

Система управления ИТ-инфраструктурой

Зодиак.АйТиЭм

Руководство по установке

Версия 3.17

ОГЛАВЛЕНИЕ

1.		Обц	цее Описание системы управления «Зодиак»	5
	1.1		Список используемых сокращений и терминов	5
	1.2	<u>2</u> A	Архитектура решения	5
	1.3	З Т	ребования к программному и аппаратному обеспечению	6
		1.3.1	1 Серверная компонента	6
		1.3.2	2 СУБД PostgreSQL	6
		1.3.3	3 Клиентские машины	6
2.		Уста	ановка системы «Зодиак» под управлением ОС семейства Windows	7
	2.1	5	/становка СУБД PostgreSQL	7
	2.2	2 F	lастройка СУБД PostgreSQL	13
		2.2.	1 Настройка языка системных сообщений	13
		2.2.2	2 Предоставление внешнего доступа	13
		2.2.3	3 Настройка брандмауера Windows	14
	2.3	3 (Создание базы данных	14
	2.4	1 3	/становка KeyCloak	18
		2.4.′	1 Установка OpenJDK	19
		2.4.2	2 Распаковка дистрибутива KeyCloak	22
		2.4.3	3 Установка SSL-сертификата	22
		2.4.4	4 Подготовка файла конфигурации	23
		2.4.	5 Запуск сервера KeyCloak	23
		2.4.6	6 Создание начальной учетной записи администратора	24
		2.4.7	7 Создание клиента для системы «Зодиак»	25
		2.4.8	3 Настройка брандмауера Windows	31
	2.5	5 3	/становка сервера администрирования	31
		2.5.1	1 Установка распространяемых компонентов Microsoft Visual C++	31
		2.5.2	2 Установка SSL-сертификата для доступа к веб-консоли	31
		2.5.3	3 Подготовка файла конфигурации	32
		2.5.4	4 Подготовка файла конфигурации с настройкой аутентификации	32
		2.5.	5 Запуск инсталлятора	33
		2.5.6	6 Настройка брандмауера Windows	34
	2.6	3	/становка сервера коммуникации	34
		2.6.′	1 Установка распространяемых компонентов Microsoft Visual C++	34

	2.	6.2	Установка SSL-сертификата для доступа агентов	. 34
	2.	6.3	Подготовка файла конфигурации	. 34
	2.	6.4	Запуск инсталлятора	. 35
	2.	6.5	Настройка брандмауера Windows	. 36
2.	7	Уста	ановка агента	. 36
	2.	7.1	Запуск инсталлятора	. 36
	2.	7.2	Конфигурирование агента	. 38
3. Astra	Ус a lir	стано пих	вка системы «Зодиак» под управлением ОС семейства Linux на примере	OC . 40
3.	1	Уста	ановка базовых компонентов	. 40
	3.	1.1	Инсталляция OC ASTRA LINUX	. 40
	3.	1.2	Установка SSL-сертификата для доступа к веб-интерфейсу	. 45
	3.	1.3	Подготовка СУБД	. 46
3.	.2	Уста	ановка keycloak	. 47
3.	.3	Уста	ановка guacamole	. 49
3.	.4	Уста	ановка сервера администрирования	. 50
	3.	4.1	Подготовка файла конфигурации	. 50
	3.	4.2	Создание служебных директорий	. 52
	3.	4.3	Установка DEB-пакета	. 52
	3.	4.4	Задание ролевой модели (опционально)	. 53
3.	.5	Уста	ановка сервера коммуникации	. 54
	3.	5.1	Подготовка файла конфигурации	. 54
	3.	5.2	Создание служебных директорий	. 55
	3.	5.3	Установка DEB-пакета	. 55
	3.	5.4	Монтирование директории распространяемых пакетов (опционально)	. 55
3.	.6	Уста	ановка агента	. 55
	3.	6.1	Установка DEB-пакета агента	. 55
	3.	6.2	Конфигурирование агента	. 56
	3.	6.3	Конфигурирование агента как точки обслуживания (опционально)	. 57
4.	Π	рилох	кения	. 59
4.	1	Имп	юрт имеющегося SSL-сертификата в формате PFX	. 59
4.	.2	Гене	ерация самоподписанного SSL-сертификата под ОС Windows	. 64
	4.	2.1	Использование PowerShell	. 64
	4.	2.2	Использование OpenSSL	. 66
4.	.3	Гене	ерация самоподписанного SSL-сертификата под ОС Linux	. 66

4.3	3.1	Установка OpenSSL	66
4.3	3.2	Генерация сертификата и зашифрованного закрытого ключа	67
4.3	3.3	Генерация сертификата в формате PFX	67
4.3	3.4	Конвертация сертификата из формата РFX в формат РEM	67
4.3	3.5	Генерация сертификата и незашифрованного закрытого ключа	68
4.4	Ген	ерация подписанного УЦ сертификата под ОС Linux	68
4.4	4.1	Создание СА-сертификата	68
4.4	4.2	Создание запроса подписи	69
4.4	4.3	Создание временного файла	69
4.4	4.4	Генерация сертификата в формате PFX	69
4.5	Hac 69	стройка доверия для самоподписанных сертификатов в ОС семейства Wind	ows
4.6	Hac	стройка доверия для самоподписанных сертификатов в ОС семейства Linux	74
4.7	Hac	стройка разрешений для порта в брандмауере Windows	74
4.8	Тип	ичные ошибки при установке системы под ОС Linux	79

1. ОБЩЕЕ ОПИСАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ «ЗОДИАК»

Система «Зодиак» предназначена для автоматизации целого ряда ключевых сценариев для централизованного управления IT-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.
Балансировщик нагрузки	Программное или аппаратное решение для распределения нагрузки входящих подключений между несколькими узлами сервиса.
Виртуальная машина, ВМ	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 ITинфраструктуры 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:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Альт 8 СП
- Альт 8
- Альт 8.1
- Альт 8.2
- Альт 9
- Альт 9.1
- Альт 9.2
- Astra Linux Common Edition, релиз «Орел» версии 2.12
- Astra Linux Special Edition, релиз «Смоленск» версии 1.6

Примечание

Операционные системы на базе ОС Linux должны включать systemd

Минимальные системные требования для серверов:

- 2 CPU;
- 1 Гбайт (GB) RAM;
- 100 Гбайт (GB) дискового пространства

1.3.2 СУБД PostgreSQL

Для установки серверной части системы «Зодиак» необходимо создать экземпляр СУБД PostgreSQL не ниже версии 12.

Данный единственный экземпляр СУБД предназначается для использования всеми компонентами серверной части системы «Зодиак».

1.3.3 Клиентские машины

Минимальные требования к ОС для установки агентов

- Windows 7
- Windows Server 2008 R2 или Windows Server 2012 R2
- Enterprise Linux 7 (RHEL and CentOS)
- Debian 8 или Ubuntu 14.04

2. УСТАНОВКА СИСТЕМЫ «ЗОДИАК» ПОД УПРАВЛЕНИЕМ ОС СЕМЕЙСТВА WINDOWS

2.1 Установка СУБД PostgreSQL

Дистрибутив СУБД PostgreSQL для Windows рекомендуется скачивать с официального сайта: <u>https://www.postgresql.org/download/windows/</u>.

Осторожно

Используйте СУБД PostgreSQL версии 12 или выше.

1. Поместите на диск и запустите инсталлятор PostgreSQL. В нашем примере используется **postgresql-12.10-2-windows-x64.exe**. На начальном экране установки нажмите кнопку «Next».



Рисунок 2.1 Начальный экран установки PostgreSQL

2. На следующем шаге **при необходимости** можно задать путь установки СУБД. Для продолжения нажмите кнопку «Next».

	Setup	_		x
Installation Direct	огу			
Please specify the dir Installation Directory	ectory where PostgreSQL will be installed. C:\Program Files\PostgreSQL\12			
VMware InstallBuilder —	< Back Next >		Cano	:el

Рисунок 2.2 Задание пути установки

3. На этапе выбора компонент СУБД, нужно оставить все значения по умолчанию. Для продолжения нажмите кнопку «Next».

📲 Set	up	– – X
Select Components		
Select the components you want to install; clear the cor you are ready to continue.	nponents you do not want to install.	Click Next when
 PostgreSQL Server pgAdmin 4 Stack Builder Command Line Tools 	PostgreSQL database server	
L VMware InstallBuilder	< Back Next >	Cancel

Рисунок 2.3 Выбор компонент СУБД

4. На следующем шаге **при необходимости** можно задать путь к папке, где будут храниться данные. Для продолжения нажмите кнопку «Next».

🧃 Set	up 🔄 🗖 🗙
Data Directory	*
Please select a directory under which to store your dat Data Directory ::\Program Files\PostgreSQL\12\data	a.
VMware InstallBuilder	< Back Next > Cancel

Рисунок 2.4 Задание пути хранения данных

5. На данном этапе установки СУБД необходимо задать пароль для суперпользователя (postgres) базы данных. После указания пароля для продолжения установки нажмите кнопку «Next».

	Setup	_		x
Password				
Please provide a Password Retype password	password for the database superuser (postgres).			
VMware InstallBuilde	<pre>er </pre> <pre>Sack Next ></pre>		Cance	el

Рисунок 2.5 Пример задания пароля супер пользователя (postgres)

6. На данном этапе TCP-порт (по умолчанию **5432**), на котором база данных принимает сетевые подключения, **не рекомендуется изменять**.

- N	Setup	– – X
Port		
Please select the port number the Port 5432	e server should listen on.	
VMware InstallBuilder	< Back	Next > Cancel

Рисунок 2.6 Окно выбора ТСР-порта

7. На данном этапе региональные настройки по умолчанию оставьте без изменения.

	Setup	_ 🗆 X
Advanced Options		
Select the locale to be used by the new datab Locale [Default locale]	ase duster.	
VMware InstallBuilder	< Back	Next > Cancel

Рисунок 2.7 Окно выбора региональных настроек по умолчанию

8. На данном этапе необходимо проверить все ранее указанные параметры и, если все задано верно, нажмите кнопку «Next» для продолжения.

•	Setup	-	• x
	Pre Installation Summary		
	The following settings will be used for the installation::		
	Installation Directory: C: \Program Files\PostgreSQL\12 Server Installation Directory: C: \Program Files\PostgreSQL\12 Data Directory: C: \Program Files\PostgreSQL\12\data Database Superuser: postgres Operating System Account: NT AUTHORITY\NetworkService Database Service: postgresql-x64-12 Command Line Tools Installation Directory: C: \Program Files\PostgreSQL\12 pgAdmin4 Installation Directory: C: \Program Files\PostgreSQL\12 Installation Log: C: \Users\Agmunuccrpatop\AppData\Local\Temp\2\install-postgresql.log		<
VM	ware InstallBuilder Kext >		Cancel

Рисунок 2.8 Окно проверки заданных параметров установки

9. На данном этапе для подтверждения начала установки нажмите кнопку «Next».

1	Setup	L	- 🗆 X
Ready to Install			
Setup is now ready to begin installing PostgreSQ	L on your computer.		
VMware InstallBuilder	< Back	Next >	Cancel

Рисунок 2.9 Окно подтверждения начала установки

10. Далее, следует дождаться завершения процесса установки.

1	Setup	_ 🗆 🗙
Installing		
Please wait while Setup installs PostgreSQL on	your computer.	
	Installing	
Unpacking C:\Program []locale\ko\LC_MESS/	AGES\pg_archivecleanup-12.mo	
VMware InstallBuilder	< Back	Next > Cancel

Рисунок 2.10 Окно прогресса установки

11. Установка СУБД успешно окончена. Для завершения работы мастера установки, необходимо нажать кнопку «Finish».



Рисунок 2.11 Окно завершения установки

2.2 Настройка СУБД PostgreSQL

2.2.1 Настройка языка системных сообщений

Некоторые приложения в определенных ситуациях могут отображать системные сообщения от PostgreSQL с включением нечитаемых символов из-за проблем с кодировкой.

Чтобы предотвратить такое поведение и избежать потенциальных проблем с диагностикой, отредактируйте (к примеру, используя приложение «Блокнот») файл **postgresql.conf** в папке **C:\Program Files\PostgreSQL\12\data** заменив следующую строчку:

```
lc messages = 'Russian Russia.1251'
```

на строчку:

```
lc messages = 'English United States.1252'
```

После этого перезапустите службу postgresql-x64-**.

