Групповые политики/LAPS

В gpupdate, начиная с версии 0.13.0, предоставляется поддержка LAPS - механизма централизованного управления паролями локальных администраторов на компьютерах домена. Текущий пароль локального администратора хранятся в защищённых атрибутах объектов Computer в Active Directory, автоматически изменяется через заданные интервалы и может быть получен только пользователем или пользователями, состоящими в группах, которым администратор явно предоставил соответствующие права (параметр в политике «Настройка авторизованных дешифраторов паролей (Расшифрование паролей)» или пользователями, которые входят в группу «Администраторы домена», если параметр отключен или не настроен).

Настраивать политики можно как ключами реестра из Windows-ADMX, так и ключами реестра, прописанными в пакете admx-basealt. При этом, если заданы оба типа ключей, приоритет отдается ключам из admx-basealt.

В этой статье будет описано, как настроить групповые политики для управления паролями локальных администраторов на клиентской машине ALT Linux.

Предполагается, что инфраструктура уже развернута: в домене Active Directory (Windows Server 2016 или более новая версия) настроен LAPS (см. [статью Microsoft](https://learn.microsoft.com/ru-ru/windows-server/identity/laps/laps-scenarios-windows-server-active-directory)), клиентская машина на ALT Linux введена в домен AD (см. [Ввод машины в домен](https://www.altlinux.org/ActiveDirectory/Join)).

**Поддержка LAPS в инфраструктуре с ALT Linux и Windows:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Контроллер домена** | **Клиент** | **Инструменты** |
| Linux | **Samba AD** - в разработке | **ALT Linux:** \* p11 \* sisyphus \* p10 на данный момент (апрель 2025) проходит тестирование На клиенте должен быть установлен gpupdate, начиная с версии 0.13.0.  **Windows:** Встроенная поддержка Windows LAPS была добавлена в следующих накопительных обновлениях, выпущенных в апреле 2023 года: \* Windows 11 22H2 — KB5025239 \* Windows 11 21H2 — KB5025224 \* Windows 10 22H2 — KB5025221 | **ALT Linux:** \* ADMC, начиная с версии 0.20.0 \* admx-basealt, начиная с версии 0.4.0  **Windows:** \* Оснастка Active Directory Users and Computers (ADUC) \* Консоль Group Policy Management Console (GPMC.msc) |
| Windows | **MS AD** - Windows Server 2016 или более новая версия Встроенная поддержка Windows LAPS была добавлена в следующих кумулятивных обновлениях, выпущенных в апреле 2023 года: \* Windows Server 2022 – KB5025230 \* Windows Server 2019 – KB5025229 |

После выполнения всех необходимых настроек на контроллере домена в Active Directory в схемы будут добавлены следующие атрибуты:

* msLAPS-PasswordExpirationTime
* msLAPS-Password
* msLAPS-EncryptedPassword
* msLAPS-EncryptedPasswordHistory
* msLAPS-EncryptedDSRMPassword
* msLAPS-EncryptedDSRMPasswordHistory

Проверить это можно в свойствах компьютера во вкладке **Атрибуты**.

Описание политик

В скобках указаны названия аналогичных политик в ALT Linux.

1. **Имя учетной записи администратора для управления (Имя учетной записи администратора)**

Этот параметр политики задает пользовательское имя учетной записи администратора, для которого нужно управлять паролем.

Если этот параметр политики включен, LAPS будет управлять паролем для локальной учетной записи с этим именем.

Если этот параметр политики отключен или не настроен, LAPS будет управлять паролем для известной учетной записи администратора.

НЕ включайте этот параметр политики для управления встроенной учетной записью администратора. Встроенная учетная запись администратора определяется автоматически по известному SID и не зависит от имени учетной записи.

1. **Включить шифрование паролей (Шифрование паролей)**

Когда вы включаете этот параметр, управляемый пароль шифруется перед отправкой в Active Directory.

Включение этого параметра не действует, если:

* + пароль не настроен для резервного копирования в Active Directory
  + функциональный уровень домена Active Directory не ниже Windows Server 2016 или выше.

Если этот параметр включен, а функциональный уровень домена не ниже Windows Server 2016, пароль управляемой учетной записи шифруется.

Если этот параметр включен, а функциональный уровень домена меньше, чем Windows Server 2016, пароль управляемой учетной записи не копируется в каталог.

Если этот параметр отключен, пароль управляемой учетной записи не шифруется.

