



Система управления  
ИТ-инфраструктурой

# Зодиак.АйТиЭм

Руководство по быстрой  
установке на ALT Linux

Версия 1.01

## ОГЛАВЛЕНИЕ

1.	Общее Описание системы управления «Зодиак».....	3
1.1	Список используемых сокращений и терминов .....	3
1.2	Архитектура решения.....	3
1.3	Требования к программному и аппаратному обеспечению .....	4
1.3.1	Серверная компонента .....	4
1.3.2	Клиентские машины .....	4
2.	Установка системы «Зодиак на ОС ALT LINUX.....	5
2.1	Подготовка СУБД.....	5
2.2	Подготовка SSL-сертификатов .....	6
2.3	Установка сервера администрирования.....	7
2.3.1	Установка сертификата сервера .....	7
2.3.2	Подготовка файла конфигурации .....	9
2.3.3	Создание служебных директорий.....	10
2.3.4	Установка сертификатов СА.....	10
2.3.5	Установка RPM-пакета .....	11
2.4	Установка сервера коммуникации .....	12
2.4.1	Подготовка файла конфигурации .....	12
2.4.2	Установка RPM-пакета .....	13
2.5	Установка агента .....	14
2.5.1	Установка RPM-пакета агента.....	14
2.5.2	Конфигурирование агента .....	14
2.5.3	Установка сертификатов СА для агента .....	15
2.6	Типичные ошибки при установке системы под ОС Linux .....	15

# 1. ОБЩЕЕ ОПИСАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ «ЗОДИАК»

Система «Зодиак» предназначена для автоматизации целого ряда ключевых сценариев для централизованного управления ИТ-инфраструктурой предприятия.

## 1.1 Список используемых сокращений и терминов

Таблица 1.1 Список используемых сокращений и терминов

Термин	Описание
База данных, БД	База данных PostgreSQL. Может использоваться сторонний кластер СУБД PostgreSQL. Хранит информацию о настройках системы, результаты сбора и анализа данных.
Виртуальная машина, VM	Программа, которая эмулирует реальный (физический) компьютер со всеми его компонентами (жесткий диск, DVD-ROM, BIOS, сетевые адаптеры и т.д.).
Система «Зодиак»	Система управления ИТ-инфраструктурой Зодиак.АйТиЭм.
Хост	Физический или виртуальный сервер, на котором установлен один или несколько компонентов системы «Зодиак».

## 1.2 Архитектура решения

Система «Зодиак» реализует агентскую схему, в которой на каждый управляемый объект ИТ-инфраструктуры устанавливается специальный **кроссплатформенный агент**, высоко оптимизированный по уровню потребления вычислительных ресурсов системы, который в дальнейшем взаимодействует с серверной компонентой системы.

Для обеспечения возможности гибкой настройки и оптимизации потоков данных в системе «Зодиак» серверная компонента разделена на две составляющие: сервер коммуникации и сервер администрирования.

**Сервер коммуникации** предназначен для непосредственного взаимодействия с агентами для получения от них результатов работы и передачи команд и изменений конфигурации. Сервер (или кластер серверов) коммуникации также осуществляет кеширование данных в случае высокой нагрузки, которая возможна при обслуживании большого количества агентов (сотни тысяч).

**Сервер администрирования** предоставляет веб-интерфейс администратора системы «Зодиак» для управления конфигурацией агентов, назначения заданий, просмотра результатов выполнения заданий, настройки представлений данных и т.п.

В минимальной конфигурации должны быть установлены по одному экземпляру каждой из серверных компонент системы.

