Корпоративная платформа хранения
и обработки больших данных

Новая безопасность в ClickHouse

Коняев Андрей

Есть Проблема №1

1. Сложно управлять пользователями:
   - Управление только через файл users.xml
   - Для этого нужен администратор
   - Это может быть долго

2. Нет возможности дать для пользователя доступ на чтение к одной базе и полный доступ к другой.

3. Нет возможности дать доступ до конкретной таблицы.

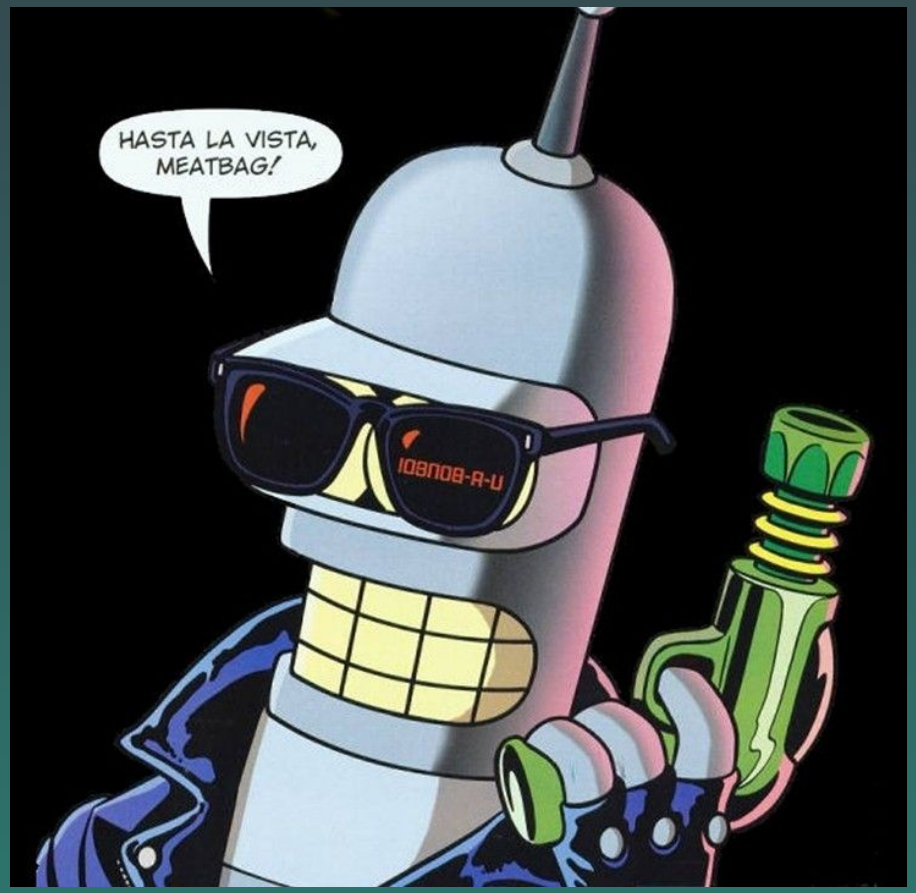
Good News Everyone №1!

1. Появился RBAC
2. Появилась интеграция с LDAP

RBAC

Объекты системы доступа:

- Пользователь
- Роль
- Доступ к строкам
- Профиль настроек
- Квоты



Хранение пользователей

В ClickHouse теперь пользователей можно хранить не только в users.xml.

Варианты:

- local directory (тот самый RBAC)
- users.xml
- ldap (с версии 20.11)

Хранение пользователей

```
SELECT
    name,
    storage,
    auth_type,
    auth_params
FROM system.users

Query id: 7b777ef0-0849-4f80-a6eb-ad27f782bb38

┌─name─────┬─storage─────────┬─auth_type──────────┬─auth_params─────────────────────────────┐
│ fry      │ local directory │ ldap_server        │ {"server":"my_ldap_server"}            │
│ bender   │ local directory │ plaintext_password │ {}                                     │
│ default  │ users.xml       │ plaintext_password │ {}                                     │
│ bender   │ users.xml       │ plaintext_password │ {}                                     │
│ professor│ ldap            │ ldap_server        │ {"server":"my_ldap_server"}            │
└──────────┴─────────────────┴────────────────────┴────────────────────────────────────────┘

5 rows in set. Elapsed: 0.001 sec.
```