Этот параметр будет включен по умолчанию, если он не настроен.

1. **Действия после проверки подлинности (Действия после проверки подлинности)**

Эта политика настраивает действия после проверки подлинности, которые будут выполняться после обнаружения проверки подлинности управляемой учетной записью.

Льготный период: указывает количество времени (в часах) ожидания после аутентификации перед выполнением указанных действий после аутентификации.

* + Если этот параметр включен и больше нуля, указанные действия после аутентификации будут выполняться по истечении льготного периода;
  + Если этот параметр равен нулю, никакие действия после аутентификации выполняться не будут;
  + Если этот параметр отключен или не настроен, указанные действия после аутентификации будут выполняться по истечении установленного по умолчанию 24-часового льготного периода.

Действия: указывает действия, которые необходимо предпринять по истечении льготного периода:

* + Сброс пароля: по истечении льготного периода пароль управляемой учетной записи будет сброшен;
  + Сбросьте пароль и выйдите из управляемой учетной записи: по истечении льготного периода пароль управляемой учетной записи будет сброшен, а все интерактивные сеансы входа с использованием управляемой учетной записи будут прекращены;

**Примечание:** После завершения любого интерактивного сеанса входа управляемая учетная запись может по-прежнему использовать другие сеансы с проверкой подлинности. Единственный надежный способ убедиться, что предыдущий пароль используется дольше, — это перезагрузить устройство.

* + Сброс пароля и перезагрузка: по истечении льготного периода пароль управляемой учетной записи будет сброшен, а управляемое устройство будет немедленно перезагружено.

**Примечания:** Если этот параметр отключен или не настроен, действия после проверки подлинности по умолчанию будут «Сбросить пароль и выйти из управляемой учетной записи».

1. **Не разрешайте сроку действия пароля превышать время, требуемое политикой (Истечение срока действия пароля)**

Если этот параметр включен или не настроен, запланированное истечение срока действия пароля дольше срока действия пароля, определяемого политикой «Параметры пароля», НЕ допускается. При обнаружении такого истечения срока действия пароль немедленно изменяется, а срок действия пароля устанавливается в соответствии с политикой.

Если этот параметр отключен, срок действия пароля может быть больше, чем требуется политикой «Настройки пароля».

1. **Настройка каталога резервного копирования паролей (Каталог резервного копирования паролей)**

Используйте этот параметр, чтобы указать, в какой каталог резервируется пароль локальной учетной записи администратора. Допустимые параметры:

* + Отключено = отключено (пароль не будет резервироваться)
  + Azure Active Directory = Резервное копирование пароля в Azure Active Directory
  + Active Directory = Резервное копирование пароля в Active Directory

Если не указано иное, значение этого параметра по умолчанию равно 0 (отключено).

Если для этого параметра установлено значение Azure Active Directory, а управляемое устройство не присоединено к Azure Active Directory, пароль локального администратора не будет управляться.

Если для этого параметра установлено значение Active Directory, а управляемое устройство не присоединено к Active Directory, пароль локального администратора не будет управляться.

Если этот параметр отключен или не настроен, пароль локального администратора не управляется.

1. **Параметры паролей (Параметры паролей)**

Политика позволяет настроить сложность, длину и срок действия паролей.

* + Параметр «Сложность пароля» — допустимые к использованию символы при создании нового пароля. По умолчанию: «Заглавные буквы, строчные буквы, цифры, специальные символы».
  + Длина пароля — количество символов в пароле. Минимум: 8 символов; Максимум: 64 символа; По умолчанию: 14 символов.
  + Срок действия пароля в днях. Минимум: 1 день (7 дней, если каталог резервного копирования настроен как Azure AD); Максимум: 365 дней; По умолчанию: 30 дней.

1. **Настройка авторизованных дешифраторов паролей (Расшифрование паролей)**

Настройте этот параметр для управления конкретным пользователем или группой, пользователям которой разрешено расшифровывать зашифрованные пароли.

Настройка этого параметра не действует, если не включено шифрование пароля.

Если этот параметр включен, зашифрованные пароли могут быть расшифрованы указанной группой.

Если этот параметр отключен или не настроен, зашифрованные пароли могут быть расшифрованы пользователями группы «Администраторы домена».

Для этого параметра необходимо указать либо SID в строковом формате ("S-1-5-21-2127521184-1604012920-1887927527-35197"), либо имя группы или пользователя в домене\( группа или пользователь). Указанный пользователь или группа должны разрешаться управляемым устройством, в противном случае резервное копирование паролей выполняться не будет.