## 1.3 Требования к программному и аппаратному обеспечению

### 1.3.1 Серверная компонента

Серверная часть системы «Зодиак» может быть установлена для работы под управлением одной из следующих операционных систем в минимальной установке:

- ALT Server 10.2

### 1.3.2 Клиентские машины

**Минимальные** требования к ОС для установки агентов

- Alt Workstation 10.2

## 2. УСТАНОВКА СИСТЕМЫ «ЗОДИАК НА ОС ALT LINUX

### 2.1 Подготовка СУБД

Все команды в данном разделе выполняются из-под пользователя root на хосте с **ALT Server**

1. Установите PostgreSQL с помощью пакетного менеджера (PostgreSQL должен быть не ниже 12 версии).

```
apt-get update
apt-get install postgresql14-server postgresql14-contrib
```

2. Инициализируйте БД:

```
/etc/init.d/postgresql initdb
```

3. Запустим службу PostgreSQL

```
systemctl enable postgresql.service
systemctl start postgresql.service
```

4. Создайте базу данных **zodiac** (если требуется создайте отдельную роль для работы с базой данных вместо postgres)

```
su - postgres -s /bin/bash
```

```
psql -c "CREATE DATABASE zodiac OWNER postgres ENCODING 'UTF8'
LC_COLLATE 'ru_RU.UTF-8' LC_CTYPE = 'ru_RU.UTF-8'
TEMPLATE='template0';"
```

5. Задайте пароль пользователю postgres

```
su - postgres -s /bin/bash
```

```
psql postgres
```

```
\password
```

6. Для создания таблиц в базе данных **zodiac** выполните скрипт **dbscripts/create-db.sql** из состава дистрибутива системы «Зодиак».

```
psql -h 127.0.0.1 -p 5432 -U postgres -d zodiac -f ./create-db.sql
```

## 2.2 Подготовка SSL-сертификатов

Все команды в данном разделе выполняются из-под пользователя root на хосте с **ALT Server**

Вы можете создать или должны иметь в наличии:

1. Сертификат(ы) CA
2. Сертификат(ы) веб-сервера, выпущенный от имени CA для серверов keycloak, администрирования (zodiac.administration), коммуникации (zodiac.communication)

Сертификатов CA может быть один или несколько.

Сертификатов веб-серверов может быть один или несколько.

Нам проще и удобней создать один сертификат CA и один сертификат веб-сервера.

Для удобства создания сертификатов можете воспользоваться shell скриптами, распространяемыми с этой инструкцией.

Задайте переменные в файле **quick\_install/gen-certs/vars.certs.sh**

1. Используйте **пароль** не менее 6 символов для переменной certPwd
2. Укажите корректные **DNS имена сервера** для переменной certDnsAltName, они используются в качестве subjectAltName

### ! Примечание

Обратите внимание на то, что для сертификата требуется корректно заполнить все DNS имена серверов, на которых он будет применяться

например

```
certDnsAltName="DNS:zodiac-admin,DNS:zodiac-comm,DNS:zodiac-keycloak,DNS:zodiac-admin.myorg.local,DNS:zodiac-comm.myorg.local,DNS:zodiac-keycloak.myorg.local"
```

Запустите **quick\_install/gen-certs/createCerts.sh**

```
./createCerts.sh
```

При выполнении будет выдана информация о процессе генерации и о сгенерированных сертификатах:

```
./createCerts.sh
./CA_certs already exists, you want delete folder and re-create CA
certificates (y/yes, others keys - no) ?
y
Generating a RSA private key
.....++++
.....++++
writing new private key to 'zdc_ca_cert.key'
-----
./certs already exists, you want delete folder and re-create
certificates (y/yes, others keys - no) ?
y
```

```
Generating a RSA private key
.....++++
.....++++
writing new private key to './../CA_certs/zdc_ca_cert.key'
-----
Generating a RSA private key
.....++++
.....++++
writing new private key to 'zdc_serv_cert.key'
-----
subjectAltName=DNS:alt-server-10Signature ok
subject=CN = alt-server-10
Getting CA Private Key
certificates in certs
CA_cert info
SHA1
Fingerprint=4F:76:3E:85:D1:50:1C:CC:1C:75:67:06:04:D0:3B:9F:63:ED:06:9
C
SHA1 Fingerprint=4F763E85D1501CCC1C75670604D03B9F63ED069C
-----
server cert info
SHA1
Fingerprint=4E:99:C2:9A:54:BE:74:FC:34:68:D0:BC:0F:AF:08:5D:E1:5C:B6:9
F
X509v3 Subject Alternative Name:
    DNS:alt-server-10
SHA1 Fingerprint=4E99C29A54BE74FC3468D0BC0FAF085DE15CB69F
```