Local Directory

- Для того чтобы активизировать добавляем в config.xml:

  <access_control_path>/var/lib/clickhouse/access</access_control_path>

- Внутри копится вся информация о пользователях, ролях, квотах и настройках. А также все гранты здесь

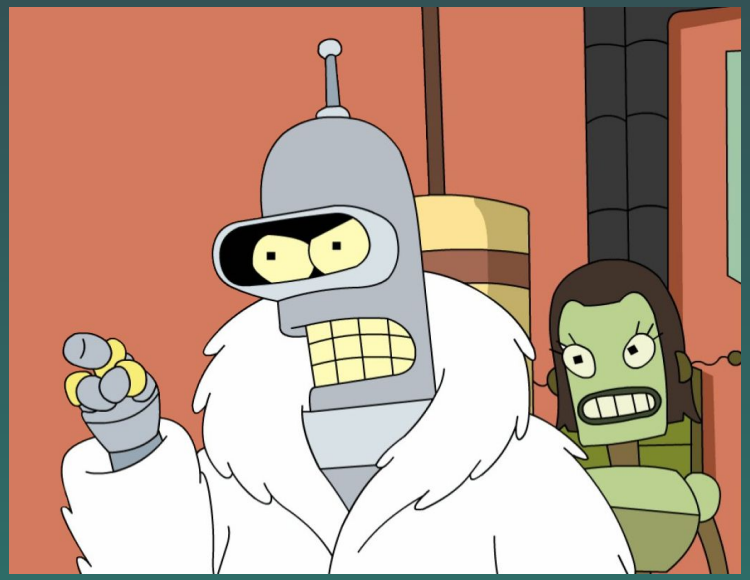
```
root@akonyaev-laptop:/var/lib/clickhouse/access# ls -la ./*
-rw-r----- 1 clickhouse clickhouse 102 ноя  9 21:49 ./634072a7-c09c-dcd7-1be6-a59dd8fbf0b5.sql
-rw-r----- 1 clickhouse clickhouse  65 ноя  9 20:51 ./6f4a8831-c316-94bd-2d49-73b55f87af94.sql
-rw-r----- 1 clickhouse clickhouse   1 ноя  9 20:50 ./quotas.list
-rw-r----- 1 clickhouse clickhouse   1 ноя  9 20:50 ./roles.list
-rw-r----- 1 clickhouse clickhouse   1 ноя  9 20:50 ./row_policies.list
-rw-r----- 1 clickhouse clickhouse   1 ноя  9 20:50 ./settings_profiles.list
-rw-r----- 1 clickhouse clickhouse  84 ноя  9 20:52 ./users.list
root@akonyaev-laptop:/var/lib/clickhouse/access# cat 634072a7-c09c-dcd7-1be6-a59dd8fbf0b5.sql
ATTACH USER bender IDENTIFIED WITH plaintext_password BY 'ben';
ATTACH GRANT SELECT ON *.* TO bender;
root@akonyaev-laptop:/var/lib/clickhouse/access#
```

Local Directory

```
<users>
      <default>
        <password_sha256_hex>65e84be33537c5</password_sha256_hex>
        <networks incl="networks" replace="replace">
            <ip>::1</ip>
            <ip>127.0.0.1</ip>
        </networks>
        <profile>default</profile>
        <quota>default</quota>
        <access_management>1</access_management>
      </default>
</users>
```

LDAP - только аутентификация

```
<ldap_servers>
    <my_ldap_server>
        <host>172.17.0.1</host>
        <port>389</port>
        <auth_dn_prefix>cn=</auth_dn_prefix>
        <auth_dn_suffix>,ou=people,dc=planetexpress,dc=com</auth_dn_suffix>
        <enable_tls>no</enable_tls>
    </my_ldap_server>
</ldap_servers>
```



Это будет простой SimpleBind

Лучше используйте TLS)))

LDAP - только аутентификация

Создаём пользователя:

```
CREATE USER fry IDENTIFIED WITH ldap_server BY 'my_ldap_server';
```

name	storage	auth_type	auth_params
fry	local directory	ldap_server	{"server":"my_ldap_server"}

LDAP - storage

Можно забирать пользователя из ldap (доступно с версии 20.11):

```
<user_directories replace="replace">
        <ldap>
                <server>my_ldap_server</server>
                <roles><my_role /></roles>
        </ldap>
</user_directories>
```

Для всех пользователей из base_dn указанных в my_ldap_server будет применяться роли указанные в конфиге.

