Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

RDP «Произошла внутренняя ошибка»: точная диагностика

Зонтичная ошибка mstsc: 5 причин на сервере — от сертификата TermService до Grace Period RDS

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Утром пользователи не заходят на терминальный сервер: mstsc выдаёт «Произошла внутренняя ошибка» сразу после ввода логина, хотя порт 3389 слушает. Это зонтичная ошибка клиента — под ней прячется до пяти сбоев на сервере: сломанный самоподписанный сертификат TermService, потеря прав на MachineKeys, ошибка Schannel при доступе к закрытому ключу, истёкший Grace Period RDS. Простой стоит денег, а гадание вслепую — часов.

Почему это важно бизнесу

- Терминальный сервер — единственная точка входа для десятков сотрудников: пока он молчит, встаёт вся смена.
- Слепой перебор причин растягивает простой на часы; точная диагностика по журналам закрывает инцидент за 15 минут.
- Перезагрузка «на удачу» рвёт активные сессии и несохранённые данные — мы чиним без ребута до последнего шага.
- Истёкший Grace Period блокирует новые входы даже при оплаченных CAL: деньги за лицензии есть, а работать нельзя.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

5

Пять серверных причин за одной ошибкой mstsc — диагностируем по журналам, а не угадываем

наша практика RDS

1057

EventID 1057: TermService не смог создать самоподписанный сертификат для SSL

журнал System Windows

36870

EventID 36870 Schannel: нет доступа к закрытому ключу TLS-сертификата сервера

по докам Schannel

120 дней

Grace Period RDS: пробный период лицензирования, после нуля новые входы блокируются

по докам Microsoft RDS

0x80090008

NTE_BAD_ALGID: legacy SChannel-провайдер ломает New-SelfSignedCertificate

по докам CNG/SChannel

1

SecurityLayer=1 (Negotiate): пробует TLS, откатывается на RDP — наш стандарт слушателя

по докам RDP WinStations

РЕАЛИЗАЦИЯ 1 ИЗ 3

Первичная диагностика по журналам через WinRM

Что настраиваем

Windows Server 2019, роль RD Session Host; доступ только по WinRM 5985/5986, RDP лежит

Как мы это делаем

1. Подключаемся по WinRM (pywinrm, транспорт NTLM) — когда RDP молчит, это единственный живой канал управления на сервер.
2. Проверяем службу: sc query TermService — статус RUNNING, порт 3389 в LISTENING (netstat, qwinsta), значит сервер жив, проблема глубже TCP.
3. Читаем System через wevtutil qe с фильтром на EventID 1057 (RemoteConnectionManager) и 36870 (Schannel) — сразу виден след сертификата.
4. 1057 = не создан самоподписанный сертификат; 36870 с кодом 0x8009030D = нет доступа к закрытому ключу TLS. Диагноз — цепочка вокруг MachineKeys.

РЕЗУЛЬТАТ

За минуты локализуем корень без гадания: клиентская «внутренняя ошибка» раскладывается на конкретные EventID и код Schannel. Работаем удалённо, активные сессии не трогаем.

КЛЮЧЕВОЙ НЮАНС

EventID 1057 говорит, что сертификат не создан, 36870 — что к ключу нет доступа; вместе они указывают на MachineKeys, а не на сеть или NLA. Смотрим оба события, а не одно.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Чиним MachineKeys и пересоздаём сертификат RDP

Что настраиваем

MachineKeys (C:\ProgramData\Microsoft\Crypto\RSA) и слушатель RDP-Tcp на RD Session Host

Как мы это делаем

1. Корень: TermService работает под NETWORK SERVICE и не может писать закрытый ключ — в MachineKeys нет доступа для служебной учётки, папка пуста.
2. Возвращаем права: icacls на MachineKeys /grant для NETWORK SERVICE и SYSTEM — TermService снова может писать и читать закрытый ключ сертификата.
3. Пересоздаём сертификат: New-SelfSignedCertificate в Cert:\LocalMachine\My без ключа -Provider — иначе legacy SChannel-провайдер даёт NTE_BAD_ALGID.
4. Привязываем: кладём сертификат в хранилище Remote Desktop и пишем его thumbprint в Win32_TSGeneralSetting.SSLCertificateSHA1Hash для RDP-Tcp.