Thumbprint сертификата **сервера** представлен в конце вывода – ‘SHA1 Fingerprint=4E99C29A54BE74FC3468D0BC0FAF085DE15CB69F, он будет использоваться в конфигурациях при дальнейшей настройке.

Сгенерированные сертификаты будут расположены в директориях **gen-certs/CA\_certs** и **gen-certs/certs**

Сертификат CA расположен в **gen-certs/CA\_certs**, вам потребуется публичный ключ **zdc\_ca\_cert.crt**

Сертификат сервера расположен в **gen-certs/certs**, вам потребуется файл **zdc\_serv\_cert.pfx**

## 2.3 Установка сервера администрирования

Все команды в данном разделе выполняются из-под пользователя root на хосте с **ALT Server**

### 2.3.1 Установка сертификата сервера

Скопируйте файл **certtool.zip** из состава дистрибутива, например, в папку **/var/zodiac/certtool**.

1. Распакуйте архив, выполнив следующую команду:

```
unzip certtool.linux.x64.zip
```

2. Задайте разрешение на исполнение файла **Zodiac.CertificateTool** (в каталоге certtool):

```
chmod 755 Zodiac.CertificateTool
```

3. От имени **суперпользователя** выполните следующую команду:

```
./Zodiac.CertificateTool add /var/zodiac/cert/zdc_serv_cert.pfx
```

Во время выполнения команды будет запрошен ввод PEM-пароля. При успешном выполнении команды на экран будет выведен отпечаток сертификата - Thumbprint.

Сохраните его в удобном месте, он пригодится в дальнейшем

```
[root@alt-server-10 certtool]# ./Zodiac.CertificateTool add /var/zodiac/cert/zdc_serv_cert.pfx
Enter password: *****
Adding certificate... OK
Successfully added certificate to store.
Thumbprint: 4E99C29A54BE74FC3468D0BC0FAF085DE15CB69F
```

*Рисунок 2.1 Добавление SSL-сертификата*

---

### **Осторожно**

Обратите внимание на то, что **по умолчанию** выполнение команды `Zodiac.CertificateTool add` следует производить от `root` (строка на рисунке начинается с `[root@zdc-srv...]`)

---



### 2.3.2 Подготовка файла конфигурации

В папке `/var/zodiac/administration-server` создайте файл `administration.ini`

```
mkdir -p /var/zodiac/administration-server  
nano /var/zodiac/administration-server/administration.ini
```

Поместите туда следующее содержимое

```
URLS="https://alt-server-10:443/"  
  
[Kestrel:EndpointDefaults]  
Protocols=Http1  
  
[Certificate]  
Store=CurrentUser  
Thumbprint=4E99C29A54BE74FC3468D0BC0FAF085DE15CB69F  
  
[WebInterface]  
WebAdministrationUrl = "https://alt-server-10:443/"  
Authenticate = false  
ShowPii = true  
  
[Roles]  
Enabled = false  
  
[ConnectionStrings]  
ZodiacContext="Server=127.0.0.1;Port=5432;Database=zodiac;UserID=postgres;Password=postgres;"  
  
[Packages]  
Dir = "/var/zodiac/scatter-packages"  
  
[Guacamole]  
DefaultGuacd = "alt-server-10:4822"  
  
[OTA]  
AgentDir = "/var/zodiac/updates"  
TempDir = "/var/zodiac/updates_temp"  
  
[Audit]  
LogFileOn = true  
LogFile = "../audit/audit.log"  
LogFilesLimit = 300  
  
SyslogOn = false  
SyslogPath = "/dev/log"  
SyslogTransport = UnixSocket  
  
[OidcConfiguration]  
ClientId = "zodiac"  
RedirectUri = "https://alt-server-10:443/#/authentication/callback"  
ResponseType = "code"  
PostLogoutRedirectUri = "https://alt-server-10:443/"
```

```
Scope = "openid profile email"
Authority = "https://keycloak:8443/auth/realms/master"
SilentRedirectUri = "https://alt-server-10:443/portal/silent_callback.html"
AutomaticSilentRenew = true
LoadUserInfo = true
AdministrationAudience = "zodiac"
```

