Интеграция Astra Monitoring со службой каталога ALD Pro

07/10/2025

Содержание

Astra Monitoring — отечественная система мониторинга ИТ-инфраструктуры, предназначенная для контроля состояния серверов, рабочих станций, сетевых устройств и сервисов. Решение разработано с учетом требований информационной безопасности и используется в организациях, работающих с конфиденциальной или государственной информацией. Система предоставляет веб-интерфейс для отображения метрик, поддерживает уведомления и гибкую настройку мониторинга.

Интеграция Astra Monitoring с ALD Pro позволяет осуществлять централизованную аутентификацию пользователей с использованием учетных записей, хранящихся в ALD Pro. Это упрощает управление доступом и обеспечивает единое хранилище учетных данных. Авторизация и разграничение прав внутри Astra Monitoring при этом продолжают настраиваться локально.

1 Добавление сервисной учётной записи в ALD Pro

Аутентификация и авторизация выполняются методом LDAP Bind, для чего необходимо создать в ALD Pro сервисную учётную запись, которая не является POSIX-пользователем, не имеет прав на вход в домен и не отображается в портале управления, а используется только для чтения LDAP.

Создание записи выполняется следующей командой:

```
kinit admin && ipa-ldap-updater bind-user.ldif
```

,где `**bind-user.ldif**` — файл с описанием записи в формате LDIF:

```
dn: uid=monitoring-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
add: objectClass: account
add: objectClass: simpleSecurityObject
add: uid: monitoring-bind
add: userPassword: securePassword123
add: passwordExpirationTime: 20380119031407Z
add: nsIdleTimeout: 0
```

Замените `**dc=ald,dc=company,dc=lan**` на актуальные значения вашей доменной структуры, а `**securePassword123**` — на надёжный пароль.

2 Настройка подключения к ALD Pro через Keycloak

2.1 Через файл values.yaml при установке Astra Monitoring

При использовании Helm-чарта для установки Astra Monitoring можно сразу задать параметры подключения к ALD Pro. Для этого в файле **values.yaml** необходимо раскомментировать и заполнить блок **keycloak.ldap**. Обязательно указывается параметр **keycloak.ldap.bindCredential**, содержащий пароль от сервисной учётной записи.

Пример конфигурации:

```
keycloak:
    ldap:
        connectionUrl: ldaps://dc-1.ald.company.lan:636
        bindDn: "uid=monitoring-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan"
        usersDn: "cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
        usernameLDAPAttribute: "uid"
        bindCredential: "securePassword123"
```

После настройки выполните установку или обновление Helm-релиза:

```
helm upgrade --install astra-monitoring ./chart-path -f values.yaml
```

Если вы выполняете подключение к ALD Pro после установки Astra Monitoring, необходимо вручную удалить ресурсы Keycloak, чтобы применились новые параметры подключения:

При установке через Kubernetes Helm:

- удалите `Deployment` и `PVC`, связанные с Keycloak;

При установке через Docker Compose:

- удалите каталог `keycloak/data/pgdata`, содержащий состояние Keycloak.

2.2 Дополнительные материалы

Подробная инструкция по настройке интеграции Keycloak с ALD Продоступна по ссылке:

Интеграция Keycloak со службой каталога ALD Pro

3 Рекомендации по безопасности

- Используйте только LDAPS (порт 636) для защиты соединения.

- Убедитесь, что система, на которой работает Keycloak, доверяет SSL-сертификату LDAP-сервера.

- При необходимости установите корневой сертификат удостоверяющего центра в хранилище доверенных CA