9,		Службы						• >	×
Файл Действие І	Вид Справка								
♦ ♦ 🗊 🙆 🖥	III ■ III								
🎑 Службы (локалы	🔍 Службы (локальные)								
	postgresql-x64-12 - PostgreSQL	Имя	Описание	Состояние	Тип запуска	Вход от имени			^
	Server 12	OHCP-клиент	Регистрирует и обновляет IP-ад	Выполняется	Автоматиче	Локальная слу			
	-	🖏 DNS-клиент	Служба DNS-клиента (dnscache)	Выполняется	Автоматиче	Сетевая служба			
Остановить службу		🎑 KtmRm для координатора распределенных тр	Координирует транзакции межд		Вручную (ак	Сетевая служба			
	Перезапустить службу	🔍 Plug and Play	Позволяет компьютеру распозн	Выполняется	Вручную	Локальная сис	_		
		🤹 postgresql-x64-12 - PostgreSQL Server 12	Provides relational database stora	Выполняется	Автоматиче	Сетевая служба			=
		🥨 SMP дисковых пространств (Майкрософт)	Служба узла для поставщика уп		Вручную	Сетевая служба			-
	Описание: Provides relational database storage	🔍 Superfetch	Поддерживает и улучшает прои		Вручную	Локальная сис			
	riovides relational database storage.	🔍 Windows Audio	Управление средствами работы		Вручную	Локальная слу			
		🍓 Windows Driver Foundation - User-mode Driver	Создает процессы драйверов по		Вручную (ак	Локальная сис			

Рисунок 2.12 Перезапуск службы PostgreSQL

2.2.2 Предоставление внешнего доступа

По умолчанию после установки PostgreSQL базы данных будут доступны только локально, т.е. только на компьютере, на котором установлена СУБД.

Для разрешения нелокальных подключений с других хостов в сети добавьте необходимую запись в файл конфигурации hba.conf в папке C:\Program Files\PostgreSQL\12\data.

Осторожно

После модификации hba.conf перезапустите службу PostgreSQL как в разделе 2.2.1.

Например, для тестовых целей, добавление следующей записи разрешает удаленное подключений без ограничений:

host all all 0.0.0/0 md5

В результате список разрешений в файле hba.conf для подключений будет выглядеть следующим образом:

#^SIf you want to allow non-local connections, you need to add more
"host" records. In that case you will also need to make PostgreSQL
listen on a non-local interface via the listen_addresses
configuration parameter, or via the -i or -h command line switches.

# TYPE	DATABASE	USER	ADDRESS	METHOD
# IPv4	local connect	tions:		
host	all	all	127.0.0.1/32	md5
host	all	all	0.0.0/0	md5
# IPv6	local connect	tions:		
host	all	all	::1/128	md5
# Allow	<pre>v replication</pre>	connections	from localhost, by a user with	the
<pre># repl;</pre>	ication privil	lege.		
host	replication	all	127.0.0.1/32	md5
host	replication	all	::1/128	md5

Рисунок 2.13 Изменение списка разрешений в файле hba.conf

Осторожно

Удаленное подключение необходимо настроить, даже если вы устанавливаете все компоненты системы «Зодиак» на том же компьютере, что и СУБД PostgreSQL, но используете в конфигурационных файлах системы «Зодиак» для подключения к базе данных внешний IP-адрес компьютера, например 192.168.1.37.

2.2.3 Настройка брандмауера Windows

Если для экземпляра PostgreSQL используется отдельный выделенный хост, в брандмауере Windows необходимо открыть порт, заданный во время установки PostgreSQL (раздел 2.1). По умолчанию используется порт 5432.

Процедура задания разрешений для порта описана в разделе 4.6

2.3 Создание базы данных

1. Зайдите в меню «Приложения» и запустите веб-консоль **pgAdmin**, установленную в составе СУБД PostgreSQL, как описано в разделе 2.1.



Рисунок 2.14 Экран «Приложения» (Windows Server 2012 R2)

2. Если **pgAdmin** запускается в первый раз, появится окно для задания мастер-пароля. Задайте пароль (для тестовых целей можно задать postgres) и нажмите кнопку «OK».

eb.					pgAdmin 4		_ D X
Admin	File 🛩	Object	✓ Tools ✓	Help 🗸			
Browser		6	Bet Master Pa	Dashhoard Properties assword	SOI Statistics Depend	dencies Dependents	×
> E Servers			Please set This will be Password	a master password for pgAo used to secure and later un	lmin. lock saved passwords and o	ther credentials.	
		I.	?	graphical administration i	nterface, an SQL query tool, a	× Cancel • OK res	QL database. It includes a and much more. The tool is
				Quick Links			
				Add N	ew Server	Configur	re pgAdmin
				Getting Started			:2:
				PostgreSQL Documentation	pgAdmin Website	Planet PostgreSQL	Community Support

Рисунок 2.15 Ввод мастер-пароля pgAdmin

3. В браузере pgAdmin (слева) нажмите правой клавишей на узел сервера **PostgreSQL**. В появившемся контекстном меню выберите «**Create»** -> «**Database**».

壁	pgAdmin 4	
Pg Admin File ~ Object ~ Tools	∽ Help∽	
Browser 🗊 🖽 🗖	Dashboard Properties SQL Statistics Dependencies Dependents	
Servers (1) PostgreSOL 12 Databa Register	Server sessions Total Active Idle Transactions Transactions Commits	Rollbac
 A Login/ Tables Tables Refresh Backup Globals Backup Server 	Dutabase Login/Croup Role Tablespace 0	
Remove Server Add Named Restore P Reload Configuration Clear Saved Password Properties	Int	Hits
	Server activity Sessions Locks Prepared Transactions Configuration Q Search	0
	Pito Database User Application Client Backend start C Image: 100 million 2022-04-17 18400 MSK 2022-04-17 18400 MSK 2022-04-17 18400 MSK	State

Рисунок 2.16 Вызов окна создания базы данных

4. В открывшемся окне на вкладке «General» введите имя базы данных – zodiac.

📒 Create	- Database						2 ×
General	Definition	Security	Parameters	Advanced	SQL		
Database		zodia	d				
Owner		🐣 po	ostgres				
Comment	t						
							li
•					× Clo	ose 🧿 Reset	Save

Рисунок 2.17 Задание имени базы данных

5. Далее, на вкладке «Definition» задайте Collation - Russian_Russia.1251. Для создания базы данных нажмите «Save».

🤤 Create - Database		2 ×
General Definition S	ecurity Parameters Advanced SQL	
Encoding	UTF8	× ~
Template	Select an item	I ~
Tablespace	Select an item	I ~
Collation	Russian_Russia.1251	× ~
Character type	Select an item	I ~
Connection limit	-1	
•	X Close 🖸 Reset	Save

Рисунок 2.18 Задание Collation

6. В браузере pgAdmin (слева) нажмите правой клавишей на узел базы данных **zodiac**. В появившемся контекстном меню выберите «Query Tool».



Рисунок 2.19 Вызов редактора запросовPostgreSQL

7. Поместите в открывшееся окно Query Editor содержимое файла dbscripts/createdb.sql из состава дистрибутива системы «Зодиак». Для создания таблиц в базе данных zodiac выполните данный скрипт нажатием на кнопку «Execute».



Рисунок 2.20 Выполнение скрипта для создания таблиц в базе данных

8. При удачном завершении выполнения скрипта появится сообщение «Query returned successfully».



Рисунок 2.21 Сообщение об удачном выполнении скрипта

2.4 Установка KeyCloak

Технология единого входа (Single Sign-On) в системе «Зодиак» реализована через поддержку протокола OpenID Connect. В качестве сервера авторизации может быть использован любой OIDC-провайдер (в том числе ADFS). В нашем примере используется установка и настройка сервера авторизации на базе открытого и свободно распространяемого ПО «KeyCloak»

Примечание

Если тестовая эксплуатация не включает в себя использование SSO, данный раздел можно пропустить, и затем в файле конфигурации сервера администрирования использовать настройку **EnableAuth=false** для выключения аутентификации, как показано в разделе 2.5.3.

2.4.1 Установка OpenJDK

Для работы KeyCloak требуется предварительная установка OpenJDK версии 11 или выше.

Microsoft Build of OpenJDK — это бесплатный дистрибутив OpenJDK, который является открытым и свободно распространяемым ПО, и содержит двоичные файлы для Java 17.

1. Зайдите на страницу официального дистрибутива: <u>OpenJDK 17</u>, скачайте файл microsoft-jdk-17.0.2.8.1-windows-x64.msi и запустите установку.



Рисунок 2.22 Окно установщика OpenJD

2. Примите лицензионное соглашение и нажмите кнопку «Next».



Рисунок 2.23 Окно принятия лицензионного соглашения OpenJDK

3. В окне задания параметров установки включите опцию Set JAVA_HOME variable и нажмите кнопку «Next».

😸 Microsoft Build of OpenJDK with Hotspot 17.0.2+8 (x6 🗖 🗖 🗙
Custom Setup Image: Custom Setup Select the way you want features to be installed. Image: Custom Setup
Click the icons in the tree below to change the way features will be installed.
Image: Set JAVA_HOME environment Image: Set JAVA_HOME variable Set JAVA_HOME variable
Will be installed on local hard drive r
Entire feature will be installed on local hard drive
Entire feature will be unavailable
Browse
Reset Disk Usage Back Next Cancel

Рисунок 2.24 Окно задания параметров установки

4. В окне готовности к установке нажмите кнопку «Install».



Рисунок 2.25 Окно готовности к установке

5. Дождитесь завершения установки.

😸 Microsoft Build of OpenJDK with Hotspot 17.0.2+8 (x6 💻 🗖 🗙
Installing Microsoft Build of OpenJDK with Hotspot 17.0.2+8 (x64)
Please wait while the Setup Wizard installs Microsoft Build of OpenJDK with Hotspot 17.0.2+8 (x64).
Status: Publishing product information
Back Next Cancel

Рисунок 2.26 Окно процесса установки

6. В окне завершения установки нажмите кнопку «Finish»



Рисунок 2.27 Окно завершения установки OpenJDK

2.4.2 Распаковка дистрибутива KeyCloak

Зайдите на страницу официального дистрибутива: <u>KeyCloak 17.0.1</u>, скачайте файл keycloak-17.0.1.zip и распакуйте архив в каталог C:\keycloak-17.0.1.

2.4.3 Установка SSL-сертификата

Для правильного функционирования сервера авторизации **KeyCloack** необходимо обеспечить его работу по протоколу **HTTPS**. Для этого потребуется **SSL-сертификат** в формате **PEM**.

Если в вашей организации используется единый центр сертификации, произведите выпуск SSL-сертификата по принятым в вашей организации правилам для выбранного DNS-имени хоста сервера.



Если центр сертификации в вашей организации предоставляет сертификат только в формате **PFX**, сконвертируйте его в формат **PEM**, как описано в разделе 4.3.4.

Поместите файлы сертификата и незашифрованного закрытого ключа (в нашем примере cert.pem и key.pem, соответственно) в каталог C:\keycloak-17.0.1\conf.

Примечание

Для тестовых целей вы можете сгенерировать файлы cert.pem и key.pem для самоподписанного SSL-сертификата, как описано в разделе 4.3.5.

Осторожно

Если вы использовали сгенерированный **самоподписанный** сертификат, добавьте его (файл **cert.pem**) в список корневых доверенных сертификатов как описано в разделе 4.4.

2.4.4 Подготовка файла конфигурации

Отредактируйте содержимое файла C:\keycloak-17.0.1\conf\keycloak.conf следующим образом:

The file path to a server certificate or certificate chain in PEM
format.
https-certificate-file=\${kc.home.dir}/conf/cert.pem

The file path to a private key in PEM format. https-certificate-key-file=\${kc.home.dir}/conf/key.pem

Hostname for the Keycloak server. hostname=keycloak

Для параметра hostname задайте сетевое имя хоста, на котором производится установка KeyCloak. (keycloak в нашем примере).

Осторожно

Обратите внимание, чтобы субъект и дополнительное имя субъекта в сертификате совпадало с именем хоста, под которым он будет доступен в сети (keycloak в нашем примере).

2.4.5 Запуск сервера КеуСloak

Перейдите в каталог C:\keycloak-17.0.1 и выполните в командной строке kc.bat start. Убедитесь в наличии сообщения "Listening on: <u>https://0.0.0.0:8443</u>".

