Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Windows LAPS: уникальный пароль локального админа

Наш регламент: схема AD, шифрование DPAPI-NG, ротация 30 дней, аудит чтения пароля

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Почти в каждой сети, которую мы принимаем на обслуживание, пароль локального админа одинаков на всех ПК и достался от прошлого подрядчика. Один снятый с ноутбука NTLM-хеш открывает весь парк: боковое перемещение, сбор сессий, эскалация до доменного админа. Закрываем это Windows LAPS: каждой машине свой случайный пароль в атрибутах AD, при включённом шифровании — зашифрованный.

Почему это важно бизнесу

- Компрометация одного ПК перестаёт означать компрометацию всего парка рабочих мест
- Увольнение инженера не требует обхода 50 машин со сменой пароля вручную
- Helpdesk чинит профиль и офлайн-вход без выдачи универсального пароля на руки
- Каждое чтение пароля именное и логируется — есть что показать аудитору и страховщику
- Лицензий и агентов не нужно: LAPS встроен в Windows 10/11 и Windows Server 2019+

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

11.04.2023

LAPS вошёл в состав Windows обновлениями от 11 апреля 2023 года

learn.microsoft.com

8–64

PasswordLength: диапазон 8-64 символа, по умолчанию 14; мы ставим 20

learn.microsoft.com

1–365

PasswordAgeDays: диапазон 1-365 дней, по умолчанию 30; наш регламент — 30

learn.microsoft.com

1 час

Фоновая задача LAPS обрабатывает политику раз в час, интервал не настраивается

learn.microsoft.com

0–24 ч

PostAuthenticationResetDelay: grace-период после входа, по умолчанию 24 часа

learn.microsoft.com

DFL 2016

Шифрование пароля в AD (CNG DPAPI) требует уровня домена 2016 и выше

learn.microsoft.com

РЕАЛИЗАЦИЯ 1 ИЗ 3

Развёртывание с нуля в домене на 40-60 рабочих мест

Что настраиваем

Типовой клиент: бухгалтерия или юрфирма, один DC Windows Server 2019, парк Windows 10 22H2 и Windows 11

Как мы это делаем

1. Проверяем уровень домена (для шифрования нужен DFL 2016+) и накат обновлений от 11.04.2023 и новее на DC и клиентов
2. Под Schema Admins — Update-LapsADSchema: в лес добавляются msLAPS-Password, msLAPS-PasswordExpirationTime, msLAPS-EncryptedPassword и msLAPS-EncryptedPasswordHistory
3. На OU компьютеров: Set-LapsADComputerSelfPermission, затем Set-LapsADReadPasswordPermission и Set-LapsADResetPasswordPermission с -AllowedPrincipals
4. GPO 'LAPS - Workstations' в разделе Administrative Templates > System > LAPS: BackupDirectory = 2 (AD), PasswordLength 20, PasswordComplexity 4, PasswordAgeDays 30
5. Включаем ADPasswordEncryptionEnabled и задаём ADPasswordEncryptionPrincipal = LAPS_Readers: расшифровать пароль сможет только эта группа

РЕЗУЛЬТАТ

Обычно за 2 рабочих дня 90-95% включённых машин отдают в AD уникальный 20-символьный пароль; остальное добираем по мере появления ноутбуков в сети. Универсальный пароль выводится из обращения, доступ к паролю остаётся только у именной группы helpdesk.

КЛЮЧЕВОЙ НЮАНС

Схему расширяем один раз на лес и заранее: без атрибутов клиент не сохраняет пароль, а в журнале LAPS копятся ошибки записи в каталог.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Отдельная управляемая учётка вместо встроенного Administrator

Что настраиваем

Клиент с парком, где встроенный Administrator включён и переименован по-разному на разных ПК

Как мы это делаем

1. Через GPO или RestrictedGroups создаём локальную учётку (например it-local) и вводим её в локальную группу Администраторы на всех ПК
2. В политике LAPS задаём AdministratorAccountName = it-local; без этого параметра LAPS управляет встроенным админом по его RID -500
3. PostAuthenticationActions оставляем 3 (сброс пароля и завершение сеанса), PostAuthenticationResetDelay 24 часа: временный пароль живёт максимум сутки
4. Включаем историю: ADEncryptedPasswordHistorySize (0-12, по умолчанию 0) работает только при включённом шифровании и SELF-праве машины на чтение
5. Форс-ротацию делаем Reset-LapsPassword на машине или Set-LapsADPasswordExpirationTime со стороны AD

РЕЗУЛЬТАТ

Атака на предсказуемую учётку с RID -500 теряет смысл, а любой выданный helpdesk пароль автоматически сбрасывается после использования. Восстановление старого диска или снапшота остаётся возможным благодаря истории зашифрованных паролей.

КЛЮЧЕВОЙ НЮАНС

Учётку нужно создать ДО применения политики: Windows LAPS не создаёт аккаунт сам и просто пишет ошибку в свой журнал.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Аудит чтения паролей и контроль привилегий

Что настраиваем

Клиенты с внешним пентестом или требованиями страховщика к зрелости ИТ-процессов

Как мы это делаем

1. Set-LapsADAuditing -Identity <OU> -AuditedPrincipals <группа> -AuditType Success — SACL на атрибуты пароля
2. В GPO контроллеров включаем Advanced Audit Policy > DS Access > Audit Directory Service Access (Success и Failure)
3. Собираем Security EventID 4662 с DC и журнал LAPS/Operational в мониторинг, алерт в Telegram на чтение вне рабочих часов
4. Раз в квартал Find-LapsADExtendedRights показывает, у кого есть extended rights на OU и кто может читать конфиденциальные атрибуты
5. На DC при включённом шифровании дополнительно включаем ADBackupDSRMPassword — резерв пароля DSRM

РЕЗУЛЬТАТ

Любое обращение к паролю локального админа именное и заметное: видно, кто, когда и какую машину смотрел. Лишние права на чтение вычищаются по факту проверки, а не по памяти прошлого администратора.