Параметр **URLS** должен содержать имя хоста и порт. По умолчанию используется 443 порт.

Параметр **WebAdministrationUrl** также должен содержать имя хоста и порт. По умолчанию используется 443 порт.

---

### **Осторожно**

Обратите внимание на то, что при установке ОС по умолчанию, на порту 443 развернут Apache Web Server. Его необходимо отключить командами `systemctl stop httpd2` и `systemctl disable httpd2`.

---

Параметр **Thumbprint** должен содержать отпечаток сертификата сервера (отображается при выполнении п. 2.3.1)

Параметр **ZodiacContext** должен содержать строку подключения к СУБД PostgreSQL. При установке по инструкции не изменяется

Остальные параметры оставить неизменными.

### **2.3.3 Создание служебных директорий**

Создайте каталог `/var/zodiac/updates`

Создайте каталог `/var/zodiac/updates_temp`

Создайте каталог `/var/zodiac/scatter-packages`

```
mkdir /var/zodiac/updates
mkdir /var/zodiac/updates_temp
mkdir /var/zodiac/scatter-packages
```

### **2.3.4 Установка сертификатов CA**

Так же следует добавить и сертификат(ы) CA от имени которых выпущен(ы) сертификат(ы) сервера администрирования.

1. Установите `ca-certificates` (или аналогичный пакет если потребуется)

```
apt-get install ca-certificates
```

2. Скопируйте сертификат CA в папку с сертификатами

```
cp $ca_cert /etc/pki/ca-trust/source/anchors/zdc_ca_cert.crt
```

где `$ca_cert` – путь до файла сертификата CA

3. Обновите сертификаты

```
update-ca-trust
```

## 2.3.5 Установка RPM-пакета

Скопируйте файл **zodiac.administration.server.linux.x64.<версия>.rpm** из состава дистрибутива на сервер, и выполните следующую команду, например:

```
apt-get install ./zodiac.administration.server.linux.x64.1.6.4.rpm
```

Корректность установки можно проверить, выполнив команду

```
systemctl status zodiac.administration.server.service
```

В случае корректной установки будет выдано следующее сообщение:

```
[root@alt-server-10 ~]# systemctl status zodiac.administration.server.service
● zodiac.administration.server.service - Zodiac Administration Server
   Loaded: loaded (/etc/systemd/system/zodiac.administration.server.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2024-02-06 20:31:29 MSK; 33s ago
     Main PID: 9829 (Zodiac.Administ)
       Tasks: 17 (limit: 2356)
      Memory: 116.7M
         CPU: 7.924s
    CGroup: /system.slice/zodiac.administration.server.service
            └─ 9829 /opt/zodiac/administration-server/Zodiac.AdministrationServer
```

Рисунок 2.2 Проверка статуса службы сервера администрирования

Также в случае корректной установки по внешнему адресу, указанному в параметре **URLS** файла конфигурации **administration.ini**, станет доступным веб-интерфейс системы «Зодиак»

