

Инструкция по обеспечению безопасной работы в домене ALD Pro: политики паролей

ALD Pro

Exported on 08/11/2023

Table of Contents

1	Пароли пользователей в домене	4
2	Что такое политики паролей.....	5
3	Механизм работы политик паролей	6
4	Создание политики паролей.....	9
4.1	Через портал управления	9
4.2	Из командной строки	10

Авторы: Федоров Руслан, Анатолий Лысов

v.1.1

Пароли являются самым простым, но при этом не самым безопасным способом аутентификации, поэтому в работе с паролями пользователи должны придерживаться определенных правил и политики паролей помогают гарантировать, что эти правила соблюдаются.

1 Пароли пользователей в домене

Пароль представляет из себя набор символов, который известен только самому пользователю и проверяющей стороне, поэтому, если пользователь может предъявить доказательство того, что пароль ему известен, это является подтверждением аутентичности пользователя, что он именно тот, за кого себя выдает.

В открытом виде пароли не хранят, в базу данных записывают хэши, и так как в домене ALD Pro (FreeIPA) используется сразу несколько разных механизмов аутентификации, у пользователей есть несколько хэшей:

- userPassword хранит PBKDF2_SHA256 хэш, который используется для обычной LDAP аутентификации, так называемой привязки (Bind). Во избежание перехвата пароля этот способ аутентификации рекомендуют использовать только с шифрованием трафика (LDAPS или LDAP+StartTLS).
- krbPrincipalKey хранит AES хэши, которые используются для аутентификации по протоколу Kerberos V5. Это наиболее рекомендуемый способ аутентификации с использованием паролей, т.к. он обеспечивает наибольший уровень безопасности.
- ipaNTHash хранит MD4 хэш, который используется для NTLM аутентификации. Этот механизм аутентификации необходим для интеграции с MS AD, простой аутентификации на файловом сервере при обращении к нему по IP адресу и интеграции с некоторыми другими внешними системами.

Для изменения пароля новое значение следует записать открытым текстом в атрибут userPassword, сервер автоматически сгенерирует все необходимые ключи и запишет в базу уже хешированные значения. В силу такой особенности работы сервера записывать в каталог уже хешированные значения запрещено. Обойти это ограничение можно только при создании новых пользователей, если сервер будет переведен в режим миграции.

2 Что такое политики паролей

Пароли, к сожалению, являются не самым безопасным механизмом аутентификации, так как их можно подобрать или перехватить, поэтому в работе с паролями необходимо следовать определенным правилам, или так называемым политикам, которые повышают уровень безопасности учетных записей в домене: пароли нужно периодически обновлять, использовать следует достаточно длинные комбинации, состоящие из разных категорий символов, и т.п.

Чем более строгие требования задает политика паролей, тем сложнее злоумышленнику подобрать пароль и воспользоваться результатами успешной атаки. Но, вместе с тем, и пользователям сложнее работать в таком домене, поэтому для разных групп пользователей следует устанавливать разные требования, обеспечивающий компромисс между удобством и безопасностью.

3 Механизм работы политик паролей

Механизм политик паролей в домене ALD Pro (FreeIPA) очень гибкий: для каждой группы пользователей можно создать свою собственную политику паролей. Список политик с их приоритетами хранится в контейнере с DN «cn=**cosTemplates**,cn=accounts,dc=ald,dc=company,dc=local», параметры политик вынесены отдельно в «cn=**kerberos**,dc=ald,dc=company,dc=local». Связь между записями осуществляется через значение атрибута krbPwdPolicyReference. При удалении группы пользователей все связанные с ней записи политики паролей удаляются автоматически.

Учитывая, что пользователь может входить сразу в несколько групп, алгоритм проверки выглядит следующим образом:

- Из «cn=cosTemplates, ...» отбираются политики, под действие которых попадает текущий пользователь в соответствии с его участием в группах. Параметры политики берутся из «cn=kerberos, ...» по ссылке из атрибута krbPwdPolicyReference.
- Если на пользователя не распространяется действие ни одной политики, ему будет назначена глобальная политика по умолчанию (global_policy).
- Если некоторый пользователь попадает под действие сразу нескольких политик, то выбирается одна из них, у которой будет наименьшее значение по приоритету, параметры политик не суммируются, см. таблицу 1.