1. **Настройка размера журнала зашифрованных паролей (Размер журнала зашифрованных паролей)**

Используйте этот параметр, чтобы указать, сколько предыдущих зашифрованных паролей будет храниться в Active Directory. Настройка этого параметра не действует, если:

* + пароль не настроен для резервного копирования в Active Directory;
  + не включено шифрование пароля.

Допустимый диапазон значений количества хранимых паролей — 0 - 12;

Если политика включена, указанное количество старых паролей будет храниться в Active Directory.

Если политика отключена или не настроена, в Active Directory не будет храниться ни одного старого пароля.

Применение

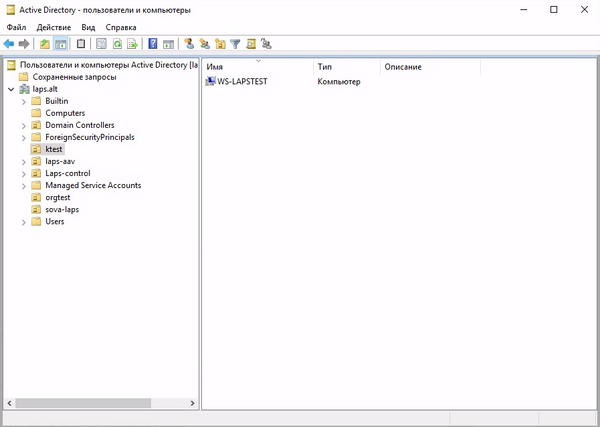
1. **Установка gpupdate на клиентах**

Для применения групповых политик на клиентах необходимо установить **gpupdate**, если он не установлен:

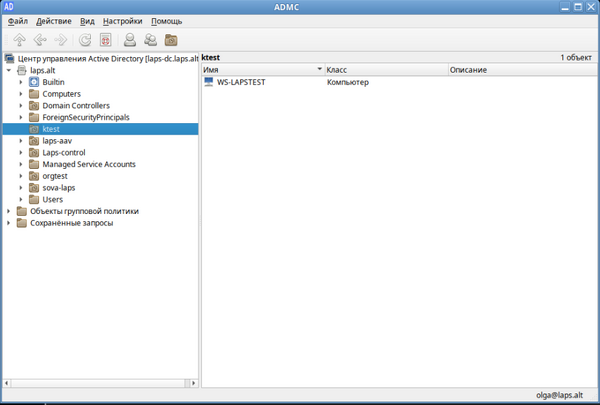
**# apt-get install gpupdate**

**# gpupdate-setup enable**

1. **Создать подразделение (OU,Organizational Units) и добавить в нее компьютеры, к которым необходимо применить политику:**

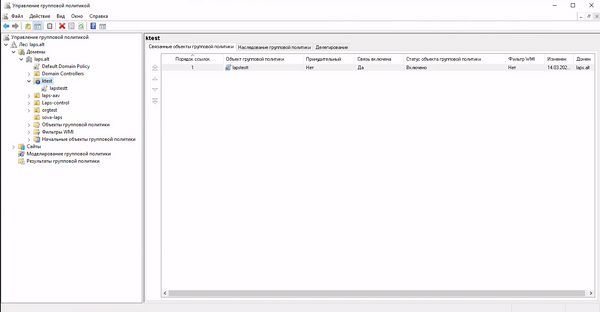


или

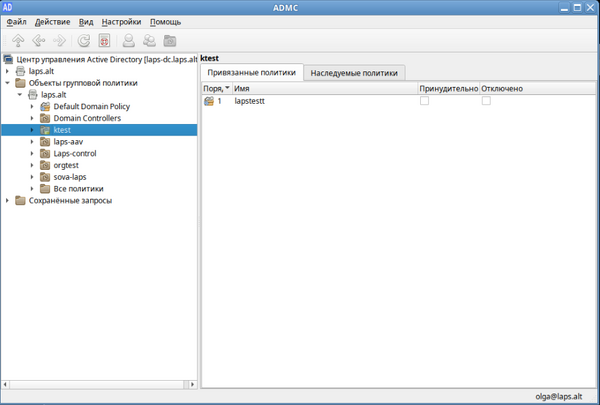


Как создать подразделение см. [ADMC](https://www.altlinux.org/%D0%93%D1%80%D1%83%D0%BF%D0%BF%D0%BE%D0%B2%D1%8B%D0%B5_%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B8/ADMC#%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE%D0%B4%D1%80%D0%B0%D0%B7%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F%D0%BC%D0%B8).