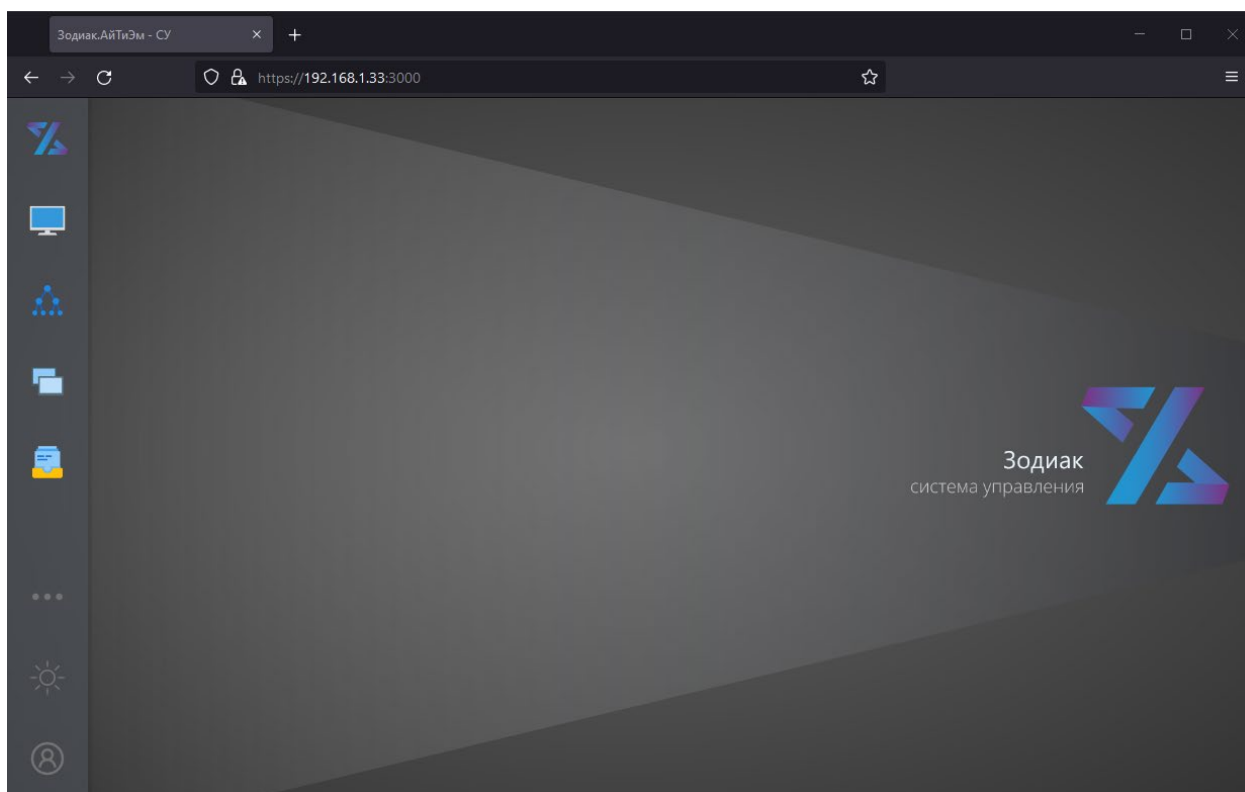


Рисунок 2.3 Экран веб-интерфейса системы «Зодиак»

## 2.4 Установка сервера коммуникации

Все команды в данном разделе выполняются из-под пользователя `root` на хосте с **ALT Server**

### 2.4.1 Подготовка файла конфигурации

В папке `/var/zodiac/communication-server` создайте файл `communication.ini`

```
mkdir -p /var/zodiac/communication-server
nano /var/zodiac/communication-server/communication.ini
```

Поместите в него следующее содержимое

```
URLS="https://alt-server-10:3001/"

[Certificate]
Store=CurrentUser
Thumbprint=4E99C29A54BE74FC3468D0BC0FAF085DE15CB69F

[ConnectionStrings]
ZodiacContext="Server=127.0.0.1;Port=5432;Database=zodiac;UserID=postgres;Password=postgres;"

[Processing:TakeLimit]
default=100
basic_inventory=100
script_stat=100
script_results=100

[Packages]
Dir = "/var/zodiac/scatter-packages"

[OTA]
AgentDir = "/var/zodiac/updates"
```

Параметр **Thumbprint** должен содержать отпечаток сертификата сервера

Параметр **URLS** должен содержать внешний адрес, который должен быть связан с сервером коммуникации.