КЛЮЧЕВОЙ НЮАНС

Без SACL и DS Access чтение пароля не оставляет следов: сам факт внедрения LAPS не даёт ни аудита, ни доказательной базы.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Шифрование при старых клиентах**
  ПК без обновлений от 11.04.2023 и новее не знают Windows LAPS: пароль в AD не попадает вообще.

- ✕ **Уровень домена ниже 2016**
  Шифрование через CNG DPAPI требует DFL 2016; иначе пароль хранится только открытым текстом под защитой ACL.

- ✕ **Забытый SELF на OU**
  Без Set-LapsADComputerSelfPermission компьютер не может записать свой пароль в собственный объект в AD.

- ✕ **Права на чтение у всех**
  Читатели пароля равны локальным админам на всём парке. Даём только именной группе, не Domain Users и не всему helpdesk.

- ✕ **Учётка не создана заранее**
  AdministratorAccountName указывает на несуществующий аккаунт — LAPS ничего не делает и пишет ошибку в журнал.

- ✕ **Старые ADMX в Central Store**
  LAPS.admx не копируется в Central Store автоматически: без ручного копирования раздел System > LAPS не виден в редакторе GPO.

- ✕ **Длина против локальной политики**
  PasswordLength или сложность несовместимы с локальной парольной политикой — пароль не создаётся, в журнале событие 10027.

- ✕ **Наследие legacy LAPS**
  MSI-продукт legacy LAPS объявлен устаревшим; при старой политике включается режим эмуляции — план миграции нужен явный.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Update-LapsADSchema и BackupDirectory = 2 (Active Directory) на OU рабочих станций
- PasswordLength не ниже 14, PasswordComplexity 4, PasswordAgeDays не больше 30
- SELF-право на запись; чтение пароля — только одной именной группе
- Проверка результата через Get-LapsADPassword и журнал LAPS/Operational

НОРМАЛЬНО

- ADPasswordEncryptionEnabled = True, ADPasswordEncryptionPrincipal = группа-читатель
- Отдельная управляемая учётка, встроенный Administrator отключён
- PostAuthenticationActions 3 и PostAuthenticationResetDelay 24 часа
- SACL через Set-LapsADAuditing плюс DS Access аудит и сбор EventID 4662

ХОРОШО

- ADEncryptedPasswordHistorySize до 12 и ADBackupDSRMPassword на контроллерах домена
- Алерты в мониторинг на нештатное чтение и на просроченные объекты
- Ежеквартальный Find-LapsADExtendedRights и сверка охвата парка
- LAPS в образе и в чек-листе ввода ПК в домен, вместе с BitLocker-ключами

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Уровень домена не ниже 2016, DC от Windows Server 2019 и клиенты с обновлениями 2023+
- [ ] Схема расширена через Update-LapsADSchema, атрибуты msLAPS-* присутствуют в лесу
- [ ] На OU компьютеров выданы SELF-запись, чтение и сброс пароля нужным группам
- [ ] GPO LAPS привязана к OU, BackupDirectory = 2, LAPS.admx скопирован в Central Store
- [ ] PasswordLength, PasswordComplexity и PasswordAgeDays заданы явно, а не по умолчанию
- [ ] AdministratorAccountName указывает на реально существующую локальную учётку
- [ ] ADPasswordEncryptionEnabled включён, ADPasswordEncryptionPrincipal не шире, чем нужно
- [ ] PostAuthenticationActions и PostAuthenticationResetDelay настроены и проверены на тесте
- [ ] Аудит: Set-LapsADAuditing плюс DS Access, события 4662 и LAPS/Operational в мониторинге
- [ ] Есть отчёт по охвату: сколько машин имеют актуальный msLAPS-PasswordExpirationTime

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).

- Проверяем готовность леса и парка, расширяем схему и настраиваем права на OU
- Собираем и раскатываем GPO LAPS с нашими длиной, сложностью и сроком ротации
- Переводим парк с общего пароля и legacy LAPS на управляемую учётку без простоя
- Подключаем аудит чтения паролей к мониторингу с алертами в Telegram
- Обучаем ваш helpdesk работе с Get-LapsADPassword и регламентом выдачи доступа

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 Windows LAPS overview: поддерживаемые ОС и дата выпуска (learn.microsoft.com — 2026)

02 Configure policy settings for Windows LAPS (learn.microsoft.com — 2026)

03 Windows LAPS architecture: цикл обработки политики (learn.microsoft.com — 2026)

04 Windows LAPS schema and rights extensions for AD (learn.microsoft.com — 2026)

05 Get started with Windows LAPS and Active Directory (learn.microsoft.com — 2026)

06 LAPS PowerShell module reference (Windows Server) (learn.microsoft.com — 2026)

07 Внутренний регламент ITfresh: LAPS и локальные админы (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.