ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

SQUADUS

СЕРВЕРНАЯ ЧАСТЬ

1.7

РУКОВОДСТВО ПО УСТАНОВКЕ

Версия 1

На 68 листах

Дата публикации: 17.12.2024

Москва
2024

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис», «MyOffice» и «Squadus» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ, ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

Сокращения, которые используются в настоящем документе, приведены в таблице 1.

Таблица 1 — Сокращения и обозначения

Сокращение	Расшифровка
ADFS	Active Directory Federation Services — компонент Windows Server обеспечивающий функции провайдера аутентификации для веб-приложений
API	Application Programming Interface — программный интерфейс приложения
Application Service	Служба приложений
АТС	Автоматическая телефонная станция
CPU	Central Processing Unit, процессор
FQDN	Fully Qualified Domain Name — «полностью определенное имя домена» — имя домена, не имеющее неоднозначности в определении. Включает в себя имена всех родительских доменов иерархии DNS
PBM	Percona Backup for MongoDB — распределенное решение с открытым исходным кодом для последовательного резервного копирования и восстановления сегментированных кластеров MongoDB и наборов реплик
OpenSCAP	Протокол автоматизации содержимого безопасности — приложение для проверки параметров конфигурации безопасности системы
SAN	Subject Alternative Name — расширение X.509 позволяющее использовать один сертификат для множества доменов
Webhook	Метод расширения или изменения поведения веб-страницы или веб-приложения с помощью обратных вызовов (в веб-разработке)
ВМ	Виртуальная машина
ООО	Общество с ограниченной ответственностью
ОС	Операционная система
ПО	Программное обеспечение
УЦ	Удостоверяющий центр

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

Настоящее руководство описывает порядок установки и настройки серверной части приложения Squadus.

1.2 О приложении

Squadus — приложение для рабочего общения с помощью текстовых, голосовых и видеосообщений, а также участия в конференциях в веб-браузерах и на операционных системах Windows, Linux, macOS.

Приложение Squadus входит в состав следующих продуктов:

– Squadus;

– Squadus PRO;

– «МойОфис Профессиональный 3».

Подробное описание возможностей приложения приведено в документе «Функциональные возможности»

1.3 Перечень изменений текущего документа

Изменения в версии 1.7

1. Добавлены разделы по подготовке конфигурации серверов:

– Конфигурирование CentOS;

– Конфигурирование ОС Astra;

– Конфигурирование файла hosts.yml;

– Карта портов.

2. Добавлены разделы с описанием нового функционала:

– Настройка интеграции с DLP;

– Настройка postfix;

– Установка Squadus за веб-прокси;

– Настройка веб-прокси для запуска playbook.

3. Дополнены уточняющей информацией разделы:

– Размещение SSL-сертификатов для шифрования;

– Обновление SSL-сертификатов

– Запуск установки.

1.4 Требования к персоналу

Для работы с ПО Администратору необходимо обладать релевантным опытом по следующим направлениям:

1. Основы сетевого администрирования:
– сетевая модель OSI и стек протоколов TCP/IP;
– IP-адресация и маски подсети;
– маршрутизация: статическая и динамическая;
– протокол обеспечения отказоустойчивости шлюза (VRRP).
2. Работа с подсистемой виртуализации на уровне эксперта:
– работа с VMware vSphere ESXi 6.5 или KVM;
– установка Docker;
– запуск, остановка и перезапуск контейнеров;
– работа с реестром контейнеров;
– получение параметров контейнеров;
– взаимодействие приложений в контейнерах (сеть в Docker);
– решение проблем контейнерной виртуализации.
3. Работа с командной строкой ОС Linux:
– опыт системного администрирования Linux;
– знания в объеме курсов AL-1702, AL-1703 (или аналогичных курсов других ОС);
– знания в объеме, достаточном для сдачи сертификационного экзамена ALCSA-1.7 (или аналогичных экзаменов других ОС).
4. Работа со службой доменных имен DNS:
– знание основных терминов (DNS, IP-адрес);
– понимание принципов работы DNS (корневые серверы, TLD-серверы, серверы имен доменов, разрешающий сервер имен);
– знание типов записи и запросов DNS.
5. Знание видов архитектуры, а также основных компонентов инфраструктуры открытых ключей (PKI):
– закрытый и открытый ключи;
– сертификат открытого ключа;
– регистрационный центр (RA);
– сертификационный центр (CA);
– хранилище сертификатов (CR).

6. Практический опыт администрирования на уровне эксперта:
– Prometheus;
– RabbitMQ;
– Redis;
– MongoDB;
– MinIO.
7. Работа с системой автоматизации развертывания Ansible.