LDAP - storage

В таблице system.users пользователь виден после того как вы впервый раз залогинетесь:

name	storage	auth_type	auth_params
professor	ldap	ldap_server	{"server":"my_ldap_server"}
leela	ldap	ldap_server	{"server":"my_ldap_server"}

Чего нет, но очень ждём.

- Группы (роли) которые можно импортировать из ldap.
- Фильтры для ldap-серверов (секция <ldap_servers>)

Есть Проблема №2

Нет возможности интеграции с сервисами требующей kerberos-аутентификации

Good News Everyone №2!

1. Библиотека krb5 теперь в contrib.
2. Авторизация в Kafka при помощи kerberos.
3. Авторизация в HDFS при помощи kerberos. (создан PR)
4. Теперь можно обсудить авторизацию в ClickHouse через kerberos.
   (Но вопросов пока много)

Авторизация в Kafka при помощи kerberos.

Конфигурация:

```
<yandex>
   <kafka>
      <security_protocol>SASL_PLAINTEXT</security_protocol>
      <sasl_mechanism>GSSAPI</sasl_mechanism>
      <sasl_kerberos_service_name>kafka</sasl_kerberos_service_name>
      <sasl_kerberos_keytab>/tmp/keytab/clickhouse.keytab</sasl_kerberos_keytab>
      <sasl_kerberos_principal>clickhouse@TEST.CLICKHOUSE.TECH</sasl_kerberos_principal>
   </kafka>
</yandex>
```

Для каждого топика можно задать свою конфигурацию.

Дополнительно: https://github.com/edenhill/librdkafka/blob/master/CONFIGURATION.md

Авторизация в Kafka при помощи kerberos.

Конфигурация:

Также необходимо поставить пакет krb5-user

И сконфигурировать /etc/krb5.conf на всех хостах clickhouse
Пример:

```
[libdefaults]
 default_realm = TEST.CLICKHOUSE.TECH
.......
[realms]
 TEST.CLICKHOUSE.TECH = {
  kdc = kafkakerberos
  admin_server = kafkakerberos
 }
[domain_realm]
 .test.clickhouse.tech = TEST.CLICKHOUSE.TECH
 test.clickhouse.tech = TEST.CLICKHOUSE.TECH
```

Авторизация в HDFS при помощи kerberos.

Ещё не вмержено.

У datanode в hdfs есть два варианта настройки безопасности:

- Привилегированный порт **РАБОТАЕТ**
- via SASL **НЕ РАБОТАЕТ**

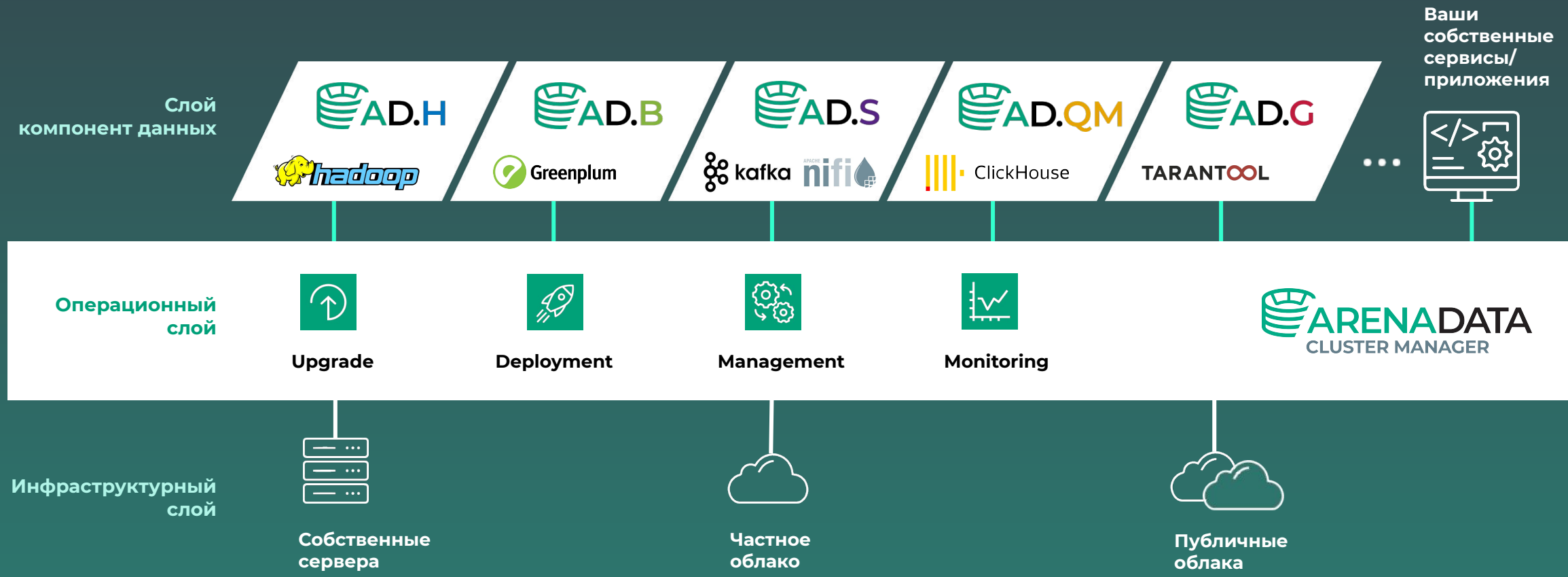
Проблема в том, что ванильный libhdfs3, используемый ClickHouse, не может использовать SASL для работы с datanode.