Таблица 1. Выбор политики в зависимости от приоритета

Параметр	Политика для группы А (приоритет 0)	Политика для группы В (приоритет 1)	Результат (используются параметры для группы А)
Максимальный срок действия	60 дней	90 дней	60 дней
Минимальная длина	10 символов	0 (без ограничений)	10 символов

Проверки паролей ограничены возможностями MIT Kerberos, поэтому они поддерживают тот же самый набор параметров, см. таблицу 2

Таблица 2. Параметры политик паролей

Параметр политики	Значение глобальной политики по умолчанию
Максимальный срок действия задает период в количестве дней, в течение которого система не будет требовать смены пароля	krbMaxPwdLife = 90 Пароль активен 90 дней, после чего пользователю будет предложено сменить его
Минимальный срок действия задает период в часах, в течение которого система будет запрещать повторную смену пароля	krbMinPwdLife = 1 После смены пароля, пользователь должен подождать 1 час перед повторной сменой

Параметр политики	Значение глобальной политики по умолчанию
<p>Размер журнала определяет количество предыдущих паролей, которые нельзя использовать повторно</p>	<p>krbPwHistoryLength = 0</p> <p>Запрет на повторное использование паролей не налагается</p>
<p>Классы символов – этот параметр указывает, сколько разных классов символов должно быть использовано в пароле.</p> <p>Все возможные символы подразделяются на следующие пять классов:</p> <ul style="list-style-type: none"> • цифры • буквы нижнего регистра • буквы верхнего регистра • символы UTF-8 • Все остальные символы, не вошедшие ни в одну из предыдущих групп, например, (! " # \$ % и т.д. <p>Использование одного и того же символа более двух раз подряд уменьшает количество классов на один, например, у пароля «Secret11pwd» будет три класса (большие буквы + маленькие буквы + цифры), а у пароля «Secret111pwd» их станет два (минус штраф за повторы символа «1»).</p> <p>Если повторяющиеся символы окажутся в конце пароля, то последний из них не будет учитываться, поэтому на пароль «Secretpwd111» штраф налагаться не будет.</p>	<p>krbPwMinDiffChars = 0</p> <p>Значение по умолчанию – 0.</p> <p>Это говорит об отсутствии каких либо требований к сложности пароля</p>
<p>Минимальная длина задает минимально допустимое количество символов в пароле</p>	<p>krbPwMinLength = 8</p> <p>Пользователь не может использовать пароль короче 8 символов</p>
<p>Максимальное количество ошибок определяет, сколько раз пользователь может неправильно ввести пароль, прежде чем его аккаунт будет временно заблокирован.</p> <p>Блокировка выполняется только на текущем контроллере, на другие сервера эта информация не передается.</p>	<p>krbPwMaxFailure = 6</p> <p>Пользователь будет заблокирован после 7 неверно введенных паролей подряд</p>

Параметр политики	Значение глобальной политики по умолчанию
Интервал сброса ошибок задает период в секундах, по истечении которого счетчик неудачных попыток входа будет сброшен	krbPwdFailureCountInterval = 60 Если после 6 неудачных попыток введения пароля подряд пользователь подождет 1 минуту, у него будет еще 6 попыток до временной блокировки учетной записи
Длительность блокировки задает период в секундах, в течение которого пользователь не сможет выполнить аутентификацию в домене. Блокировка накладывается после превышения количества разрешенных неудачных попыток входа. Блокировка выполняется только на текущем контроллере, на другие сервера эта информация не передается.	krbPwdLockoutDuration = 600 Заблокированный пользователь не сможет выполнить вход в систему в течение 10 минут

Следствием интеграции с MIT Kerberos является возможность использования таких атрибутов, как krbPasswordExpiration, krbPrincipalExpiration и krbLastSuccessfulAuth. Например, при изменении пароля через панель управления для него автоматически устанавливается срок истечения действия пароля krbPasswordExpiration, поэтому пользователь не может использовать этот пароль до тех пор, пока не установит новый. Если вы хотите снять это ограничение, воспользуйтесь командой ipa user-mod

```
ipa user-mod alexander.kuznetsov --password-expiration 20250101115110Z
```

Эта же команда позволит вам установить срок действия учетной записи, после которого пользователю станет недоступна Kerberos аутентификация:

```
ipa user-mod alexander.kuznetsov --principal-expiration='20230717040953Z'
```