1.5 Состав дистрибутива

Комплект поставки ПО предназначен для подготовки инфраструктуры сервера с ролью `operator` и дальнейшей установки ПО Squadus. Комплект включает в себя:

– исполняемый файл `squadus_ansible_bin_<RELEASE>.run`, предназначенный для установки подсистемы управления конфигурациями;
– исполняемый файл `squadus_infra_<RELEASE>.run`, предназначенный для установки хранилища образов Docker
– файл, содержащий лицензионное соглашение, политику конфиденциальности и список лицензий используемого ПО в формате html;
– руководство по установке ПО продукта.

1.6 Перечень технической документации

Перечень технической документации, представленный в таблице 2, предназначен для развертывания серверной части, настройки и дальнейшего администрирования продукта.

Таблица 2 — Перечень технической документации

Наименование документа	Содержание документа
Squadus_XX_System_Requirements	Системные и программные требования к продукту
Squadus_Server_Web_XX_Architecture	Описание архитектуры продукта для выбора типа установки и выделения ресурсов для серверов
Squadus_Server_Web_XX_ Installation_Guide	Порядок установки серверной части продукта
Squadus_Server_Web_XX_Backup_Guide	Порядок резервного копирования баз данных

1.7 Программные и аппаратные требования

Программные и аппаратные требования к текущей версии ПО указаны в документе «Системные требования».

1.8 Работа с системами виртуализации

Для обеспечения работы ПО поддерживаются следующие системы виртуализации:

- VMware;
- KVM.

2 ПОДГОТОВКА К УСТАНОВКЕ

2.1 Подготовка ОС

На серверы, предназначенные для развертывания системы, необходимо установить ОС, соответствующую требованиям документа «Системные требования».

Установка на ОС Astra и использование ОС CentOS потребует дополнительных настроек:

– для установки на ОС Astra необходимо выполнить операции, изложенные в разделе «Конфигурирование ОС Astra»;
– при использовании ОС CentOS следует ознакомиться с разделом «Конфигурирование CentOS».

2.1.1 Конфигурирование CentOS

С связи с прекращением поддержки CentOS 7 со стороны компании RedHat чистая установка на Linux дистрибутив CentOS невозможна.

Следует отключить обновление ядра в соответствии с разделом «Порядок обновления ядра Linux».

2.1.1.1 Восстановление доступа

Для востановления доступа к актуальным репозиториям на целевых хостах следует выполнить следующую команду:

```
sed -i s/mirror.centos.org/vault.centos.org/g /etc/yum.repos.d/*.repo
sed -i s/^#.*baseurl=http/baseurl=http/g /etc/yum.repos.d/*.repo
sed -i s/^mirrorlist=http/#mirrorlist=http/g /etc/yum.repos.d/*.repo
```

2.1.1.2 Миграция на другую ОС

Перед началом миграции на другую ОС Linux необходимо выполнить резервное копирование баз данных

Для миграции продукта на другую ОС Linux необходимо:

1. Перед установкой следует учитывать, что настройки, внесенные в систему с помощью панели администрирования, не сохраняются.

2. Установить ПО Squadus той же версии на новую ОС Linux с использованием конфигурационных файлов (`hosts.yaml` и `main.yaml`) от предыдущей установки.

3. При необходимости выполнить обновление до последней версии.

4. Восстановить базы данных из резервной копии.

2.1.2 Конфигурирование ОС AstraLinux

2.1.2.1 Установка на AstraLinux SE 1.7 в защищенных вариантах

Основные отличия между вариантами защищенности Astra SE 1.7 приведены в таблице 3.

Таблица 3 — Уровни защищенности ОС Astra

Функция безопасности	Уровень защиты «Базовый»*	Уровень защиты «Усиленный»*	Уровень защиты «Максимальный»*
Замкнутая программная среда	Не доступна	Доступна (по умолчанию выключена)	Доступна (по умолчанию выключена)
Очистка освобождаемой внешней памяти	Не доступна	Доступна (по умолчанию выключена)	Доступна (по умолчанию выключена)
Мандатный контроль целостности	Не доступна	Доступна (по умолчанию включена)	Доступна (по умолчанию включена)
Мандатное управление доступом	Не доступна	Не доступна	Доступна (по умолчанию включена)

* — наименование ОС Астра в соответствии с уровнем защиты:

– Базовый уровень — Астра 1.7 «Орел»;

– Усиленный уровень — Астра 1.7 «Воронеж»;

– Максимальный уровень — Астра 1.7 «Смоленск».