ARENADATA

Корпоративная платформа хранения
и обработки больших данных

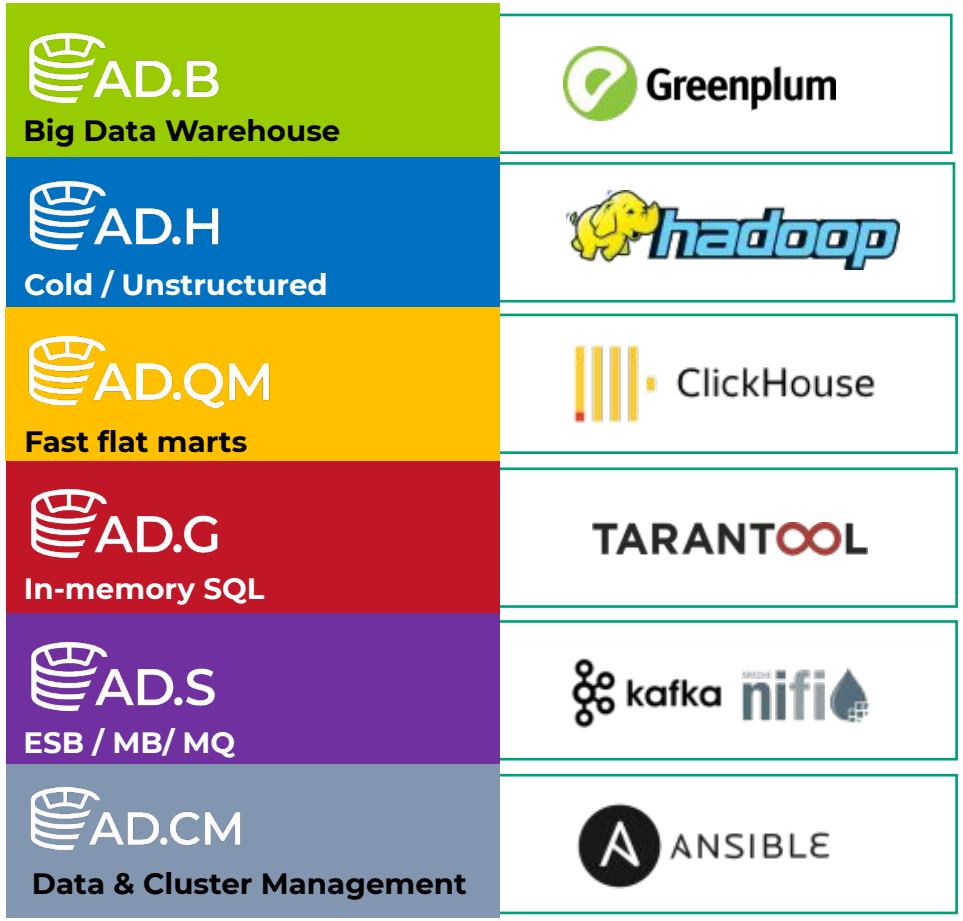
О нас

Гибридная корпоративная платформа



ARENADATA

Vanilla vs Arenadata EDP



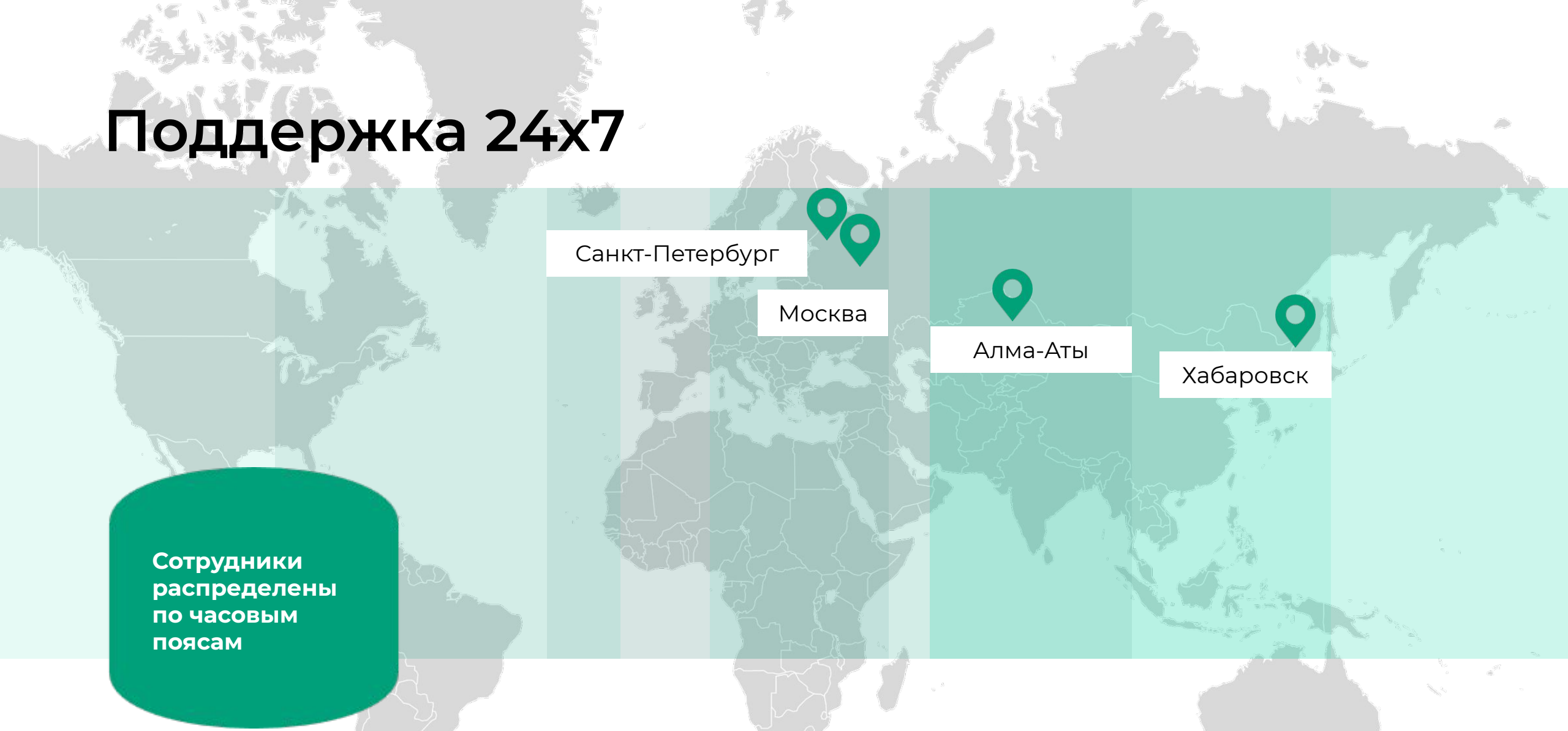
Каждый добавляемый компонент платформы доработан, чтобы стать её частью.