::\keycloak-17.0.1>bin\kc.bat start 2022-04-26 16:35:04.526 INFO [org.keycloak.quarkus.runtime.hostname.DefaultHost nameProvider1 (nain) Hostname settings: FrontEnd: keycloak, Strict HTIPS: true, Fath: (request), Strict BackChannel: false, Admin: (request), Port: -1, Proxied: false 2022-04-26 16:35:05,705 WARN [org.infinispan.CONFIG1 (keycloak-cache-init)] 18PN000554: jboss-marshalling is deprecated and planned for removal 2022-04-26 16:35:05,707 INFO [org.infinispan.CONTAINER] (keycloak-cache-init) 18PN000554: jboss-marshalling is deprecated and planned for removal 2022-04-26 16:35:05,737 INFO [org.infinispan.CONTAINER] (keycloak-cache-init) I 2022-04-26 16:35:05,893 INFO [org.infinispan.CONTAINER] (keycloak-cache-init) I 2022-04-26 16:35:05,893 INFO [org.infinispan.CONTAINER] (keycloak-cache-init) I 2020-24-26 16:35:05,973 INFO [org.infinispan.CLUSTER] (keycloak-cache-init) I 2020-24-26 16:35:05,973 INFO [org.infinispan.CLUSTER] (keycloak-cache-init) IS 2020-24-26 16:35:05,973 INFO [org.infinispan.CLUSTER] (keycloak-cache-init) IS 2020-24-26 16:35:05,971 INFO [org.infinispan.CLUSTER] (keycloak-cache-init) IS 2020-24-26 16:35:05,971 INFO [org.infinispan.CLUSTER] (keycloak-cache-init) IS 2020-24-26 16:35:06,382 INFO [org.infinispan.CLUSTER] (keycloak-cache-init) IS 2020-44-26 16:35:06,382 INFO [org.infinispan.CLUSTER] (keycloak-cache-init) IS 2020-44-26 16:35:06,382 INFO [org.infinispan.CLUSTER] (keycloak-cache-init) IS 2020-44-26 16:35:06,382 INFO [org.keycloak.cunnections.infinispan.DefaultInfini 2022-04-26 16:35:07,477 INFO [org.keycloak.cunnections.infinispan.DefaultInfini 2022-04-26 16:35:07,477 INFO [org.keycloak.cunections.infinispan.DefaultInfini 2022-04-26 16:35:07,477 INFO [org.keycloak.cunections.infinispan.DefaultInfini 2022-04-26 16:35:07,477 INFO [org.keycloak.cennections.infinispan.DefaultInfini 2022-04-26 16:35:07,477 INFO [org.keycloak.cennections.infinispan.DefaultInfini 2022-04-26 16:35:07,477 INFO [org.keycloak.cennections.infinispan.DefaultInfini 2022-04-26 16:35:07,477 INF

Рисунок 2.28 Экран успешного старта сервера КеуСloak

р Осторожно

Убедитесь, что сетевое имя хоста (keycloak в нашем примере) успешно разрешается. При необходимости добавьте запись в файл C:\Windows\System32\drivers\etc\hosts.

2.4.6 Создание начальной учетной записи администратора

Зайдите локально на <u>https://localhost:8443</u> и задайте параметры начальной учетной записи администратора – Username и Password. Затем введите подтверждение пароля (Password confirmation) и нажмите «Create».

Осторожно

Для работы с веб-консолью KeyCloak требуется установить современный веб-браузер с поддержкой HTML5 и CSS3.

Welcome to Keycloak		
Administration Console Please an Initial admin user to	User Guide, Admin REST API and	@ Keycloak Project >
get startea. Username admin Password	Javadocs	Mailing List >
Password confirmation		虃 Report an issue >
	1	Boss' JBcss Community

Рисунок 2.29 Создание начальной учетной записи администратора Keycloak

В результате выполнения должно появиться сообщение «User created».

🕼 Welcome to Keycloak 🛛 🗙 🕂		~ L		×
← → С ▲ Не защищено https://localhost	:8443	☞ ☆ [1 🗈	:
Welcome to Keycloak	Documentation >	☑ Keycloak Project >		
Centrally manage all aspects of the Keycloak server	Javadocs	Mailing List >		
		癙 Report an issue >		
AT	12/1	JRoss Community	4	

Рисунок 2.30 Сообщение об успешном создании пользователя

2.4.7 Создание клиента для системы «Зодиак»

1. Зайдите на <u>https://keycloak:8443/auth/admin</u>, введите логин и пароль учетной записи администратора и нажмите «Sign In».

🛛 Sign in to Keydbak × +	~	_	x
\leftrightarrow \rightarrow C 🔒 keycloak:8443/realms/master/protocol/openid-connect/auth?client_id=security-adm ${\bowtie}$	☆		:
KEYCLOAK			
Sign in to your account			
Username or email			
Password			
Sign In			

Рисунок 2.31 Вход в веб-консоль администрирования KeyCloak

2. В окне веб-консоли администратора нажмите «Clients».

🚳 Keycloak Admin Console 🛛 🗙	+ ~ ×				
← → C	idmin/master/console/#/realms/master 💁 🖻 😩 🗄				
	🛔 Admin 🛩				
Master 🗸	Master 👕				
Configure	General Login Keys Email Themes Localization Cache Tokens				
🚻 Realm Settings	Client Registration Client Policies Security Defenses				
Clients	* Name				
🚓 Client Scopes	master				
📰 Roles	Display name				
😅 Identity Providers	Keycloak				
User Federation	HTML Display name				
Authentication	<div class="kc-logo-text">Keycloak</div>				
Manage	Frontend URL ()				
🚈 Groups					
💄 Users	Enabled @				
 Sessions 					
🛗 Events	User-Managed Access 🚱				
🖾 Import	Orr				
Export	Endpoints @				
	OpenID Endpoint Configuration				

Рисунок 2.32 Окно веб-консоли администратора KeyCloak

3. В окне списка клиентов нажмите «Create».

🚳 Keycloak Admin Console	× +				× _	
ightarrow $ ightarrow$ $ ightarrow$ keycloak:844	13/admin/master/console/#/re	alms/maste	er/clients •	Ē	☆	
						Admin
Master ~	Clients					
	Loonop					
👫 Realm Settings	Search	Q				Create
🕤 Clients	Client ID	Enabled	Base URL	Actio	ns	
🚳 Client Scopes	account	True	https://keycloak:8443/realms/master/account/	Edit	Export	Delete
🛒 Roles	account-console	True	https://keycloak:8443/realms/master/account/	Edit	Export	Delet
Identity Providers	admin-cli	True	Not defined	Edit	Export	Delete
	broker	True	Not defined	Edit	Export	Delete
User Federation	master-realm	True	Not defined	Edit	Export	Delete
Authentication	security-admin-console	True	https://keycloak:8443/admin/master/console/	Edit	Export	Delete
Groups						
Groups						
🛓 Users						
 Sessions 						
🛗 Events						
🔄 Import						

Рисунок 2.33 Окно списка клиентов KeyCloak

4. Введите zodiac в поле Client ID и нажмите «Save».

🚳 Keycloak Admin Console 🛛 🗡	+				~		•	x
← → C 🔒 keycloak:8443/	admin/master/console/#/create/client/master		07	Ŀ	☆			:
						1 A	ldmin	>
Master 🗸 🗸	Clients > Add Client							
Configure	Add Client							
👫 Realm Settings	Import Select file 🖄							
🍞 Clients	zodiac	Client ID * 🚱						
🚳 Client Scopes	openid-connect 🗸	Client Protocol 🔞						
Roles		Root LIRI @						
		NOOL ONE O						
User Federation	Save							
Authentication								
Manage								
🐁 Groups								
💄 Users								
 Sessions 								
🛗 Events								
🖸 Import								
🖾 Export								

Рисунок 2.34 Добавление клиента KeyCloak

5. На форме клиента заполните следующие поля, затем нажмите «Save»:

🔰 Keycloak Admin Console	× +	↓ – □ ×
· → C 🔒 keycloak:8	443/admin/master/console/#/realms/master/clients/30c1c	96f-d3a9-4f8f-83ad-9d 🕶 🖻 🏠 🔲 😩 🗄
	Direct Access Grants Enabled @	,
	OAuth 2.0 Device Authorization Grant Enabled @	
	OFF	Front Channel Logout 🔞
	\${authAdminUrl}	Root URL 🕖
	* +	* Valid Redirect URIs 🕼
	/zodiac/	Base URL 🕖
		Admin URL 🕖
		Logo URL 😡
		Policy URL 😡
		Terms of service URL 😡
	* +	Web Origins 🚱
		Backchannel Logout URL 🚱
	ON	Backchannel Logout Session Required 😡
	OFF	Backchannel Logout Revoke Offline Sessions 🛿

Рисунок 2.35 Заполнение формы клиента KeyCloak

Таблица 2.1 Поля формы клиента для заполнения

Наименование поля	Значение
Root URL	\${authAdminUrl}
Valid Redirect URIs	*
Base URL	/zodiac/
Web Origins	*

6. В списке клиентов в строке клиента zodiac нажмите «Edit»

Keycloak Admin Console Section 2 Section 2	× +				~ L-	. 🗆 🔿
\leftrightarrow \rightarrow C $$ keycloak:8443,	/admin/master/console/#	/realms/maste	er/clients 💁	Ê	☆□	
						Admin Y
Master 🗸	Clients					
	Lookup 📀					
👫 Realm Settings	Search	Q				Create
🍞 Clients	Client ID	Enabled	Base URL	Actio	ns	
🙈 Client Scopes	account	True	https://keycloak:8443/realms/master/account/	Edit	Export	Delete
Roles	account-console	True	https://keycloak:8443/realms/master/account/	Edit	Export	Delete
	admin-cli	True	Not defined	Edit	Export	Delete
	broker	True	Not defined	Edit	Export	Delete
User Federation	master-realm	True	Not defined	Edit	Export	Delete
Authentication	security-admin- console	True	https://keycloak:8443/admin/master/console/	Edit	Export	Delete
	zodiac	True	https://keycloak:8443/zodiac/	Edit	Export	Delete
🛓 Groups	-					
Sessions						
Events						
🖸 Import						
Export						

Рисунок 2.36 Вызов формы редактирования клиента KeyCloak с ID=zodiac

7. На форме клиента Zodiac нажмите на пункт меню «Mappers».

🚳 Keycloak Admin Console	× +	↓ - □ ×
← → C 🔒 keycloak:8443	/admin/master/console/#/realms/master/clients/30c1c9	6f-d3a9-4f8f-83ad-9d 🕶 🖻 🏠 🚹 😩 🗄
		🛔 Admin 🗸
Master 🗸 🗸	Clients > zodiac	
Configure	Zodiac 👕	
👫 Realm Settings	Settings Keys Roles Client Scopes	Mappers O Scope O Revocation
😙 Clients	Sessions 😨 Offline Access 😨 Installation	10
🚓 Client Scopes	zodiac	Client ID 🖗
Roles		Name 😡
User Federation		Description @
Authentication	ON	Enabled 🔞
Manage	OFF	Always Display in Console 😡
🚢 Groups	OFF	Consent Required 😡
🛓 Users		Login Thome @
O Sessions	· · · · · · · · · · · · · · · · · · ·	Login meme 🗸
🛗 Events	openid-connect 🗸	Client Protocol 🔞
🛛 Import	public 🗸	Access Type @
🖸 Export	Standard Flow Enabled 🔞	

Рисунок 2.37 Переход к списку мапперов для клиента

8. В списке марреров клиента нажмите «Create».



Рисунок 2.38 Вызов формы создания маппера клиента

9. Заполните форму маппера следующим образом, затем нажмите «Save».

💿 Keycloak Admin Console 🛛 🗙 🕂			~	-		x
← → C 🔒 keycloak:8443/admin/maste	r/console/#/create/client/master/30c1c96f-d3a9-4f8f-83ad-9d03c66e3f05/mappers	ŀ	☆			:
				💄 Adm	in Y	Î
Clients → zodiac → I	Aappers > Create Protocol Mappers					
Create Prot	ocol Mapper					
Protocol @	openid-connect					
Name 😡	zodiac					
Mapper Type Ø	Audience 🗸					
Included Client Audience 😡	zodiac x v					
Included Custom Audience 😡						
Add to ID token ©	OFF					
Add to access token @	ON					
	Save					Ŧ

Рисунок 2.39 Заполнение формы создания маппера

Таблица 2.2 Поля формы маппера для заполнения

Наименование поля	Значение
Name	Zodiac

Mapper Type	Audience
Included Client Audience	zodiac

2.4.8 Настройка брандмауера Windows

Для удаленного использования сервера авторизации KeyCloak необходимо открыть порт 8433 (в нашем примере используется порт по умолчанию).

Процедура задания разрешений для порта описана в разделе 4.6

2.5 Установка сервера администрирования

Примечание

Ниже приведен пример установки под ОС Windows Server 2012 R2. Установка для других версий ОС Windows выполняется аналогично.

2.5.1 Установка распространяемых компонентов Microsoft Visual C++

Зайдите на официальный сайт <u>Microsoft Visual C++ последние поддерживаемые</u> <u>скачиваемые файлы</u>.

В разделе Visual Studio 2015, 2017, 2019 и 2022 загрузите файлы vc_redist.x86.exe и vc_redist.x64.exe.

По очереди запустите оба установщика и пройдите процесс установки.