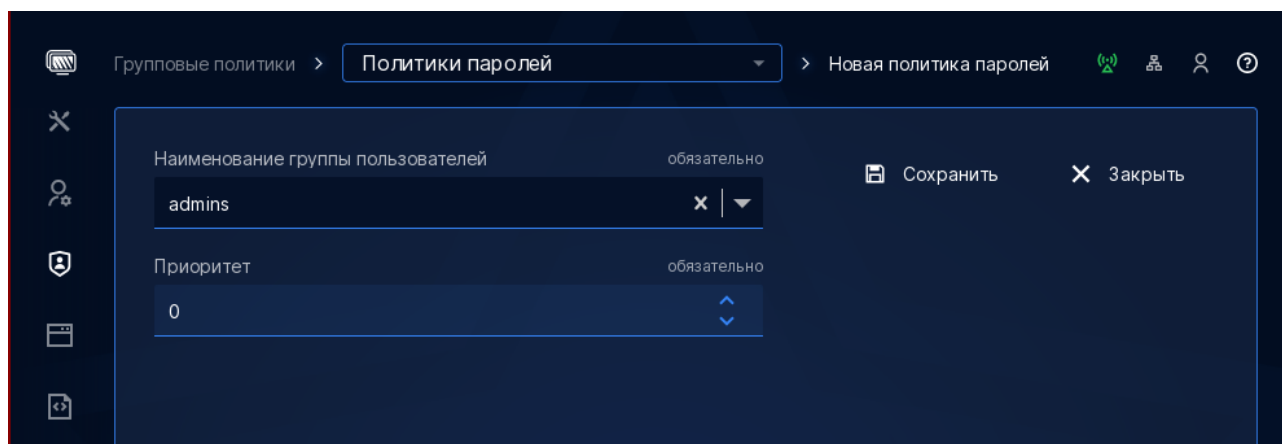
Логирование даты последнего входа можно включить изменением конфигурации сервера, для этого потребуется посмотреть текущие настройки и установить новое значение параметра ipaconfigstring, исключив из него значение «KDC:Disable Last Success»

```
ipa config-show | grep паролей
Возможности подключаемого модуля паролей: AllowNThash, KDC:Disable Last Success
ipa config-mod --ipaconfigstring='AllowNThash'
ipactl restart
kinit admin
ipa user-show admin --all --raw | grep krbLastSuccessful
krbLastSuccessfulAuth: 20230608094515Z
```


4 Создание политики паролей

4.1 Через портал управления

Откройте страницу «Групповые политики > Политики паролей» и нажмите кнопку «+ Новая политика паролей». Заполните поля «Наименование группы пользователей», «Приоритет» и нажмите кнопку «Сохранить».



The screenshot shows a web interface for creating a new password policy. The breadcrumb navigation at the top reads 'Групповые политики > Политики паролей'. The main heading is 'Новая политика паролей'. The form contains two required fields: 'Наименование группы пользователей' (User group name) with the value 'admins' and 'Приоритет' (Priority) with the value '0'. Both fields are marked as 'обязательно' (required). To the right of the form are two buttons: 'Сохранить' (Save) and 'Закрыть' (Close). A vertical sidebar on the left contains several icons for navigation.

Рис. 1. Создание политика паролей.

Далее вам станет доступна страница управления политикой, где вы можете задать необходимые настройки.