#### **Осторожно**

Внешний адрес сервера коммуникации должен отличаться от адреса, используемого сервером администрирования. Если оба сервера устанавливаются на одной машине, должны различаться используемые порты – например **3000** и **3001**, соответственно.

Параметр **ZodiacContext** должен содержать строку подключения к СУБД PostgreSQL,

#### **Примечание**

Для подключения сервера коммуникации к БД должен использоваться тот же экземпляр БД, который использовался при установке сервера администрирования.

## 2.4.2 Установка RPM-пакета

Для работы сервера на некоторых Linux потребуется установить curl и после этого уже можно устанавливать пакет сервера.

Скопируйте файл **zodiac.communication.server.rhel80.x64.<version>.rpm** из состава дистрибутива на сервер, и выполните следующую команду, например:

```
apt-get install ./zodiac.communication.server.rhel80.x64.1.6.4.rpm
```

Корректность установки можно проверить выполнив команду

```
systemctl status zodiac.communication.server.service
```

В случае корректной установки будет выдано следующее сообщение:

```
[root@zdc-srv ~]# systemctl status zodiac.communication.server.service
● zodiac.communication.server.service - Zodiac Communication Server
   Loaded: loaded (/opt/zodiac/communication-server/zodiac.communication.server.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2022-03-29 11:08:29 UTC; 2min 12s ago
     Main PID: 16545 (Zodiac.Communic)
        Tasks: 49 (limit: 1081)
       Memory: 141.7M
      CGroup: /system.slice/zodiac.communication.server.service
              └─16545 /opt/zodiac/communication-server/Zodiac.CommunicationServer
                 └─16606 /opt/zodiac/communication-server/mongod --dbpath /var/zodiac/communication-server/store/ --logpath /var/z
```

Рисунок 2.4 Проверка статуса службы сервера коммуникации

## 2.5 Установка агента

Все команды в данном разделе выполняются из-под пользователя root на хосте с **ALT WORKSTATION**

### 2.5.1 Установка RPM-пакета агента

Скопируйте файл `zodiac.agent.linux.x64.<version>.rpm` из состава дистрибутива системы «Зодиак», и выполните следующую команду:

```
apt-get install ./zodiac.agent.linux.x64.1.6.3.rpm
```

Корректность установки можно проверить выполнив команду

```
systemctl status zodiac-agent.service
```

В случае корректной установки будет выдано следующее сообщение:

```
[root@zdc-srv ~]# systemctl status zodiac.agent.service
● zodiac.agent.service - zodiac agent
   Loaded: loaded (/opt/zodiac/agent/zodiac.agent.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2022-03-30 04:42:31 UTC; 3min 51s ago
     Main PID: 79998 (zodiac)
        Tasks: 11 (limit: 1081)
       Memory: 18.0M
      CGroup: /system.slice/zodiac.agent.service
             └─79998 /opt/zodiac/agent/zodiac /opt/zodiac/agent/lib/agent.js
```

Рисунок 2.5 Проверка статуса службы агента



### Совет

В случае возникновения критических ошибок при запуске агента, информацию об ошибках можно найти в файле `/var/zodiac/agent/agent.critical.log`.