Текущий уровень защищенности проверяется с помощью команды:

```
root@voronezh:~# astra-modeswitch list
0   base(orel)
1   advanced(voronezh)
2   maximum(smolensk)
root@voronezh:~# astra-modeswitch get
1
```

Текущий статус замкнутой программной среды проверяется с помощью команды:

```
root@voronezh:~# astra-digsig-control status
ACTIVE
```

Текущий статус очистки освобождаемой внешней памяти (очистка разделов подкачки и гарантированное удаление файлов) проверяется с помощью команды:

```
root@voronezh:~# astra-swapwiper-control status
ACTIVE
root@voronezh:~# astra-secdel-control status
ACTIVE
```

Текущий статус мандатного контроля целостности проверяется с помощью команды:

```
root@voronezh:~# astra-mic-control status
ACTIVE
```


Текущий статус мандатного управления доступом проверяется с помощью команды:

```
root@voronezh:~# astra-mac-control status
INACTIVE
```

Текущий статус запрета включения бита выполнения проверяется с помощью команды:

```
root@voronezh:~# astra-nochmodx-lock status
ACTIVE
```

2.1.2.2 Установка на усиленном уровне защищенности («Воронеж»)

Установка осуществляется Ansible от имени пользователя, для которого должна быть настроена возможность выполнять sudo без пароля.

1. Пользователю astra необходимо установить максимальный уровень целостности 63 (соответствует администратору ОС). Проверить уровень целостности пользователя возможно с помощью команды:

```
root@voronezh:~# pdp-id -i
63
```

2. Установка Ansible и работа продукта невозможна при включенном запрете бита исполнения. Перед началом установки на всех серверах необходимо выполнить команду:

```
astra@voronezh:~$ sudo astra-nochmodx-lock disable
astra@voronezh:~$ sudo astra-nochmodx-lock status
INACTIVE
```

3. Установка Ansible и работа продукта невозможна при включенном режиме замкнутой программной среды. Необходимо проверить статус режима с помощью команды:

```
astra@voronezh:~$ sudo astra-digsig-control status
INACTIVE
```

4. При статусе `ACTIVE` перед началом установки на всех серверах необходимо выполнить команду:

```
astra@voronezh:~$ sudo astra-digsig-control disable
astra@voronezh:~$ sudo reboot
astra@voronezh:~$ sudo astra-digsig-control status
INACTIVE
```

5. Необходимо проверить статусы параметров безопасности, значения которых должны соответствовать таблице 4.

Таблица 4 — Параметры безопасности по умолчанию

Наименование команды	Статус
astra-bash-lock status	INACTIVE
astra-commands-lock status	INACTIVE
astra-docker-isolation status	INACTIVE
astra-hardened-control status	INACTIVE
astra-interpreters-lock status	ACTIVE
astra-lkrg-control status	INACTIVE
astra-macros-lock status	INACTIVE

Наименование команды	Статус
astra-modban-lock status	INACTIVE
astra-overlay status	INACTIVE
astra-ptrace-lock status	ACTIVE
astra-sumac-lock status	INACTIVE
astra-shutdown-lock status	INACTIVE
astra-ufw-control status	INACTIVE
astra-ulimits-control status	INACTIVE

6. Для проверки доступности репозиториев необходимо выполнить команду:

```
apt-get update
```

Команда должна завершаться без ошибки.

При наличии сбойного зеркала репозитория (например, http://mirror.yandex.ru/astra/stable/orel/repository orel InRelease), его необходимо удалить из директории `/etc/apt/sources.list`.

2.2 Настройка сетевых соединений

Настройка сетевого соединения должна быть выполнена на всех серверах, предназначенных для установки системы, в том числе на сервере с ролью `operator`.

Для работы серверов в локальной сети необходимо задать следующие параметры:

– IP-адрес;
– Маска подсети;
– Основной шлюз;
– DNS-сервер.

Пример настройки сетевого соединения с помощью командной строки в ОС Astra представлен в приложении В.

2.3 Подготовка инфраструктуры серверов

2.3.1 Установка в сети без выхода в интернет

Для установки продукта в локальной сети, без прямого выхода в интернет, необходимо обеспечить доступность дополнительных пакетов ПО. Перечень необходимого ПО приведен в документе «Системные требования».

Для обеспечения доступности следует выполнить следующие действия:

– скачать файлы со стандартного репозитория с помощью прямого выхода в интернет;
– разместить файлы на локальном сервере;
– обеспечить доступ к серверу по локальной сети;
– установить ПО и настроить локальный репозиторий (см. Приложение А);
– выполнить замену стандартного репозитория на локальный (см. Приложение Б).