1. **Создать групповую политику и связать с подразделением:**

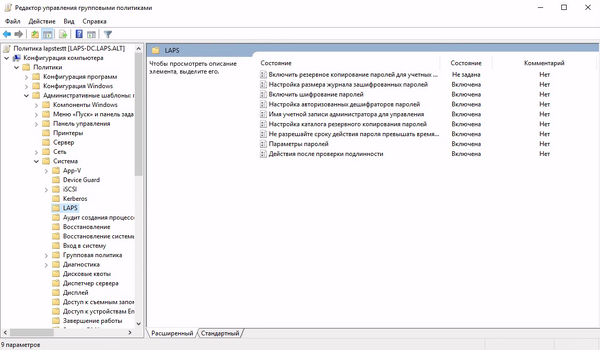


или

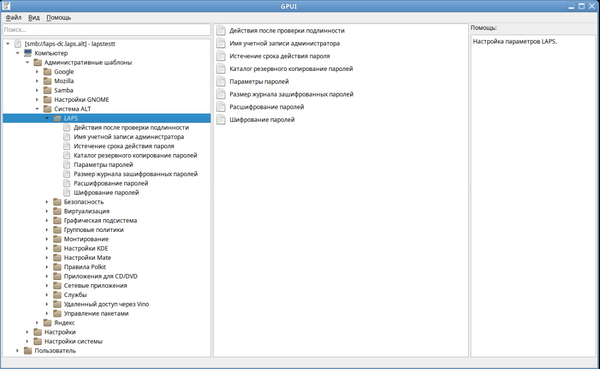


Как создать групповую политику и связать с подразделением см. [ADMC](https://www.altlinux.org/%D0%93%D1%80%D1%83%D0%BF%D0%BF%D0%BE%D0%B2%D1%8B%D0%B5_%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B8/ADMC#%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BE%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D0%B0%D0%BC%D0%B8_%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D0%BE%D0%B2%D1%8B%D1%85_%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA).

1. **Настроить групповые политики ключами реестра из Windows-ADMX или ключами реестра из admx-basealt:**



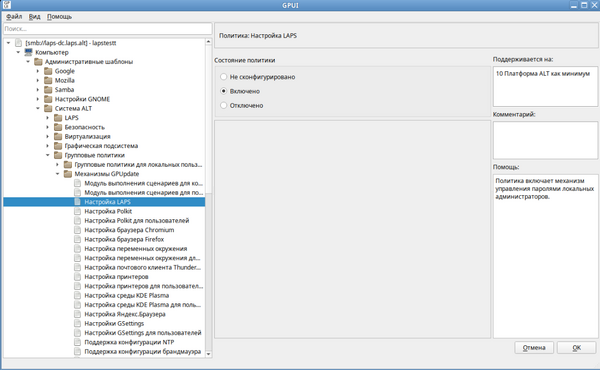
или



Как редактировать групповые политики см. [GPUI](https://www.altlinux.org/%D0%93%D1%80%D1%83%D0%BF%D0%BF%D0%BE%D0%B2%D1%8B%D0%B5_%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B8/GPUI).

Необходимо **обязательно установить параметр «Active Directory»** в политике «Настройка каталога резервного копирования паролей (Каталог резервного копирования паролей)» и **установить состояние «Включено»** в политике Включить шифрование паролей (Шифрование паролей).

В ADMC обязательно нужно включить **механизм GPUpdate «Настройка LAPS»**



1. **Применить групповые политики с помощью gpupdate**:
2. **$ gpupdate**
3. Apply group policies for computer.
4. Apply group policies for user.

Проверка применения групповых политик

Проверим, что LAPS будет управлять паролем для локальной учетной записи **root**.

Для этого в политике «Имя учетной записи администратора для управления (Имя учетной записи администратора)» необходимо указать в параметре root.

После применения политики должны заполниться атрибуты машины, к которой они были применены:

|  |  |
| --- | --- |
|  |  |

Данный пароль можно скопировать и использовать для аутентификации на клиентской машине с учетной записью root. После истечения срока действия, заданного групповой политикой, будет автоматически сгенерирован новый пароль и выполнено действие в зависимости от политики «Действия после проверки подлинности (Действия после проверки подлинности)».