Например, сразу после установки агент нуждается в задании такого параметра конфигурации как адрес сервера коммуникации. Если адрес не задан, журнал будет содержать следующую запись:

```
2022-03-30T04:42:31.822Z ERROR [79998] Agent.main: error
reading configuration files: StaticConfig.load: failed to load:
server url missing
```

### 2.5.2 Конфигурирование агента

Для конфигурирования агента нужно задать как минимум адрес сервера коммуникации. С этой целью нужно создать файл `/var/zodiac/agent/agent.ini` со следующим содержимым:

```
[Server]
url=https://192.168.1.33:3001
```

Здесь, параметр `url` должен содержать адрес сервера коммуникации, сконфигурированный при его создании. После этого перезагрузите агент командой

```
systemctl restart zodiac-agent.service
```

### 2.5.3 Установка сертификатов СА для агента

Вам следует добавить сертификат(ы) СА от имени которых выпущен сертификат **сервера коммуникации** в доверенные.

1. Скопируйте сертификат СА, созданный на этапе 2.2. на хост, а затем положите его в папку с сертификатами

```
cp $ca_cert /etc/pki/ca-trust/source/anchors/zdc_ca_cert.crt
```

где \$ca\_cert – путь до файла сертификата СА

2. Обновите сертификаты.

```
update-ca-trust
```

## 2.6 Типичные ошибки при установке системы под ОС Linux

Для просмотра журналов всех systemd unit-сервисов удобно использовать такой инструмент как **journalctl**. Следующая команда выводит записи в конце журнала (параметр **-f**) для сервиса сервера администрирования (параметр задания юнита **-u**).

```
journalctl -u zodiac.administration.server.service -f
```

В результате выполнения команды можно обнаружить сообщения об ошибках, препятствующих штатному запуску системы:

```
[root@zdc-srv srv-adm]# journalctl -u zodiac.administration.server.service -f
-- Journal begins at Tue 2022-03-15 12:27:08 UTC. --
Apr 04 09:21:11 zdc-srv Zodiac.AdministrationServer[530081]: The configuration file 'config.ini' was not found
odiac/administration-server/config.ini'.
Apr 04 09:21:11 zdc-srv systemd[1]: zodiac.administration.server.service: Main process exited, code=exited, st
Apr 04 09:21:11 zdc-srv systemd[1]: zodiac.administration.server.service: Failed with result 'exit-code'.
```

Рисунок 2.6 Вывод журнала сервера администрирования

В следующей таблицы приведены сообщения о наиболее часто встречающихся ошибках при неправильном конфигурировании системы.

Сообщение	Причина и устранение
The configuration file 'administration.ini' was not found and is not optional. The physical path is '/var/zodiac/administration-server/administration.ini'.	Отсутствует файл конфигурации. Для устранения ошибки нужно создать файл конфигурации для сервера администрирования или для сервера коммуникации.
Message "28000: no pg_hba.conf entry for host "192.168.1.41", user "postgres", database "zodiac", SSL off"	Нет доступа извне к серверу БД. Для устранения в рамках тестовой эксплуатации достаточно будет обеспечить наличие в файле конфигурации <b>postgresql.conf</b> сервера БД параметра

	<pre>listen_addresses = '*'</pre> <p>и наличие в файле конфигурации <b>hba.conf</b> сервера БД записи</p> <pre>host all all 0.0.0.0/0 md5</pre>
Microsoft.AspNetCore.Authentication.JwtBearer.JwtBearerHandler[3] Exception occurred while processing message.	Проверьте сертификаты на ПК с соответствующим сервером
Npgsql.PostgresException (0x80004005): 3D000: database "postgres" does not exist	Не была создана БД <b>zodiac</b>
Npgsql.PostgresException (0x80004005): 42P01: отношение "scatter_package_upload" не существует	Не был выполнен скрипт <b>dbscripts/create-db.sql</b>
Нечитаемые символы в сообщениях Npgsql.PostgresException от сервера БД.	Поменяйте в файле конфигурации <b>postgresql.conf</b> сервера БД значение параметра <b>lc_messages</b> : <pre>lc_messages = 'English_United States.1252'</pre>
Ошибка 401 в UI после логина	Проверьте совпадение часов на сервере и на хосте, откуда производится подключение