добавлена группа helpdesk, а не отдельные учётки инженеров?
- [ ] MachineAccountQuota приведена к 0 и права на OU делегированы явно?
- [ ] Сервисная учётка деплоя (SCCM/MDT) совпадает с той, что пре-стейджит объекты?
- [ ] Проверяются Netsetup.log и событие 4101 (Netjoin) на клиенте перед эскалацией тикета на 3 линию?
- [ ] Реестровый ключ NetJoinLegacyAccountReuse не оставлен постоянно ни на одной машине?
- [ ] GPO реплицирована на все DC сайта и подтверждена через gpupdate /force?
- [ ] На DC установлены обновления от 12.09.2023 и новее, иначе allowlist не обрабатывается?
- [ ] Есть регламент удаления stale-объектов компьютеров перед повторным join?
- [ ] Ведётся учёт, кто фактически создал (CreatorSID) каждый пре-стейджед объект?

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).

- Настраиваем allowlist владельцев на всех DC и делегируем helpdesk-группе join/reuse без эскалаций
- Пересматриваем MachineAccountQuota и делегирование Create/Delete Computer Objects по OU
- Разворачиваем сбор событий 4100/4101 клиентов и 16995-16998 с DC для раннего обнаружения блокировок re-imaging
- Готовим сервисные учётки и пре-стейджинг для SCCM/MDT так, чтобы CreatorSID не ломал повторный join
- Проводим аудит и убираем оставленные реестровые обходы NetJoinLegacyAccountReuse

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 KB5020276 — Netjoin: Domain join hardening changes (support.microsoft.com — 2022-2024)

02 Failure When You Use an Existing Computer Account to Join a Domain (learn.microsoft.com — 2024)

03 Domain controller: Allow computer account re-use during domain join (learn.microsoft.com — 2023-2024)

04 CVE-2022-38042 — AD DS Elevation of Privilege (msrc.microsoft.com — 2022)

05 Active Directory Domain Services functional levels (learn.microsoft.com — 2025)

06 ms-DS-MachineAccountQuota attribute (learn.microsoft.com — 2023)

07 Delegation of Control — Create/Delete Computer objects (learn.microsoft.com — 2023)

08 Наш шаблон делегирования и allowlist для helpdesk (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.