2.5.2 Установка SSL-сертификата для доступа к веб-консоли

Для доступа к веб-консоли сервера администрирования по протоколу HTTPS в системе необходимо установить SSL-сертификат соблюдая следующие требования:

- Сертификат должен быть помещен в хранилище Локальный Компьютер > Личное
- Сертификату должны быть выдано разрешение для учетной записи Network Service

Если в вашей организации используется единый центр сертификации, произведите выпуск SSL-сертификата по принятым в вашей организации правилам для выбранного DNS-имени хоста сервера администрирования или для выбранного DNS-имени балансировщика.

В случае, если у вас уже есть сертификат в формате **PFX**, нужно выполнить его импорт, например, способом, описанным в разделе 4.1.

🔊 Совет

Для тестовых целей вы можете установить **самоподписанный** сертификат как описано для OC Windows в разделе 4.2.1.

2.5.3 Подготовка файла конфигурации

Поместите в папку C:\ProgramData\Zodiac\administration-server файл administration.ini со следующим содержимым:

```
URLS="https://192.168.1.37:3000/"
[ConnectionStrings]
ZodiacContext="Server=192.168.1.37;Port=5432;Database=zodiac;User
ID=postgres;Password=postgres;"
[Zodiac]
Cors=false
[Kestrel:EndpointDefaults]
Protocols=Http1
[Zodiac:Certificate]
Store=LocalMachine
Thumbprint=099A857875125A553B2D2CB1B51850F7792D6660
[Zodiac:WebInterface]
WebAdministrationUrl = "https://192.168.1.37:3000/"
EnableAuth = false
[Packages]
Dir = "C:\ScatterPackages"
```

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

Параметр WebAdministrationUrl также должен содержать внешний адрес, связанный с сервером (в конфигурации без балансировщика).

Параметр **Thumbprint** должен содержать отпечаток сертификата, установленного в системе, как описано в разделе 2.5.2.

Параметр ZodiacContext должен содержать строку подключения к СУБД PostgreSQL.

2.5.4 Подготовка файла конфигурации с настройкой аутентификации

Для использования системы «Зодиак» с сервером авторизации KeyCloak добавьте в файл конфигурации секцию [Zodiac:OidcConfiguration] следующим образом:

```
[Zodiac:WebInterface]
WebAdministrationUrl = "https://192.168.1.37:3000/"
EnableAuth = true
[Zodiac:OidcConfiguration]
ClientId = "zodiac"
RedirectUri = "https://192.168.1.37:3000/#/authentication/callback"
ResponseType = "code"
PostLogoutRedirectUri = "https://192.168.1.37:3000/"
Scope = "openid profile email"
Authority = "https://keycloak:8443/realms/master"
SilentRedirectUri =
"https://192.168.1.37:3000/#/authentication/silent_callback"
AutomaticSilentRenew = true
LoadUserInfo = true
AdministrationAudience = "zodiac"
```

Также задайте настройку EnableAuth = true

Осторожно

Если вы использовали **самоподписанный** сертификат при настройке сервера авторизации Keycloak (раздел 2.4.4), сделайте его доверенным на хосте, где установлен сервер администрирования как описано в разделе 4.4.

2.5.5 Запуск инсталлятора

Поместите инсталляционный MSI-пакет administration\win-x64\setup.msi из состава дистрибутива во временную папку на компьютере.

Запустите инсталлятор, нажмите кнопку «Далее», дождитесь окончания установки.



Рисунок 2.40 Запуск инсталлятора сервера администрирования

2.5.6 Настройка брандмауера Windows

Для удаленного использования веб-консоли сервера администрирования необходимо открыть порт, используемый во внешнем адресе, заданном в разделе 2.5.3 (В нашем примере используется порт 3000).

Процедура задания разрешений для порта описана в разделе 4.6.

2.6 Установка сервера коммуникации

2.6.1 Установка распространяемых компонентов Microsoft Visual C++

Примечание

Если установка сервера коммуникации осуществляется на той же машине, на которой был установлен сервер администрирования, можно перейти к пункту 2.6.3.

Зайдите на официальный сайт <u>Microsoft Visual C++ последние поддерживаемые</u> <u>скачиваемые файлы</u>.

В разделе Visual Studio 2015, 2017, 2019 и 2022 загрузите файлы vc_redist.x86.exe и vc_redist.x64.exe.

По очереди запустите оба установщика и пройдите процесс установки.

2.6.2 Установка SSL-сертификата для доступа агентов

Выполните действия по установке из раздела 2.5.2 аналогично действиям при установке сервера администрирования.

2.6.3 Подготовка файла конфигурации

Поместите в папку C:\ProgramData\Zodiac\communication-server файл communication.ini со следующим содержимым:

```
URLS="https://192.168.1.37:3001/"
[Kestrel:EndpointDefaults]
Protocols=Http1
[Zodiac:Certificate]
Store=LocalMachine
Thumbprint=099A857875125A553B2D2CB1B51850F7792D6660
[ConnectionStrings]
ZodiacContext="Server=192.168.1.41;Port=5432;Database=zodiac;User
ID=postgres;Password=postgres;"
[Store]
Dir=%ALLUSERSPROFILE%\Zodiac\communication-server\store
Log=%ALLUSERSPROFILE%\Zodiac\communication-server\store\log.txt
Port=27027
[Processing:TakeLimit]
default=100
basic inventory=100
script_stat=100
script results=100
[Packages]
Dir = "C:\ScatterPackages"
```

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 **Thumbprint** должен содержать отпечаток сертификата, полученный в разделе 2.6.2.

Параметр ZodiacContext должен содержать строку подключения к СУБД PostgreSQL.

2.6.4 Запуск инсталлятора

Поместите инсталляционный MSI-пакет communication\win-x64\setup.msi из состава дистрибутива во временную папку на компьютере.

Запустите инсталлятор, нажмите кнопку «Далее», дождитесь окончания установки.



2.6.5 Настройка брандмауера Windows

Для удаленного использования веб-арі сервера коммуникации необходимо открыть порт, используемый во внешнем адресе сервера коммуникации, заданном в разделе 2.6.3 (В нашем примере используется порт 3001).

Процедура задания разрешения для порта описана в разделе 4.6.

2.7 Установка агента

2.7.1 Запуск инсталлятора

Скопируйте файл agent\win-x64\agent.msi из состава дистрибутива системы «Зодиак» на компьютер, на который вы хотите установить агент и запустите его.


Рисунок 2.41 Окно MSI-инсталлятора агента

Нажмите кнопку «Далее», затем нажмите кнопку «Установить», затем дождитесь окончания установки. В случае корректной установки в списке служб появится служба **Zodiac.Agent** в статусе «Выполняется».

Q		Службы			>	ĸ
Файл Действие Вид	Справка					
🧇 🏟 📰 🙆 🗟						
🔍 Службы (локальные)	Имя	Описание	Состояние	Тип запуска	Вход от имени	^
	🖓 Windows Audio	Управление средствами работы		Вручную	Локальная слу	
	🔍 Windows Driver Foundation - User-mode Driver	Создает процессы драйверов по		Вручную (ак	Локальная сис	_
	Zodiac.AdministrationServer	Сервер администрирования Zo	Выполняется	Автоматиче	Сетевая служба	=
	Codiac.Agent	Агент Zodiac	Выполняется	Автоматиче	Локальная сис	П
	Codiac.CommunicationServer	Сервер коммуникаций Zodiac	Выполняется	Автоматиче	Сетевая служба	1.1
	🥋 Агент защиты сетевого доступа	Агент службы защиты доступа к		Вручную	Сетевая служба	
	🥋 Агент политики IPsec	Безопасность протокола IP (IPse	Выполняется	Вручную (ак	Сетевая служба	
	🧠 Адаптер производительности WMI	Предоставляет сведения библи		Вручную	Локальная сис	
	🖏 Брандмауэр Windows	Брандмауэр Windows помогает	Выполняется	Автоматиче	Локальная слу	

Рисунок 2.42 Служба Zodiac.Agent в списке служб Windows.

🔊 Совет

В случае возникновения критических ошибок при запуске агента, информацию об ошибках можно найти в файле C:\Program Files\Zodiac\Agent\lib\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:

```
2022-04-18T14:21:42.492Z ERROR [3472] Agent.main: error reading configuration files: StaticConfig.load: failed to load: server url missing
```

2.7.2 Конфигурирование агента

Для конфигурирования агента нужно задать как минимум адрес сервера коммуникации. С этой целью нужно создать файл C:\ProgramData\Zodiac\agent\agent.ini со следующим содержимым:

```
[Server]
url=https://192.168.1.37:3001
```

Здесь параметр **url** должен содержать адрес сервера коммуникации, сконфигурированный при его установке в разделе 2.6.3.

🔊 Совет

Установку и конфигурацию агента можно выполнить одновременно одной командой, задав нужный параметр в командной строке **msiexec**:

```
msiexec /i agent.msi
ZDC SET SERVER URL=https://192.168.1.37:3001
```

В этом случае файл C:\ProgramData\Zodiac\agent\agent.ini будет создан автоматически.

Для задания нескольких параметров:

```
msiexec /i agent.msi
ZDC_SET_SERVER_URL=https://192.168.1.37:3001
ZDC_SET_SERVER_INTERVAL=5
```

Успешная коммуникация агента с сервером отражается появлением в штатном журнале агента C:\ProgramData\Zodiac\agent\logs записей вида:

```
2022-03-30T05:13:32.658Z INFO [79998] Communicator.communicate: succeeded in 44ms
```

Также в случае успешной коммуникации агента с сервером в веб-интерфейсе сервера администрирования во вкладке «Компьютеры» появится запись с результатами базовой инвентаризации компьютера, на котором был установлен агент.



Рисунок 2.43 Экран веб-интерфейса системы с результатами базовой инвентаризации, полученной от агента

3. УСТАНОВКА СИСТЕМЫ «ЗОДИАК» ПОД УПРАВЛЕНИЕМ ОС СЕМЕЙСТВА LINUX НА ПРИМЕРЕ ОС ASTRA LINUX

3.1 Установка базовых компонентов

3.1.1 Инсталляция ОС ASTRA LINUX

Примечание

Ниже приведен пример установки ОС Astra Linux версии 1.7.3. Установка других версий ОС Astra Linux выполняется аналогично. Также необходимо обеспечить подключение официальных репозиториев из сети **интернет**.



Рисунок 3.1 Главное окно инсталлятора ОС Astra Linux

1. Примите лицензионное соглашение.

ASTRA LINUX ОПЕРАЦИОННАЯ СИСТЕМА
Лицензия
ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ
Операционная система специального назначения «Astra Linux Special Edition»
Внимание!Внимательно прочитайте нижеследужцие условия, прежде чем устанавливать, копировать или иным способом использовать операционную систему специального назначения «Astra Linux Special Edition» (далее - ПО). Установка, копирование или использование ПО иным способом означает Ваше согласие с приведенными ниже условиями без каких-либо изыятий.
Настоящее лицензионное соглашение с конечным пользователем (далее - Соглашение) заключается между Обществом с ограниченной ответственностью «РусБИТех-Астра» (далее - Компания) и Вами - кридическим лицом, и определяет порядок и условия использования Вами ПО.
Соглашение вступает в силу, когда Вы начали использовать ПО либо, если это предусмотрено функциональными возможностями ПО, с момента, когда Вы принимаете условия Соглашения, в процессе установки ПО на своем устройстве или иным, предложенным образом выражаете свое согласие на экране Вашето устройства с помощью интерфейса установки ПО.Любое из вышеуказанных действий овначает, что Вы ознакоматись с Соглаением, поняли его и приняли содержащиеся в нем условия.
Если Вы не согласны с условиями Соглавения, то Вы не имеете права устанавливать, запускать, копировать или иным способом использовать ПО.
Принимая условия Соглашения Пользователь подтверждает, что действует на добровольных началах, сознательно, без какого-либо принуждения со стороны Компании и/или третьих лиц, он правоспособен, и вправе заключать Соглашение.
Предоставление права использования ПО сопровождается отдельным договором, заключенным между Компанией или Партнером Компании и Вами. При заключении между Вами и Компанией или Партнером Компании договора, Соглашение и все его положения является неотъемпемой частью такого договора.
Термины и определения
«Компания»-Общество с ограниченной ответственностью «РусБИТех-Астра», ИН 7726388700, являющееся правообладателем семейства операционных систем специального назначения «Astra Linux Special Edition».
«Пользователь» («Вы»)- кридическое лицо, орган государственной власти или индивидуальный предприниматель, который приобреп ПО для собственного использования, а не для перепродажи или оказания услуг с понощью ПО третьим лицам.
«Програминое обеспечение» («ПО»)- семейство операционных систем специального назначения «Astra Linux Special Edition», включая все и каждый отдельный компонент (модуль), встроенный в продукты семейства, все последующие обновления такого програминого обеспечения, а также сопутствующая документация.
«Лицензия»-предоставленное Компанией право на установку,запуск и использование функциональности ПО на условиях простой (ненсключительной)лицензии в соответствии с условиями договора между Пользователем и Компанией или Партнером Компании.
«Партнер Компании»-кридическое лицо, которому Компания предоставила право распространения или иного использования ПО.
-Устройство»-физическое или виртуальное устройство, на котором Пользователь использует ПО.
1. Общие положения
Снинок экрана) Справка Продолжить

Рисунок 3.2 Страница лицензионного соглашения

- 2. Выберите способ переключения раскладки клавиатуры.
- 3. Выберите имя компьютера.