Производится:

- Анализ кода
- Интеграция с модулем мониторинга
- Проверки отказоустойчивости
- Проведение пилотных проектов и PoC
- Подбор компетентного персонала поддержки
- Доработка возможностей параллельной интеграции
- Множественные прочие проверки и доработки

ARENADATA

Поддержка 24x7



Сотрудники распределены по часовым поясам

ARENADATA

Курсы по Arenadata QuickMarts

Знания из первых рук
Наши преподаватели — практикующие специалисты, имеющие за плечами богатую экспертизу и значительное количество реализованных бизнес-кейсов.

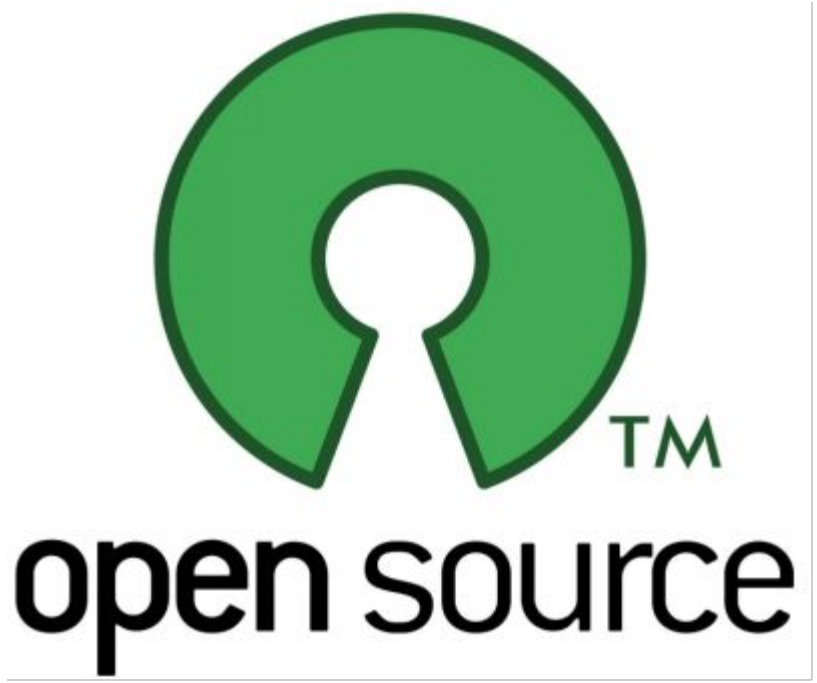
Только 40% теории
Все курсы построены на реальных кейсах и практических примерах, а лабораторные работы проходят на стендах, симулирующих рабочую среду.

Сертификация
Пройдя обучение на курсах Arenadata и успешно сдав экзамен, слушатель станет обладателем именного сертификата, подтверждающего полученные знания.

ARENADATA

Открытый исходный код

- **Вносим вклад в проекты Apache Software Foundation:**
  - Apache Ambari
  - Apache Bigtop
  - Apache PXF
- **2ой в мире контрибьютор** Greenplum Database
- Активный контрибьютор **ClickHouse** и **Tarantool**
- Выпускаем **собственное ПО** в Community-редакциях



ARENADATA

Корпоративная платформа хранения
и обработки больших данных

Оцените потенциал Big Data и Open Source вместе с Arenadata Enterprise Data Platform

- Узнайте больше на **arenadata.tech**
- Скачайте бесплатно на **store.arenadata.io**
- Получите консультацию по почте **info@arenadata.io**

ARENADATA