РЕЗУЛЬТАТ

После возврата прав очередь запросов на ключи отрабатывает разом: папка наполняется, Schannel получает доступ к ключу, RDP-хендшейк по SSL проходит. Сертификат выписываем с запасом по сроку.

КЛЮЧЕВОЙ НЮАНС

Ключевой нюанс — не указывать -Provider «Microsoft RSA SChannel Cryptographic Provider»: он держит только SHA1 и валит генерацию SHA256-сертификата в NTE_BAD_ALGID. Пусть CNG выберет провайдер сам.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Снимаем истёкший Grace Period и фиксируем SecurityLayer

Что настраиваем

Ключ RCM\GracePeriod и WinStations\RDP-Tcp; роль RDS-Licensing с пулом CAL на сервере

Как мы это делаем

1. Grace Period RDS — 120 дней с установки роли; хранится в HKLM\...\Terminal Server\RCM\GracePeriod как REG_BINARY с именем L$RTMTIMEBOMB.
2. Ключ защищён ACL — админ напрямую не удалит; создаём разовую задачу планировщика от NT AUTHORITY\SYSTEM, она делает Remove-Item, затем задачу снимаем.
3. Фиксируем безопасность слушателя: SecurityLayer=1 (Negotiate) и UserAuthentication=1 (NLA включён) в WinStations\RDP-Tcp — баланс TLS и отказоустойчивости.
4. Рестарт: Restart-Service TermService — слушатель поднимается с новым сертификатом; проверяем qwinsta (rdp-tcp Listen) и протокольным тестом X.224.

РЕЗУЛЬТАТ

Новые подключения снова принимаются даже при живом лицензном сервере: истёкший GracePeriod больше не блокирует вход. SecurityLayer=1 держит SSL там, где он есть, и не роняет вход при проблеме с сертификатом.

КЛЮЧЕВОЙ НЮАНС

Даже при тысячах свободных CAL истёкшая метка L$RTMTIMEBOMB имеет приоритет и режет входы. Сброс Grace Period — не замена лицензиям: лицензный сервер и CAL должны быть настроены.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Гадание вместо чтения журнала**
  «Внутренняя ошибка» ничего не говорит клиенту. Мы не перебираем причины наугад, а читаем System: EventID 1057 и 36870 сразу задают вектор.

- ✕ **Перезагрузка «на всякий случай»**
  Ребут рвёт активные сессии и несохранённые данные, а корень (права MachineKeys) не лечит. Чиним по WinRM без рестарта до последнего шага.

- ✕ **Явный -Provider в сертификате**
  New-SelfSignedCertificate с явным «Microsoft RSA SChannel Cryptographic Provider» даёт NTE_BAD_ALGID. Убираем -Provider — CNG выберет провайдер сам.

- ✕ **Лечим сертификат, забыв про ключи**
  Новый сертификат бесполезен, если у NETWORK SERVICE нет доступа к MachineKeys: Schannel всё равно упадёт 0x8009030D. Сначала права, потом сертификат.

- ✕ **Уверенность, что CAL спасут**
  Пул из тысяч CAL не помогает, пока в RCM\GracePeriod висит истёкший L$RTMTIMEBOMB — этот ключ приоритетнее и блокирует новые входы.

- ✕ **Удаление GracePeriod из-под админа**
  Ключ защищён ACL, обычный админ его не сотрёт. Нужна задача планировщика от NT AUTHORITY\SYSTEM с Remove-Item, иначе Access Denied.