ASTRA LINUX ОПЕРАЦИОННАЯ СИСТЕМА		
Настройка сети		
Введите имя этого компьютера.		
Имя компьютера — это одно слово, которое идентифицирует вашу систему в сети. Если вы не знаете каким доляно быть имя вашей системы, то посоветуйтесь с администратором вашей сети. Если вы устанавливаете вашу собственную домашнюю сеть, можете выбрать любое имя.		
Иня контьютера:		
สงกล		
*		
Снимок экрана Справка Вернуться Продолжить		
Рисунок 3.3 Выбор имени этого компьютера		

4. Введите логин администратора и пароль от него.

ASTRA LINUX® ОПЕРАЦИОННАЯ СИСТЕМА	
Настройка учётных записей пользователей и паролей	
Выберите имя учётной записи администратора. Учётная запись должна начинаться со строчной латинской буквы, за которой может следовать любое количест цифр. Имя учётной записи администратора:	во строчных латинских букв или
₩	
Снимок экрана	Вернуться Продолжить

Рисунок 3.4 Выбор имени администратора и пароля

- 5. Выберите часовой пояс.
- 6. Разметьте диск любым удобным способом. Для разметки виртуальной машины можно оставить настройки по умолчанию.

ASTRA LINUX ОПЕРАЦИОННАЯ СИСТЕМА	
Разметка дисков	
Программа установки может провести вас через процесс разметки диска (предпагая разные стандартные схемы) на разделы, либо это можно сделать вручную. Если выбрать использование инструмента управления разметкой, у вас всё равно будет возможность позже посмотреть и подправить результат.	
Если выбрать использование инструмента управления разметкой всего диска, то дапее вас попросят указать нужный диск. <i>Метод разметки</i> :	
Авто -использовать весь диск	
Авто - использовать весь диск и настроить LVM	
Авто -использовать весь диск с защитным преобразованием на LVM	
Bpyseryw	
*	
Снимок экрана Справка Вернуться Продоли	КИТЬ

Рисунок 3.5 Разметка дисков

7. Выберите желаемую базовую систему.

	операционная система		
Установка базовой системы			
Список содержит доступные ядра В	ыберите одно из них,чтобы система могла загрузить	ся с жёсткого диска.	
Ядро для установки:			
linux-5.10-generic			
linux-5.10-hardened			
linux-5.15-generic			
linux-5.15-nardened			
linux-5.4-generic			
linux-5.4-hardened			
	*		
Снимок экрана Справка			Вернуться Продолжить

Рисунок 3.6 Выбор базовой системы

8. Выберите следующее дополнительное ПО.

	ОПЕРАЦИОННАЯ СИСТЕМА			
Выбор программного обеспечен	ия			
В данный момент установлена топы Выберите устанавливаемое програм	ко основа системы.Исходя из ваших потребност «мное обеспечение:	гей,можете выбрать один и более из п	готовых наборов программного обесп	ечения.
Графический интерфейс Fly				
🗹 Средства работы с Интернет				
Офисные приложения				
🗌 Средства работы с графикой				
Средства мультимедиа				
Средства Виртуализации				
🗆 Игры				
🗹 Консольные утилиты				
Средства фильтрации сетевых п	акетов ufw			
Расширенные средства для рабо	ты с сенсорным экраном			
Средства удаленного подключен	ия SSH			
Снимок экрана Справка				Продолжить
			•	

Рисунок 3.7 Выбор дополнительного ПО

9. Выберите уровень защищенности.

ASTRA LINUX ОПЕРАЦИОННАЯ СИСТЕМА			
Дополнительные настройки ОС			
Выберите уровень защищенности в зависимости от приобретенной	лицензии:		
Максимальный уровень защищенности "Смоленск"			
Усиленный уровень защищенности "Воронеж" Базовый уровень защищенности "Орел"			
and the second second contraction of the			
Снимок экрана Справка			Продолжить

Рисунок 3.8 Выбор уровня защищенности

10. Выберите следующие дополнительные настройки ОС.

ASTRA LINUX® ОПЕРАЦИОННАЯ СИСТЕМА	
Дополнительные настройки ОС	
Вы можете настроить параметры безопасности ОС в зависимости от выбранного режима работы, с Дополнительные настройки ОС	тключить автоматическую настройку сети и настроить системные часы.
🗌 Запрет вывода меню загрузчика	
Запрет трассировки ptrace	
Запрос пароля для команды sudo	
Запрет установки бита исполнения	
Запрет исполнения скриптов пользователя	
Запрет исполнения макросов пользователя	
Запрет консоли	
Cистемные ограничения ulimits	
Запрет автонастройки сети	
Местное время для системных часов	
Снимок экрана Справка	Продолжить

Рисунок 3.9 Выбор дополнительных настроек ОС

11. Установите GRUB.

Установка системного загрузчика GRUB на жёсткий диск	
Системный загрузчик GRUBпредоставляет возможности, которые могут быть использованы для н настройкам GRUB. Dля защиты от этого необходимо задать пароль, который будет запрашиватьс: номает быть настроен запрос пароля при выборе пунктов мене для загрузки системы. По умолча системы.	есанкционированного доступа к системе,если неавторизованный пользователь получит доступ к я при редактировании меню GRUBи при входе в режим командной строки GRUB Дополнителью нию любой пользователь может выбрать без ввода пароля любой пункт меню GRUBдля загрузки
Введите пароль для GRUB.	
Паропь для GRUB:	
🗌 Показывать вводимый пароль	
Снимок экрана Справка	Вернуться Продолжить
•	
Dual way 2 10 V	COUD

Рисунок 3.10 Установка GRUB

- 12. Завершите установку и зайдите на компьютер.
- 13. Настройте сетевые подключения согласно <u>статье</u> через редактирование конфигурационных файлов

```
sudo nano /etc/network/interfaces
sudo nano /etc/hosts
sudo nano /etc/resolv.conf
```

14. Для установки СУБД и других компонентов подключите <u>базовый и расширенный</u> <u>репозитории Astra Linux</u> или используйте собственный репозиторий, предварительно загрузив в него соответствующие версии дистрибутивов. Установку расширенного репозитория можно выполнить раскомментировав строки в /etc/apt/sources.list и выполнив команду

```
sudo astra-ce <u>https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-</u>
extended/
sudo apt update
```

3.1.2 Установка SSL-сертификата для доступа к веб-интерфейсу

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

Распакуйте архив, выполнив следующую команду:

unzip certtool.zip

Задайте разрешение на исполнение файла Zodiac.CertificateTool:

chmod 755 Zodiac.CertificateTool

Разместите pfx-сертификат на сервере, например, **test.pfx** в папке /var/cert, и выполните следующую команду:

./Zodiac.CertificateTool add ../cert/test.pfx

🔊 Совет

Для тестовой инсталляции можно сделать сертификат подписанный УЦ по инструкции в разделе <u>4.5</u> (рекомендовано) или самоподписанный сертификат по инструкции, приведенной в разделе 4.3.3

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

```
[root@zdc-srv certtool]# ./Zodiac.CertificateTool add ../cert/test.pfx
Enter password: *****
Adding certificate... OK
Successfully added certificate to store.
Thumbprint: D4666758C400513A3398DFF36A58FE185DBAB545
```

Рисунок 3.11 Добавление SSL-сертификата

🔊 Совет

Скопируйте Thumbprint в удобное место для дальнейшего использования в файлах конфигурации системы «Зодиак».

3.1.3 Подготовка СУБД

- 1. Установите СУБД PostgreSQL 14 в соответствии с руководством <u>"Установка и развертывание СУБД PostgreSQL"</u>
- sudo apt install postgresql-14

```
2. Создайте базу данных zodiac
su - postgres
psql -c "CREATE DATABASE zodiac OWNER postgres ENCODING 'UTF8'
LC_COLLATE 'ru_RU.UTF-8' LC_CTYPE = 'ru_RU.UTF-8'
TEMPLATE='template0';"
3. Задайте пароль пользователю postgres
sudo -u postgres psql postgres
```

\password

Совет

При установке postgresql может потребовать правка hba.conf, разрешая доступы с удаленных хостов к postgresql. При наличии проблем с доступом необходимо добавить в hba.conf следующие параметры

```
listen addresses = '*'
host all all 0.0.0/0 md5.
```

Путь hba.conf зависит OC к ОТ и версии postgres, например, /etc/postgresql/14/main/pg_hba.conf или может быть получен командой

sudo -u postgres psql postgres -c "SHOW hba file;

4. 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

3.2 Установка keycloak

Keycloak может быть установлен как на машину, на которой планируется установка серверов администрирования и коммуникации zodiac, так и на отдельную. Возможно использование более новых версий keycloak, создание клиента в которых может происходить с незначительными изменениями.

1. Установите JDK

sudo apt -y install openjdk-11-jdk



🚫 Совет

При установке на другую ОС семейства Linux, команда установки open jdk может быть другая, установите open jdk 11 согласно инструкции на вашу ОС.

2. Создайте директорию для установки keycloak

sudo mkdir -p /opt/keycloak

3. Скачайте дистрибутив keycloak 12.04 и распакуйте его в данную директорию wget

https://github.com/keycloak/keycloak/releases/download/12.0.4/keycloak -12.0.4.tar.gz

```
sudo tar --strip-components 1 -xf keycloak-12.0.4.tar.gz -C
/opt/keycloak
```

4. Задайте параметры учетной записи администратора Keycloak, указав желаемый пароль вместо \$keycloakPwd. Этот пароль будет использоваться для дальнейшего входу в УЗ администратора keycloak

```
/opt/keycloak/bin/add-user-keycloak.sh -r master -u admin -p
$keycloakPwd || true
```

5. Создайте хранилище сертификата zodiac.keystore для Keycloak, например командой /usr/lib/jvm/java-11-openjdk-amd64/bin/keytool -importkeystore srckeystore \$certPfx -srcstoretype pkcs12 -destkeystore ./zodiac.keystore -deststoretype JKS -srcstorepass \$keycloakCertPwd deststorepass **\$keycloakKeyPwd** -alias "1" -destalias zodiac

Параметр certPfx должен содержать путь к .pfx файлу

Параметр keycloakCertPwd должен содержать пароль от сертификата

Придумайте keycloakKeyPwd в качестве пароля к хранилищу

Параметр alias должен содержать alias сертификата, предоставленного УЦ. По умолчанию равен 1.



🚫 Совет

В случае использования самоподписанного сертификата, используйте пароль, полученный в п. <u>4.3.3</u>.

При использовании другой ОС семейства Linux используйте соответствующий путь к keytool.