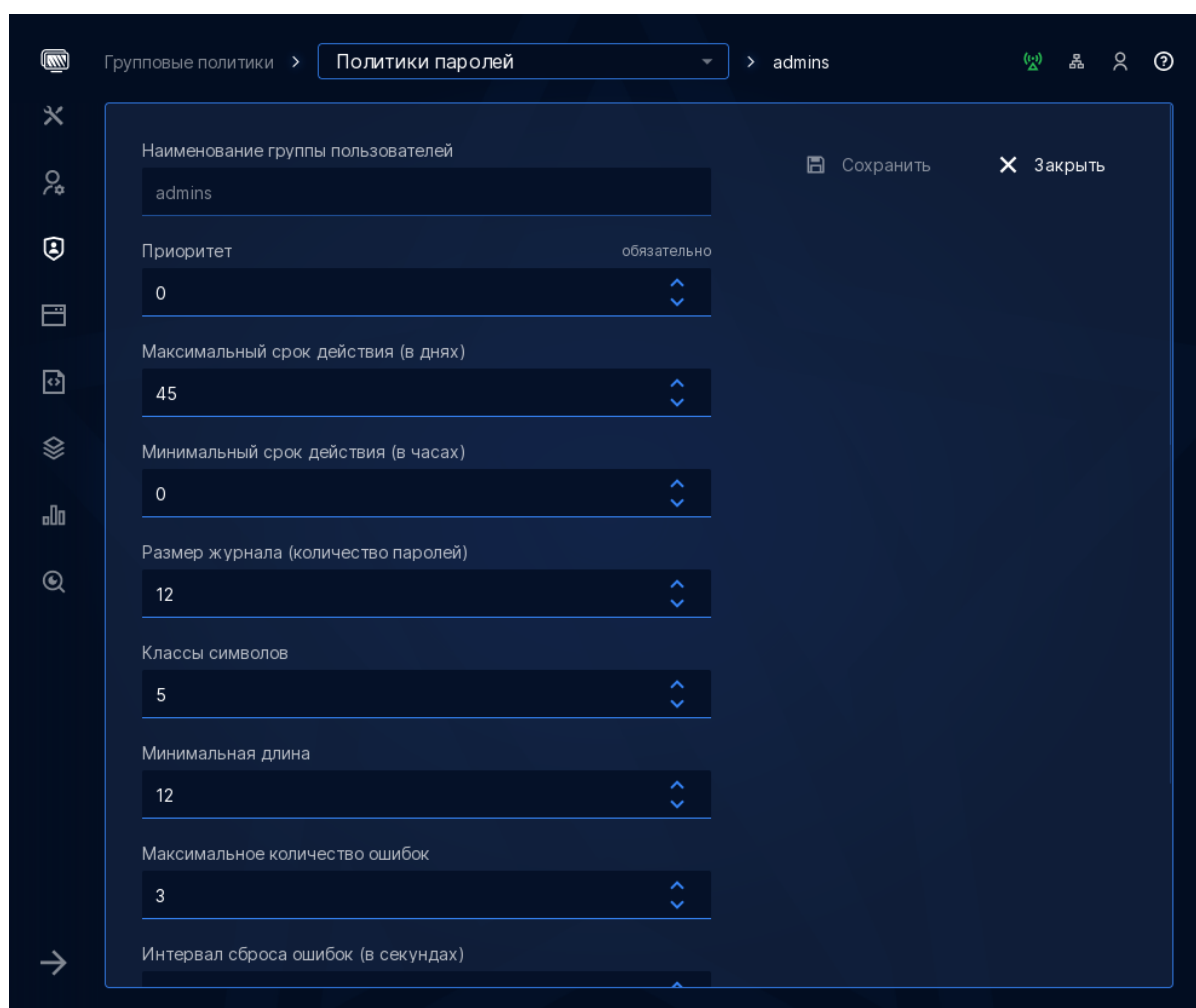


Рис. 2. Настройка политики паролей

4.2 Из командной строки

Для создания политики паролей воспользуйтесь командой `rwpolicy-add`

```
$ ipa pwpolicy-add admins --priority=0 --maxlife=45 --minlife=0 --history=12 \
--minclasses=5 --minlength=12 --maxfail=3 --failinterval=120 --lockouttime=1200
Группа: admins
Максимальный срок действия (в днях): 45
Минимальный срок действия (в часах): 0
Размер журнала : 12
Классы символов: 5
Минимальная длина: 12
Приоритет: 0
Максимальное количество ошибок: 3
Интервал сброса ошибок: 120
Длительность блокировки: 1200
```

где,

- --maxlife=<число> - Максимальный срок действия в днях;
- --minlife=<число> - Минимальный срок действия в часах;
- --history=<число> - Размер журнала;
- --minclasses=<число> - Классы символов;
- --minlength=<число> - Минимальная длина;
- --priority=<число> - Приоритет политики;
- --maxfail=<число> - Максимальное количество ошибок;
- --failinterval=<число> - Интервал сброса ошибок в секундах;
- --lockouttime=<число> - Длительность блокировки в секундах.

Чтобы изменить параметры уже существующей политики, воспользуйтесь командой `ipa pwpolicy-mod`:

```
$ ipa pwpolicy-mod admins --maxlife=30
Группа: admins
Максимальный срок действия (в днях): 30
Минимальный срок действия (в часах): 0
Размер журнала : 12
Классы символов: 5
Минимальная длина: 12
Приоритет: 0
Максимальное количество ошибок: 3
Интервал сброса ошибок: 120
Длительность блокировки: 1200
```

Следует учитывать, что срок действия пароля проверяется не по значению `maxlife` в политике, а по значению атрибута `krbPasswordExpiration`, которое устанавливается пользователю при изменении пароля, поэтому изменение параметра в политике сразу ни на что не повлияет. Чтобы принудительно изменить пользователю значение атрибута `krbPasswordExpiration` вы можете воспользоваться командой `user-mod`:

```
$ ipa user-mod admin --password-expiration 20230528010101Z
-----
Изменён пользователь "admin"
-----
Имя учётной записи пользователя: admin
Фамилия: Administrator
Домашний каталог: /home/admin
Оболочка входа: /bin/bash
Псевдоним учётной записи: admin@ALD.COMPANY.LOCAL, root@ALD.COMPANY.LOCAL
Окончание действия пароля пользователя: 20230528010101Z
UID: 959800000
ID группы: 959800000
Учётная запись отключена: False
Link to department:
ou=ald.company.local,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=local
Пароль: True
Участник групп: trust admins, lpadmin, admins
Роли: ALDPRO - Main Administrator
Доступные ключи Kerberos: True
```

Срок действия пароля задается в формате временной метки, где:

- 2023 – год
- 05 – месяц
- 28 – день месяца;
- 010101 – часы, минуты, секунды
- Z – часовой пояс. Точность до секунд не имеет большого значения, поэтому обычно используют время по нулевому (Zero) меридиану.

Проверить текущее значение можно командой user-show

```
$ ipa user-show admin --raw --all | grep krbPasswordExpiration
krbPasswordExpiration: 20230528010101Z
```