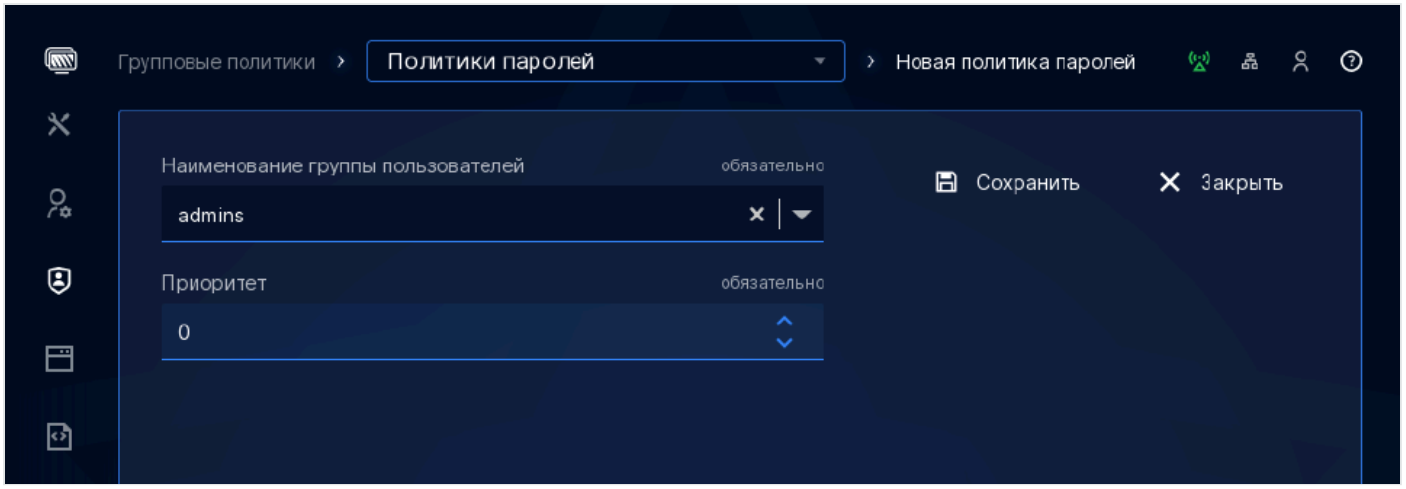
Astra
Infrastructure
Cloud

Создание политики паролей

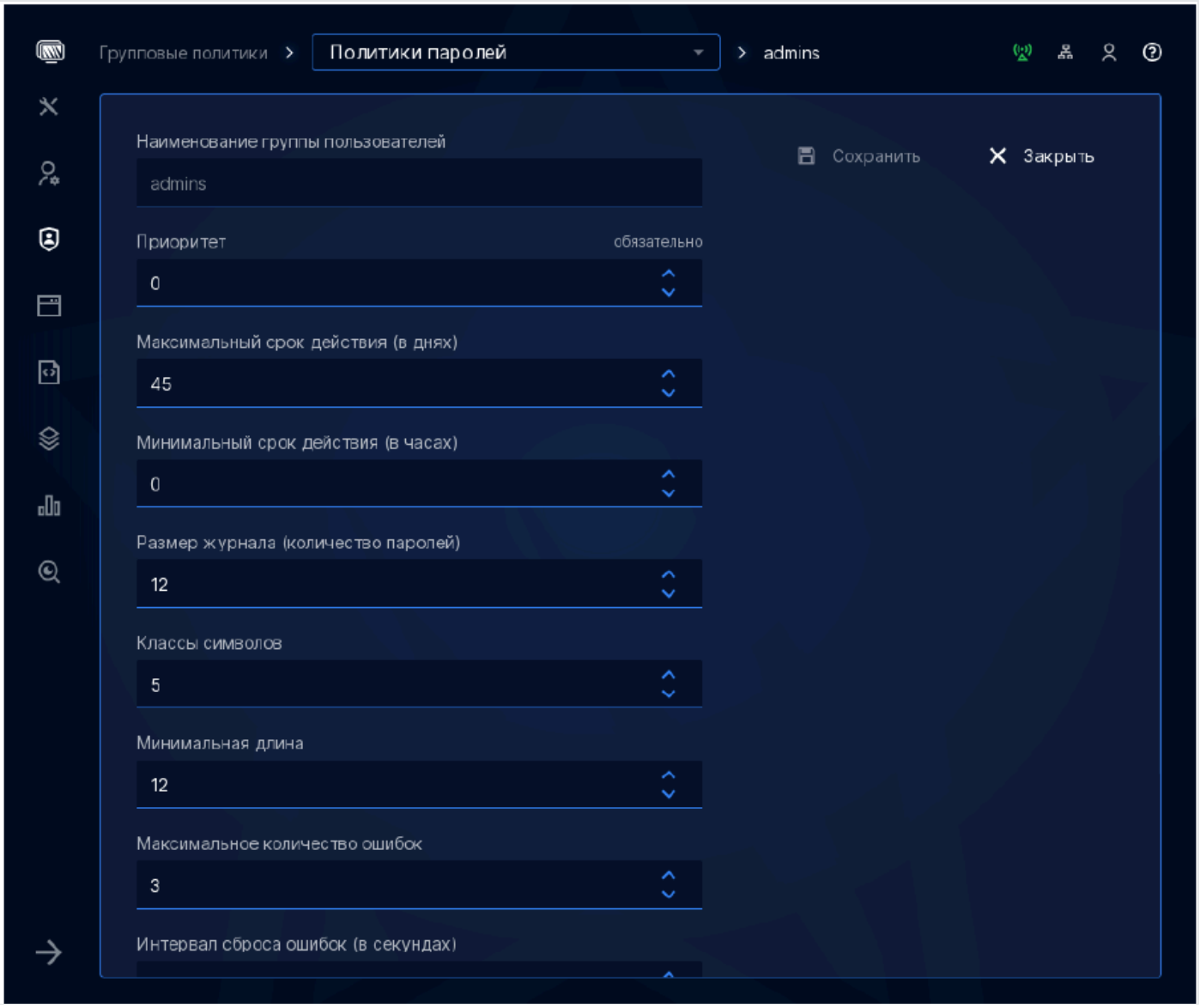
Через портал управления

Открыть страницу **Групповые политики — Политики паролей** и нажать кнопку **+ Новая политика паролей**.

Заполнить поля **Наименование группы пользователей**, **Приоритет** и нажать кнопку **Сохранить**.



Далее станет доступна страница управления политикой, где можно задать необходимые настройки.



Из командной строки

Для создания политики паролей воспользуйтесь командой `pwpolicy-add`:

```
$ ipa pwpolicy-add admins --priority=0 --maxlife=45 --minlife=0 --history=12 --mincla
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` можно воспользоваться командой `user-mod`:

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

рок 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
```