6. Скопируйте zodiac.keystore в одну папку С /opt/keycloak/standalone/configuration/standalone.xml: cp ./zodiac.keystore

/opt/keycloak/standalone/configuration/zodiac.keystore

7. Измените секцию server-identities в файле /opt/keycloak/standalone/configuration/standalone.xml

sudo nano /opt/keycloak/standalone/configuration/standalone.xml

```
<server-identities>
  <ssl>
    <keystore path="zodiac.keystore" relative-
to="jboss.server.config.dir" keystore-password="$keycloakKeyPwd"
alias="zodiac" key-password="$keycloakCertPwd" />
  </ssl>
</server-identities>
```

Параметр keycloakCertPwd должен содержать пароль от сертификата

Параметр keycloakKeyPwd должен содержать пароль от хранилища, придуманный ранее

8. Создайте файл keycloak.service в /etc/systemd/system/ со следующими параметрами, указав название компьютера, на котором установлен keycloak, вместо \$ServerName

```
sudo nano /etc/systemd/system/keycloak.service
```

```
[Unit]
Description=Keycloak Server
After=syslog.target network.target
Before=httpd.service
[Service]
SuccessExitStatus=0 143
ExecStart=/opt/keycloak/bin/standalone.sh -b $ServerName
[Install]
WantedBy=multi-user.target
```

Параметр ServerName должен содержать имя ПК

9.	Выполните запуск сервиса
sudo	systemctl daemon-reload
sudo	systemctl enable keycloak
sudo	systemctl restart keycloak
10	. Проверьте его статус
sudo	systemctl status keycloak
<pre>root@astra keycloak Loaded: Active: Main PID: Tasks: Memory: CGroup: </pre>	a-test-3:/etc/systemd/system# systemctl status keycloak.service <.service - Keycloak Server : loaded (/etc/systemd/system/keycloak.service; enabled; vendor preset: enabled) : active (running) since Tue 2023-06-20 09:15:57 MSK; 14s ago : 21863 (standalone.sh) : 125 (limit: 2300) : 541.4M : /system.slice/keycloak.service -21863 /bin/sh /opt/keycloak/bin/standalone.sh -b astra-test-3 -21950 java -D[Standalone] -server -Xms64m -Xmx512m -XX:MetaspaceSize=256m -Djava.net.preferIPv4Stack=true

Рисунок 3.12 Проверка статуса службы keycloak

11. Зайдите в UI keycloak через браузер, по умолчанию keycloak использует порт 8443

Welcome to Keycloak

Centrally manage all aspects of the Keycloak server	Documentation > User Guide, Admin REST API and Javadocs	Keycloak Project >
		☑ Mailing List >
		渝 Report an issue >

Рисунок 3.13 Экран главной страницы keycloak

12. Выполните создание клиента keycloak аналогично п. 2.4.3

3.3 Установка guacamole

При самостоятельной сборке guacamole для использования в ОС семейства Linux, отличной от Astra Linux, версия guacamole должна быть не менее 1.4. В других ОС семейства Linux, могут устанавливаться другие зависимости, следуйте инструкциям по установке Guacamole для вашей ОС.

```
1. Установите зависимости
```

```
apt install libcairo2 libjpeg62-turbo libssh2-1 libfreerdp-client2-2
libfreerdp-shadow-subsystem2-2 libpng-tools libavcodec58 libavformat58
libavutil56 libswscale5 libpango1.0 libvncserver1 libvncclient1
libvorbisenc2 libwebpdemux2 libwebpmux3 libpulse0
```

2. Распакуйте архив с guacamole в папку usr

```
tar -xvf ./gbin.tar.gz -C /usr
   Выполните команды для применения предыдущих действий
ldconfig
systemctl daemon-reload
   Создайте файл guacd.conf в директории /etc/guacamole
mkdir /etc/guacamole
sudo nano /etc/guacamole/guacd.conf
   5. Поместите в него следующие параметры
[server]
bind host=0.0.0.0
   Включите сервис guacd
sudo systemctl enable guacd
sudo systemctl restart guacd
   7. Проверьте его статус
systemctl status guacd.service
root@astra-test-3:~# systemctl status guacd.service
💿 guacd.service - Guacamole Server
   Loaded: loaded (/lib/systemd/system/guacd.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-06-20 08:08:50 MSK; 3s ago
     Docs: man:quacd(8)
 Main PID: 29066 (guard)
    Tasks: 1 (limit: 2300)
   Memory: 11.8M
   CGroup: /system.slice/guacd.service

-29066 /usr/sbin/guacd -f
```

Рисунок 3.14 Проверка статуса службы Guacamole

3.4 Установка сервера администрирования

3.4.1 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://astra-test-2:443/"
```

```
[Kestrel:EndpointDefaults]
Protocols=Http1
[Certificate]
Store=CurrentUser
Thumbprint=EA03203E3A251752DDF25403F7C151D3130AC432
[WebInterface]
WebAdministrationUrl = "https://astra-test-2:443/"
Authenticate = true
ShowPii = true
```

```
[Roles]
Enabled = false
[ConnectionStrings]
ZodiacContext="Server=127.0.0.1;Port=5432;Database=zodiac;UserID=postg
res;Password=postgres;"
[Packages]
Dir = "/var/scatter-packages"
[Guacamole]
DefaultGuacd = "astra-test-2:4822"
[OTA]
AgentDir = "/var/updates"
TempDir = "/var/updates temp"
[Audit]
LogFileOn = true
LogFile = "./../audit/audit.log"
LogFilesLimit = 300
SyslogOn = false
SyslogPath = "/dev/log"
SyslogTransport = UnixSocket
[OidcConfiguration]
ClientId = "zodiac"
RedirectUri = "https://astra-test-2:443/#/authentication/callback"
ResponseType = "code"
PostLogoutRedirectUri = "https://astra-test-2:443/"
Scope = "openid profile email"
Authority = "https://astra-test-2:8443/auth/realms/master"
SilentRedirectUri = "https://astra-test-
2:443/portal/silent callback.html"
AutomaticSilentRenew = true
LoadUserInfo = true
AdministrationAudience = "zodiac"
```

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

Параметр WebAdministrationUrl также должен содержать внешний адрес, связанный с сервером (в конфигурации без балансировщика).

Параметр **Thumbprint** должен содержать отпечаток сертификата, полученный в разделе 2.5.1.

Параметр ZodiacContext должен содержать строку подключения к СУБД PostgreSQL.

Параметр **DefaultGuacd** должен содержать строку подключения к Guacamole.

Параметры RedirectUri, PostLogoutRedirectUri, SilentRedirectUri также должны содержать внешний адрес, связанный с сервером (в конфигурации без балансировщика).

Параметр Authority должен содержать строку подключения к используемому Realm Keycloak. Если используется keycloak версии, отличной от 12, в строке подключения может не быть /auth, необходимость /auth в пути можно увидеть, посмотрев главную страницу web UI keycloak

В случае использования cleint secret open-id провайдером в секции OidcConfiguration следует создать параметр ClientSecret с соответствующим значением.

Осторожно

Если вы использовали самоподписанный сертификат или СА-сертификат при настройке сервера авторизации Keycloak (раздел <u>3.2</u>), сделайте его доверенным на хосте, где установлен сервер администрирования как описано в разделе 4.6.

3.4.2 Создание служебных директорий

Создайте каталог /var/updates

Создайте каталог /var/updates_temp

Создайте каталог /var/scatter-packages

```
mkdir /var/updates
mkdir /var/updates temp
mkdir /var/scatter-packages
```

3.4.3 Установка DEB-пакета

Скопируйте файл zodiac.administration.server.deb из состава дистрибутива на сервер, и выполните следующую команду:

apt install ./zodiac.administration.server.deb

Корректность установки можно проверить выполнив команду

systemctl status zodiac.administration.server.service

В случае корректной установки будет выдано следующее сообщение:



Рисунок 3.15 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 3.16 Экран веб-интерфейса системы «Зодиак»

🔊 Совет

В случае возникновения проблем при установке обратитесь к разделу <u>4.8</u>, где приведены рекомендации по устранению возможных ошибок при установке системы «Зодиак» под ОС семейства Linux.

3.4.4 Задание ролевой модели (опционально).

Для включения ролевой модели для разграничения доступа к системе «Зодиак» между различными пользователями, измените /var/zodiac/administration-server/administration.ini

nano /var/zodiac/administration-server/administration.ini

В разделе [Roles] укажите следующую информацию

```
[Roles]
Enabled = true
SaExprs = "$.resource_access.zodiac.roles[?(@ == 'zodiac_ac_sa')];$.ro
les[?(@ == 'zodiac_ac_sa')]"
RaExprs = "$.resource_access.zodiac.roles[?(@ == 'zodiac_ac_ra')];$.ro
les[?(@ == 'zodiac_ac_ra')]
```

Измените zodiac_ac_sa на роль для суперпользователя системы «Зодиак» (может управлять всем функционалом).

Измените zodiac_ac_ra на роль для администратора ролей системы «Зодиак» (может управлять ролями).

Данные роли и соответствующие им пользователи должны быть настроены в keycloak или другом используемом SSO-провайдере.

Настройка других ролей производится в веб-интерфейсе системы «Зодиак» и описана в руководстве по администрированию.

3.5 Установка сервера коммуникации

3.5.1 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://astra-test:3001/"
[Certificate]
Store=CurrentUser
Thumbprint=D4666758C400513A3398DFF36A58FE185DBAB545
[ConnectionStrings]
ZodiacContext="Server=127.0.0.1;Port=5432;Database=zodiac;UserID=po
stgres;Password=postgres;"
[Processing:TakeLimit]
default=100
basic inventory=100
script stat=100
script results=100
[Packages]
Dir = "/var/scatter-packages"
[OTA]
AgentDir = "/var/updates"
```

Параметр **Thumbprint** должен содержать отпечаток сертификата, полученный в разделе 2.5.1.

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.

3.5.2 Создание служебных директорий

Создайте каталог /var/updates

Создайте каталог /var/scatter-packages

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

3.5.3 Установка DEB-пакета

Скопируйте файл zodiac.communication.server.deb из состава дистрибутива на сервер, и выполните следующую команду:

apt install ./zodiac.communication.server.deb

Корректность установки можно проверить выполнить 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.com	nunication.server.service - Zodiac Communication Server
Loaded:	<pre>loaded (/opt/zodiac/communication-server/zodiac.communication.server.service; enabled; vendor preset: disabled)</pre>
Active:	active (running) since Tue 2022-03-29 11:08:29 UTC; 2min 12s ago
Main PID:	16545 (Zodiac.Čommunic)
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/mongoddbpath /var/zodiac/communication-server/store/logpath /var/z

Рисунок 3.17 Проверка статуса службы сервера коммуникации

3.5.4 Монтирование директории распространяемых пакетов (опционально)

При использовании сервера администрирования и сервера коммуникации на разных ПК, необходимо примонтировать папку /var/scatter-packages с сервера администрирования на сервер коммуникации или использовать общую папку, примонтировав ее к обоим ПК. Подробнее о монтировании папок в Astra Linux можно почитать <u>здесь</u>.

3.6 Установка агента

3.6.1 Установка DEB-пакета агента

Скопируйте файл zodiac.agent.linux.deb из состава дистрибутива системы «Зодиак», и выполните следующую команду:

apt install ./zodiac.agent.linux.deb

Корректность установки можно проверить выполнить 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 3.18 Проверка статуса службы агента



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
```

3.6.2 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 установке в пункте Error! Reference source not found.. После этого перезагрузите агент командой

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

🔊 Совет

Установку агента можно выполнить одной командой, задав нужный параметр конфигурации в переменной окружения сессии:

```
env ZDC_SET_SERVER_URL=https://192.168.1.33:3001 apt install
./zodiac.agent.linux.deb
```

В этом случае файл /var/zodiac/agent/agent.ini будет создан автоматически.

Для задания нескольких параметров:

```
env ZDC_SET_SERVER_URL=https://192.168.1.45:3001 env
ZDC SET SERVER INTERVAL=5 apt install ./zodiac.agent.linux.deb
```

В случае работы не из-под root нужно использовать команду sudo с параметром -E.:

```
env ZDC_SET_SERVER_URL=https://192.168.1.45:3001 sudo -E apt
install ./zodiac.agent.linux.deb
```

Успешная коммуникация агента с сервером отражается появлением в штатном журнале areнта /var/zodiac/agent/log/agent.log записей вида:

2022-03-30T05:13:32.658Z INFO [79998] Communicator.communicate: succeeded in 44ms

Также в случае успешной коммуникации агента с сервером в веб-интерфейсе сервера администрирования во вкладке «Компьютеры» появится запись с результатами базовой инвентаризации компьютера, на котором был установлен агент.

3.6.3 Конфигурирование агента как точки обслуживания (опционально)

Для конфигурирования агента как точки обслуживания, в файл его конфигурации по адресу /var/zodiac/agent/agent.ini нужно добавить следующие строки:

```
[ServicePoint]
enabled = true
```

После чего перезагрузить агент командой

systemctl restart zodiac-agent.service

Для проверки, что агент является точкой обслуживания можно зайти в UI зодиака, выбрать вкладку «компьютеры» и в разделе «столбцы» включить столбец «ПТО». После прохождения следующей инвентаризации, в столбце появится соответствующая информация.

E	Фильтр 📄 Группировка	💽 Столбцы 📲 Экспорт	С Обновить
	Компьютер	IP	ПТО
۵	ASTRA-TEST-1	192.168.116.175	\checkmark
۵	ASTRA-TEST-4	192.168.116.178	

Рисунок 3.19 Проверка точки обслуживания

4. ПРИЛОЖЕНИЯ

4.1 Импорт имеющегося SSL-сертификата в формате PFX

1. Запустите консоль «Сертификаты – локальный компьютер» certim.msc.

	Выполнить	x
	Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.	
Открыть:	certim.msc 💱 Это задание будет создано с правами администратора	~
	ОК Отмена Обзор.	

Рисунок 4.1 Запуск консоли «Сертификаты – локальный компьютер»

2. В панели слева на узле «Личное» вызовите контекстное меню. Далее, вызовите подменю «Все задачи». Нажмите пункт меню «Импорт».

🚡 certim - [Ce	ртификаты –	— локальный компьютер	\Личное]	_	x
Файл Действие Вид Справка < 🔿 🖄 📰 🖺 🐼 🛃 🗊					
Сартификаты — локальный компьютер Сартификаты — локальный компьютер Сартификатов р ☐ довере Поиск сертификатов		Нет элемен	тов для отображения в этом виде.		
р Довери р Проме р Довере р Сертиф р Сертиф р Сторон р Пороне р Сорон р Сорон р Пороне р Сертифовать список	Поиск сер Запросит Импорт Дополнит	ртификатов ть новый сертификат С			
 № Постав Справка № Удаленный рабочий стол № Доверенные корневые сертификаты смарт-кар № Доверенные устройства 	ти клиентов		1		
Перечень действий, которые могут быть выполнены с	данным элемен	том.			

Рисунок 4.2 Вызов мастера импорта сертификатов

3. Далее, в мастере импорта сертификатов нажмите «Обзор».

	x
📀 🐓 Мастер импорта сертификатов	
Импортируемый файл	
Укажите файл, который вы хотите импортировать.	
	—
Имя файла:	
Обзор	
Замечание: следующие форматы файлов могут содержать более одного сертификата в одном файле:	
Файл обмена личной информацией - PKCS #12 (.PFX,.P12)	
Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)	
Хранилище сериализованных сертификатов (.SST)	
Далее Отмен	a

Рисунок 4.3 Диалога выбора файла сертификата

4. Далее, выберите файл сертификата.

	Откр	ытие		x
🔄 🔄 🔻 🛉 📕 « Л	окальный диск 🕨 temp	~ ¢	Поиск: temp	Q
Упорядочиты 🗸 Созда	ть папку		:== :==	- 🔟 🔞
쑦 Избранное	Имя		Дата изменения	Тип
〕 Загрузки	🏂 test.pfx		06.04.2022 0:51	Файл обм
Недавние места Рабочий стол				
🌉 Этот компьютер				
🗣 Сеть				
	<	Ш		>
Имя	файла: test.pfx	×	Файлы обмена личної Открыть (й инфор 👻 Отмена

Рисунок 4.4 Диалог выбора файла сертификата

5. Введите пароль закрытого ключа импортируемого сертификата.

x
📀 🍠 Мастер импорта сертификатов
Защита с помощью закрытого ключа
Для обеспечения безопасности закрытый ключ защищен паролем.
Введите пароль для закрытого ключа.
Пароль:
1
Показывать пароль
Параметры импорта:
Включить усиленную защиту закрытого ключа. В этом случае при каждом использовании закрытого ключа приложением будет запрашиваться разрешение.
Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его.
✓ Включить все расширенные свойства.
Далее Отмена

Рисунок 4.5 Окно параметров импорта

6. Убедитесь, что для импорта выбрано хранилище сертификатов «Личное» и нажмите «Далее».

×
📀 🝠 Мастер импорта сертификатов 💦
Хранилище сертификатов
Хранилища сертификатов - это системные области, в которых хранятся сертификаты.
Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.
О Автоматически выбрать хранилище на основе типа сертификата
Поместить все сертификаты в следующее хранилище
Хранилище сертификатов:
Личное Обзор
Далее Отмена

Рисунок 4.6 Выбор хранилища сертификатов

7. При удачном импорте сертификата отобразится диалог с соответствующим сообщением. Нажмите «ОК».



Рисунок 4.7 Сообщение об успешном импорте сертификата

8. Далее, в списке сертификатов выберите на созданном сертификате пункт контекстного меню «Все задачи > Управление закрытыми ключами…»

🧧 certim - [Cep	ги <mark>д</mark> икаты — ло	жальный компьюте	р\Личное\Сертифи	каты]	- 🗆 X
CertIm - [Сер Файл Действие Вид Справка Файл Доверительные отношения в предприятии Доверительные отношения в предприятии Доверительные сотношения в предприятии Доверитины цантры сертификации Доверенные издатели Сертификаты к которым нет доверия Доверенные издатели Доверенные издате	Кому выдан [®]	Кем выдан test.zodiac.ru Открыть Все задачи • Вырезать Копировать Удалить Свойства Справка	р\Личное\Сертифи Срок действия 12.04.2023 Открыть Запросить сертифика Обновить сертифика Управление закрыты Дополнительные опи Экспорт	каты] Назначения Проверка подлинности к ат с новым ключом т с новым ключом ми ключами грации	Ил лиента, П < †
< <u> </u>	4				
Перечень действий, которые могут быть выполнень	с данным элемен	том.			

Рисунок 4.8 Вызов окна настройки разрешений

8. Далее, добавьте разрешения для учетной записи **NETWORK SERVICE**.

Paspeшeния для группы " <heт> priva</heт>	ate ke X	покалы	ный компьютер\.	Личное\Сертифи	каты]			x
безопасность		-I-						
[руппы или пользователи:			Кем выдан	Срок действия	Назначения			N
🚨 СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ			test.zodiac.ru	12.04.2023	Проверка подлинности	клиент	а, П	<+
№ СИСТЕМА	торы) ⊻далить							
Разрешения для группы "СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ"	Выбор: "По	ользова	атели" или "Групг	ты" 🔽				
Чтение Выберите тип об	бъекта:							
Особые разрешения "Пользователи	", "Группы" или "	Встроенны	ые субъекты безопасн	Типы объектов				
В следующем м	есте:							
ZDC-SRV-W12				Размещение				
Чтобы задать особые разреше параметры, нажиите кнопку "Дополнительно".	выбираемых объ RVICE	ектов (<u>при</u>	імеры):	Проверить имена				
ОК								
Дополнительн	10		O	КОтмена				>

Рисунок 4.9 Добавление прав для учетной записи NETWORK SERVICE

4.2 Генерация самоподписанного SSL-сертификата под OC Windows

4.2.1 Использование PowerShell

В современных версиях Windows, начиная с Windows 8.1 и Windows Server 2012 R2, вы можете создать **самоподписанный** сертификат с помощью **PowerShell** без установки дополнительных утилит.

Чтобы создать новый SSL-сертификат типа SSLServerAuthentication (по умолчанию) для DNS имени, например, test.zodiac.ru (указывается FQDN имя) и поместить его в список персональных сертификатов компьютера, выполните команду:

```
New-SelfSignedCertificate -DnsName test.zodiac.ru -CertStoreLocation cert:\LocalMachine\My
```

Осторожно

Длительность выполнения данной команды может достигать 30 и более секунд.

В результате выполнения команды на экран будет выведен **отпечаток (thumbprint),** который следует **сохранить** для использования в конфигурационных файлах системы «Зодиак»

Далее, запустите консоль certlm.msc, и выберите на созданном сертификате пункт контекстного меню «Управление закрытыми ключами...»

Рисунок 4.10 Вызов окна настройки разрешений

Далее, добавьте права для учетной записи **NETWORK SERVICE**.

Разрешения для группы "<Нет> private ke	K IOK	альный компьютер\Ли	ичное\Сертифи	каты] 📃 🗖	x
Безопасность		<u>_</u>			
руппы или пользователи:		Кем выдан	Срок действия	Назначения	N
💐 СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ	4	test.zodiac.ru	12.04.2023	Проверка подлинности клиента, П	<+
СИСТЕМА Администраторы (ZDC-SRV-W12-Администраторы) Добавить					
Разрешения для группы "СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ" Выбор:	"Польз	зователи" или "Группь	ı" ×		
Полный доступ Выберите тип объекта:					
Чтение Высорите нип об вскта. Особые разрешения "Пользователи", "Группы" и	ли "Встр	оенные субъекты безопасно	Типы объектов		
В следующем месте: ZDC-SRV-W12			Размещение		
Чтобы задать сосбые разреше параметры, нажмите кнопку "Дополнительно". <u>NETWORK SERVICE</u>	объектов	в (примеры):	Проверить имена		
ОК Дополнительно		ОК	Отмена	at the second se	>

Рисунок 4.11 Добавление прав для учетной записи NETWORK SERVICE

4.2.2 Использование OpenSSL

Единственным способом безопасной установки OpenSSL под OC Windows является установка <u>Git for Windows</u> и использование исполняемого файла **openssl.exe**, входящего в его состав.

Использование **openssl.exe** в составе Git for Windows аналогично использованию под OC Linux, описанному в разделе 4.3.

Если **openssl.exe** установлен в папку "c:\Program Files\Git\mingw64\bin", то команда, описанная, например, в разделе 4.3.2, может быть выполнена следующим образом:

```
"c:\Program Files\Git\mingw64\bin\openssl.exe" req -x509 -newkey
rsa:4096 -sha256 -days 365 -subj "/CN=zodiac" -addext
"subjectAltName = DNS:zodiac" -keyout key.pem -out cert.pem
```

4.3 Генерация самоподписанного SSL-сертификата под OC Linux

Самоподписанные сертификаты рекомендуется использовать в тестовых целях или для обеспечения сертификатами внутренних интранет служб в тех случаях, когда по какой-то причине приобретение сертификата у внешнего провайдера или разворачивание инфраструктуры PKI/CA невозможны.

4.3.1 Установка OpenSSL

Проверьте, установлен ли пакет OpenSSL выполнив команду:

```
rpm -q openssl
```

При наличии установленного пакета OpenSSL будет выведено сообщение, содержащее версию пакета:

[root@zdc-srv /]# rpm -q openssl
openssl-1.1.1k-alt1.x86_64

Рисунок 4.12 Сообщение при наличии пакета OpenSSL

В случае отсутствия пакета OpenSSL, следует установить его командой:

apt-get install openssl

4.3.2 Генерация сертификата и зашифрованного закрытого ключа

Перейдите во временный каталог, например, /var/cert и выполните команду:

```
openssl req -x509 -newkey rsa:4096 -sha256 -days 365 -subj
"/CN=zodiac" -addext "subjectAltName = DNS:zodiac" -keyout
key.encrypted.pem -out cert.pem
```

Во время выполнения команды будет запрошено задание РЕМ-пароля с подтверждением для шифрования закрытого ключа.

В результате работы данной команды в текущем каталоге будут сгенерированы два файла: файл сертификата cert.pem, и файл зашифрованного закрытого ключа key.encrypted.pem для субъекта zodiac. Сертификат будет действителен 365 дней.

🔊 Совет

Чтобы изменить название субъекта, для которого создается сертификат, измените значение параметров subj и subjectAltName.

4.3.3 Генерация сертификата в формате PFX

Для создания **pfx-файла** используйте файлы **cert.pem** и **key.encrypted.pem**, полученные в результате выполнения команды, приведенной в разделе 4.3.2 и затем выполните следующую команду:

```
openssl pkcs12 -export -out test.pfx -inkey key.encrypted.pem -in
cert.pem
```

Во время выполнения команды нужно будет ввести РЕМ-пароль, который был задан при создании закрытого ключа **key.encrypted.pem**, а также будет запрошено задание Exportпароля с подтверждением.

В результате будет сгенерирован файл сертификата **test.pfx**, который может быть использован для тестовой инсталляции системы «Зодиак».

4.3.4 Конвертация сертификата из формата PFX в формат PEM

Для экспорта открытой части сертификата test.pfx выполните следующую команду:

openssl pkcs12 -in test.pfx -clcerts -nokeys -out cert.pem

В результате выполнения команды будет создан файл cert.pem, содержащий открытую часть сертификата в формате PEM.

Для экспорта закрытого ключа сертификата test.pfx выполните следующую команду:

openssl pkcs12 -in test.pfx -nocerts -out key.encrypted.pem

Во время выполнения команды нужно будет ввести Import-пароль, который был задан для защиты файла **test.pfx** при его создании, а также будет запрошено задание нового PEMпароля с подтверждением для шифрования экспортируемого закрытого ключа.

В результате выполнения команды будет создан файл key.encrypted.pem, содержащий зашифрованный закрытый ключ сертификата в формате PEM.

openssl pkcs12 -in test.pfx -nocerts -out key.encrypted.pem

🔊 Совет

Закрытый ключ сертификата с парольной защитой не всегда возможно или удобно использовать. Например, при подготовке конфигурационного файла KeyCloak предполагается использование незашифрованного закрытого ключа. Обойти проблему можно, сняв пароль с закрытого ключа:

openssl rsa -in key.encrypted.pem -out key.pem

Здесь, key.encrypted.pem – файл с зашифрованным закрытым ключом, key.pem – имя выходного файла с незашифрованным закрытым ключом без парольной защиты.

4.3.5 Генерация сертификата и незашифрованного закрытого ключа

Перейдите во временный каталог, например, /var/cert и выполните команду аналогично как описано в разделе 4.3.2 с добавлением параметра –nodes (сокращение от no DES) :

```
openssl req -x509 -newkey rsa:4096 -sha256 -days 365 -subj
"/CN=keycloak" -addext "subjectAltName = DNS: keycloak " -keyout
key.pem -out cert.pem -nodes
```

В результате работы данной команды в текущем каталоге будут сгенерированы два файла: файл сертификата cert.pem, и файл незашифрованного закрытого ключа key.pem для субъекта keycloak. Сертификат будет действителен 365 дней.

4.4 Генерация подписанного УЦ сертификата под ОС Linux

В тестовых целях можно произвести генерацию подписанного УЦ сертификата, в которой УЦ будет выступать сам пользователь.

4.4.1 Создание СА-сертификата

Создайте сертификат следующей командой