- ✕ **SecurityLayer=2 без сертификата**
  Строгий SSL/TLS требует валидный сертификат; при любой проблеме с ключом вход намертво падает. Держим SecurityLayer=1 (Negotiate) как безопасный дефолт.

- ✕ **Диагностика только порта**
  TcpClient(3389) покажет, что порт открыт, но не проверит протокол. Мы шлём X.224 Connection Request и ждём байт 0xD0 — реальный RDP-хендшейк.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Держать открытым WinRM (5985/5986) как аварийный канал, когда RDP лёг
- Знать связку EventID 1057 и 36870 — первый маркер проблемы с сертификатом RDP
- Проверить SecurityLayer в WinStations\RDP-Tcp: не строгий ли 2 без сертификата

НОРМАЛЬНО

- Права на MachineKeys для NETWORK SERVICE и SYSTEM под контролем конфигурации
- SecurityLayer=1 и UserAuthentication=1 (NLA) как зафиксированный стандарт слушателя
- Настроенный лицензный сервер RDS с активными CAL, а не жизнь на Grace Period
- Сертификат RDP с запасом по сроку, чтобы не ловить внезапный отказ SSL

ХОРОШО

- Плановый контроль Grace Period и метки L$RTMTIMEBOMB до её истечения
- Валидный TLS-сертификат от внутреннего PKI вместо самоподписанного на слушателе
- Протокольный мониторинг RDP (X.224-хендшейк), а не только проверка порта 3389
- Runbook на «внутреннюю ошибку»: удалённый разбор по WinRM без ребута и потери сессий

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] В журнале System нет свежих EventID 1057 (TerminalServices-RemoteConnectionManager)?
- [ ] Нет ли EventID 36870 Schannel с кодом 0x8009030D — доступа к закрытому ключу TLS?
- [ ] У NETWORK SERVICE и SYSTEM есть доступ к папке MachineKeys, и она не пуста?
- [ ] Сертификат RDP пересоздан без явного -Provider (нет ошибки NTE_BAD_ALGID)?
- [ ] Thumbprint привязан к RDP-Tcp через Win32_TSGeneralSetting.SSLCertificateSHA1Hash?
- [ ] SecurityLayer=1 (Negotiate) и UserAuthentication=1 (NLA) в WinStations\RDP-Tcp?
- [ ] Grace Period не на нуле, а ключ L$RTMTIMEBOMB не истёк и не блокирует входы?
- [ ] Лицензный сервер RDS настроен и в пуле есть активные CAL?
- [ ] После правок TermService перезапущен, qwinsta показывает rdp-tcp в Listen?
- [ ] RDP проверен протокольным тестом X.224 (ответ 0xD0), а не только открытием порта?

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).

- Удалённо диагностируем «внутреннюю ошибку» RDP по WinRM — без перезагрузки и потери активных сессий
- Восстанавливаем права MachineKeys и пересоздаём рабочий SSL-сертификат слушателя RDP-Tcp
- Снимаем истёкший Grace Period RDS через задачу от SYSTEM и подключаем лицензный сервер с CAL
- Фиксируем стандарт слушателя: SecurityLayer=1, NLA, сертификат с запасом по сроку
- Пишем runbook под ваш терминальный сервер, чтобы инцидент закрывался за 15 минут

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 Default permissions for MachineKeys folders (KB278381) (learn.microsoft.com — 2026)

02 Guidance for troubleshooting RDS Licensing (learn.microsoft.com — 2026)

03 Remote Desktop listener certificate configurations (learn.microsoft.com — 2026)

04 SecurityLayer / UserAuthentication (RDP WinStationExtensions) (learn.microsoft.com — 2026)

05 An internal error has occurred connecting to remote machine (learn.microsoft.com — 2026)

06 Event ID 1057: failed to create self-signed certificate (learn.microsoft.com — 2026)

07 Win32_TSGeneralSetting (SSLCertificateSHA1Hash) (learn.microsoft.com — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.