```
openssl req -nodes -x509 -days 1825 -newkey rsa:4096 -keyout zdc ca cert.key -out zdc ca cert.crt -subj "/CN=$CN NAME"
```

В параметре CN_NAME укажите произвольное имя удостоверяющего центра.

4.4.2 Создание запроса подписи

Создайте запрос подписи (CSR)

```
openssl req -nodes -new -newkey rsa:4096 -keyout zdc_serv_cert.key -
out zdc_cert_req.csr -subj "/CN=$HOSTNAME" -addext
"subjectAltName=DNS:$HOSTNAME,IP:$HOSTIP"
```

В HOSTNAME укажите имя хоста на котором будет установлен Зодиак.

В HOSTIP укажите IP хоста на котором будет установлен Зодиак.

В случае изготовления сертификата для нескольких хостов в subjectAltName следует указать все DNS и/или IP серверов, которые сертификат будет разрешать использовать, включая указанный в -subj.

4.4.3 Создание временного файла

Создайте временный файл для хранения altname, включив в него все subjectAltName, указанные в предыдущем пункте

printf "subjectAltName=DNS:\$HOSTNAME, IP:\$HOSTIP" | tee ext-file.conf

На основе СА-сертификата создайте сертификат для вебсервера

```
openssl x509 -req -extfile "ext-file.conf" -in zdc_cert_req.csr -days
1825 -CA ./zdc_ca_cert.crt -CAkey ./zdc_ca_cert.key -CAcreateserial -
out zdc serv cert.crt
```

4.4.4 Генерация сертификата в формате PFX

На основе полученного сертификата сгенерируйте сертификат в формате PFX

openssl pkcs12 -export -out zdc_serv_cert.pfx -inkey zdc_serv_cert.key
-in zdc serv cert.crt -passout pass:\$PFXPASS

В PFXPASS придумайте пароль от pfx файла, он потребуется при установке Зодиака.

4.5 Настройка доверия для самоподписанных сертификатов в ОС семейства Windows

1. Запустите консоль «Сертификаты – локальный компьютер» certim.msc



Рисунок 4.13 Запуск консоли «Сертификаты – локальный компьютер»

2. Вызовите контекстное меню на узле «Доверенные корневые центры сертификации», далее нажмите «Все задачи», затем «Импорт».



Рисунок 4.14 Вызов мастера импорта сертификата

3. На следующем шаге нажмите «Далее».



Рисунок 4.15 Окно мастера импорта файла сертификата

4. На следующем шаге нажмите «Обзор», затем выберите файл сертификата, затем нажмите «Далее».

		45
мпортируемый файл		
Укажите файл, который	і вы хотите импортирова	ать.
Имя файла:		Обзор
Замечание: следующие сертификата в одном ф	форматы файлов могут айле:	содержать более одного
Файл обмена личной	информацией - РКСЅ #12	(.PFX,.P12)
Стандарт Cryptograp	hic Message Syntax - cep	гификаты PKCS #7 (.p7b)
Хранилище сериализ	ованных сертификатов ((.SST)

Рисунок 4.16 Выбор файла сертификата для импорта

5. На следующем шаге убедитесь, что выбрано хранилище «Доверенные корневые центры сертификации», затем нажмите «Далее».

I
📀 🔗 Мастер импорта сертификатов
Vosuuruus consultuusson
Хранилище сертификатов - это системные области, в которых хранятся сертификаты.
Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.
О Автоматически выбрать хранилище на основе типа сертификата
Поместить все сертификаты в следующее хранилище
Хранилище сертификатов:
Доверенные корневые центры сертификации Обзор
Далее Отмена

Рисунок 4.17 Выбор хранилища сертификата

6. На следующем шаге нажмите «Готово».

катия кнопки "Готово". <mark>взователем</mark> Доверенные корневые це Сертификат C:\keydoak-17.0.1\conf\cr
<mark>ьзователен</mark> Доверенные корневые це Сертификат С:\keydoak-17.0.1\conf\ce
ызователен Доверенные корневые це Сертификат С: keydoak-17.0.1kconfkce
Сертификат C:\keycloak-17.0.1\conf\ce
C:\keycloak-17.0.1\conf\ce

Рисунок 4.18 Окно подтверждения готовности к импорту сертификата.

7. В случае успешно импорта появится следующее сообщение


Рисунок 4.19 Окно сообщения при успешном импорте сертификата

8. Найдите импортированный сертификат в списке и откройте его двойным кликом. Перейдите на вкладку «Путь сертификации» и убедитесь, что состояние сертификата имеет статус «Этот сертификат действителен».

сертификат	X
Общие Состав Путь сертификации	\leftrightarrow
Путь сертификации	
Просмотр сертифи	иката
Состояние сертификата: Этот сертификат действителен.	
	ОК

Рисунок 4.20 Проверка состояния сертификата

4.6 Настройка доверия для самоподписанных сертификатов в ОС семейства Linux

- 1. Установите ca-certificates
- sudo apt install ca-certificates

```
2. Скопируйте сертификат в папку с сертификатами в соответствии с вашей ОС
```

```
sudo cp $ca cert /usr/local/share/ca-certificates/zdc ca cert.crt
```

```
3. Обновите сертификаты
```

sudo update-ca-certificates

4.7 Настройка разрешений для порта в брандмауере Windows

1. Запустите консоль «Брандмауер Windows» wf.msc.

📼 Выполнить 🎴		x
	Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.	
Открыть:	wf.msd	~
	💡 Это задание будет создано с правами администратора	
-		_
	ОК Отмена Обзор	

Рисунок 4.21 Запуск консоли «Брандмауер Windows»

2. В панели «Действия» выберите «Правила для входящих подключений» нажмите «Создать правило».

🖌 Брандмауэр Windows в режиме повышенной безопасности		
Файл Действие Вид Справка		
(= =) (2 📰 🔒 🛛 📰		
🔗 Брандмауэр Windows в режиме повышенной безо	Правила для входящих подключений Действия	
 Ррандикаузр Windows в режиме повышенной безо	Правила для входящих подключений Миа	> > >
	Обнаружение сети (LLMNR UDP - входя Обнаружение сети Обнаружение сети (SSDP - входящий) Обнаружение сети	
< III >		

Рисунок 4.22 Запуск мастера создания правила для входящих подключений.

3. Выберите тип правила «Для порта» и нажмите «Далее»

💣 Mac	стер создания правила для нового входящего подключения	x
Тип правила Выберите тип правила бранду	наузра, которое требуется создать.	
Шалк: Тип правила Протокол и порты Действие Профиль Имя	Правило какого типа вы хотите создать? Ляя программы Правило, управляющее подключениями для программы. Пля порта Правило, управляющее подключениями для порта TCP или UDP. Предопределенные ВтаnchCache - обнаружение кзширующих узлов (использует WSD) v Правило, управляющее подключениями для операций Windows. Настраиваемые Настраиваемое правило.	ia

Рисунок 4.23 Окно выбора типа правила

4. Укажите протокол **TCP** и порт, для которого будет применяться правило. Нажмите «Далее».

💣 Ma	Мастер создания правила для нового входящего подключения	
Протокол и порты		
Укажите протоколы и порты, к которым применяется данное правило.		
Шапи:		
🧶 Тип правила	Укажите протокол, к которому будет применяться это правило.	
Протокол и порты	Протокол ТСР	
Действие	Протокол UDP	
 Профиль 		
● Имя	Укажите порты, к которым будет применятся это правило.	
	• Определенные порты: 3000	
	Пример: 80, 443, 5000-5010	
	< Назад Далее > Отмена	



5. На этапе выбора действия выберите «Разрешить подключение». Нажмите «Далее».

Maci	гер создания правила для нового входящего подключения 🌅
Действие Укажите действие, выполняем	ое при соответствии подключения условиям, заданным в данном правиле.
Ишали: • Тип правила • Протокол и порты • Действие • Профиль • Имя	истри соответствии подключения условиям, заданным травиле. Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям. Разрешить подключение Влючая как подключения, защищенные IPSec, так и подключения без защиты. С Разрешить безопасное подключение Влючая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений. Настроить

Рисунок 4.25 Окно выбора действия

6. В окне указания профилей оставьте настройки по умолчанию и нажмите «Далее».

🔐 📩 Mac	тер создания правила для нового входящего подключения	x
Профиль Укажите профили, к которым г	применяется это правило.	
Шапк:	Для каких профилей применяется правило? ✓ Доменный Применяется при подключении компьютера к домену своей организации. ✓ Частный Применяется, когда компьютер подключен к частной сети, например дома или в работе. ✓ Публичный Применяется при подключении компьютера к общественной сети.	ena

Рисунок 4.26 Окно указания профилей

7. Далее, задайте имя правила, например «Zodiac Inbound». Нажмите «Готово» для применения всех настроек.

🔐 Ma	астер создания правила для нового входящего подключения
Имя	
Укажите имя и описание дан	ного правила.
Шапи:	1
💩 Тип правила	
🧶 Протокол и порты	
Действие	
🥘 Профиль	
💩 Имя	
	Описание (необязательно):
	< Н <u>а</u> зад <u>Г</u> отово Отмена

Рисунок 4.27 Окно задания имени для правила нового входящего подключения

8. Новое правило с заданным именем должно появиться в списке правил для входящих подключений.

Брандмауэр Windows в режиме повышенной безопасности		
Файл Действие Вид Справка		
(+ +) (2 📰 🔒 🛛 🖬		
💣 Брандмауэр Windows в режиме повышенной безо	Правила для входящих подключений Действия	
Правила для входящих подключений Правила для исходящего подключения	Има Группа Лана Правила для входящих подключений	-
Правила безопасности подключения Маблюдение	Создать правило Фильторать по профилю	•
	Флаторизация службы входа в сеть (RPC) Служба входа в сеть Фильтровать по состоянию Фильтровать по состоянию	•
	Журналы и оповещения производител Журналы и оповещения п Фильтровать по группе Журналы и оповещения производител Журналы и оповещения п	•
	Журналы и оповещения производител Журналы и оповещения п Вид Обновить Обновить	•
	 Укрытив и оповещения производител журналы и оповещения п Инструментарий управления Windows Инструментарий управлен Экспортировать список 	
	Ø Инструментарий управления Windows Инструментарий управлен Ø Инструментарий управления Windows Инструментарий управлен Z Справка	
	Координатор распределенных транзак Координатор распределен Zodiac Inbound	-
	Координатор распределенных транзак Координатор распределен Отключить правило	
	Координатор распределенных транзак Координатор распределен	
	Маршрутизация и удаленный доступ (Маршрутизация и удаленн.	
	Маршрутизация и удаленный доступ (Маршрутизация и удаленн	
	Маршрутизация и удаленный доступ (Маршрутизация и удаленн 🗙 Удалить	
	Свойства	
	мастер настроики оезопасности: прав Мастер настроики оезопас Г Справка	
	мастер настрижи сезопасности прав мастер настрижи освопас	
	наолюдение за вирудолени машинов Наолюдение за вирудолени. Наблюзение за виртидањи машинов Наблюзение за вирудолени.	
	новладение за виртуальной машиной Наблюдение за виртуальн	
	новлодение за виртуальной машиной Набладение за виртуальн	
	Наблюдение за виртуальной машиной Наблюдение за виртуальн	
	Oбнаружение кэширующих узлов Bran BranchCache - обнаружен	
< III >	Сбызлоскение сети (LI MNR LIDP - входа Обналоскение сети У	

Рисунок 4.28 Созданное правило в списке правил для входящих подключений

4.8 Типичные ошибки при установке системы под ОС Linux

Для просмотра журналов всех systemd unit-сервисов удобно использовать такой инструмент как jornalctl. 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.s	server.service -f
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.se	rver.service: Main process exited, code=exited, st
Apr 04 09:21:11 zdc-srv systemd 1: zodiac.administration.se	rver.service: Failed with result 'exit-code'.

Рисунок 4.29 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 как описано в пункте Error! Reference source not found. для сервера администрирования или пункте Error! Reference source not found. 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 postgresql.conf сервера БД параметра
	listen_addresses = '*'
	и наличие в файле конфигурации hba.conf сервера БД записи
	host all all 0.0.0/0 md5
Microsoft.AspNetCore.Authentication.JwtBearer.JwtBe arerHandler[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 zodiac (раздел Error! Reference source not found.)
Npgsql.PostgresException (0x80004005): 42P01: отношение "scatter_package_upload" не существует	Не был выполнен скрипт dbscripts/create-db.sql (раздел Error! Reference source not found.)
Нечитаемые символы в сообщениях Npgsql.PostgresException от сервера БД.	Поменяйте в файле конфигурации postgresql.conf сервера БД значение параметра lc_messages:
	<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