Замена стандартного репозитория на локальный выполняется на сервере с ролью `operator`.

2.3.2 Установка Squadus за веб-прокси

При использование веб-прокси сервера в окружении установки потребуются дополнительные настройки серверов с ролью `operator` и `squadus_infra`.

2.3.2.1 Параметры настройки Squadus за веб-прокси

Для работы через веб-прокси необходимо запросить у системного администратора значения переменных, перечисленных в таблице 5.

Таблица 5 — *Список переменных* веб-прокси

Параметр	Тип	Описание
WEB_PROXY_LOGIN	Str	Имя пользователя
WEB_PROXY_PASSWD	Str	Пароль пользователя
WEB_PROXY_ADDR	Str	FQDN или IP адрес веб-прокси *
WEB_PROXY_PORT	Int	Порт веб-прокси *

***** — обязательные переменные

Полученные переменные оформляем следующим образом:

```
http://WEB_PROXY_LOGIN:WEB_PROXY_PASSWD@WEB_PROXY_ADDR:WEB_PROXY_PORT
https://WEB_PROXY_LOGIN:WEB_PROXY_PASSWD@WEB_PROXY_ADDR:WEB_PROXY_PORT
```

Если используемый веб-прокси не поддерживает TLS-подключение между клиентом и веб-прокси, следует переменной `https_proxy` указать значение переменной `http_proxy`. Такое решение позволит направить запросы к HTTPS страницам в интернете через веб-прокси без шифрованного подключения между клиентом и веб-прокси.

Для корректной работы серверов `squadus_infra`, `squadus_ansible` следует разрешить метод HTTP протокола — CONNECT на веб-прокси сервере.

2.3.2.2 Подготовка веб-прокси на серверах с ролью operator и squadus_infra

Для настройки окружения на серверах с ролью `operator` и `squadus_infra` необходимо открыть с помощью текстового редактора файл `/etc/environment` и добавить в конец файла следующие строки:

```
http_proxy="http://WEB_PROXY_LOGIN:WEB_PROXY_PASSWD@WEB_PROXY_ADDR:WEB_PROXY_PORT
"
https_proxy="https://WEB_PROXY_LOGIN:WEB_PROXY_PASSWD@WEB_PROXY_ADDR:WEB_PROXY_PO
RT"
```

Для применения нового окружения следует переподключиться по протоколу ssh или перезайти в систему.

2.3.3 Установка подсистемы управления конфигурациями

Установка выполняется на сервере с ролью `operator`. Необходимо проверить соблюдение следующих условий:

1. Вход выполнен под пользователем root или под пользователем с sudo-привилегиями на пакетный менеджер.

2. Сервер, на котором выполняется установка, соответствует требованиям, указанным в документе «Системные требования».

3. С выбранного сервера есть возможность доступа по SSH-протоколу к другим серверам, на которых выполняется установка.

4. Подсистема управления конфигурациями Ansible установлена, другие конфигурационные файлы Ansible не присутствуют в ОС.

Этапы установки:

1. Скопировать файл `squadus_ansible_bin_<RELEASE>.run` в домашнюю директорию пользователя root.
2. Запустить файл `squadus_ansible_bin_<RELEASE>.run` с помощью команды:

```
bash squadus_ansible_bin_<RELEASE>.run
```

3. Согласиться на продолжение установки, нажать на клавишу "Y".

```
      [root@squadus_infra ~]# bash ./squadus_ansible_bin_<RELEASE>.run Verifying
archiveintegrity...100% All good.
      Uncompressing SQUADUSAnsible Package <RELEASE>100%
      #
      # Copyright (c) New Cloud Technologies, Ltd., 2013-2024 #
      # You can not use the contents of the file in any way without New Cloud
Technologies, Ltd. written permission.
      # To obtain such a permit, you should contact New Cloud Technologies, Ltd.
at http://ncloudtech.com/contact.html
      # Welcome to Squadus AnsibleInstaller version <RELEASE>
      This script is meant to be used on operator workstation
      Do you want to continue? [y/N]Y
      Install ucs-storm[ OK ]
      Ensure that python-netaddr is installed                [ OK ]
      Ensure that python2-jmespath is installed              [ OK ]
      Ensure that version directory is present               [ OK ]
      Ensure that version <RELEASE> is present               [ OK ]
      Set <RELEASE> as latest                                [ OK ]
      Create roles symlink                                   [ OK ]
      Create collections symlink                             [ OK ]
      Create contrib symlink                                 [ OK ]
```

Администратору отобразится следующее (список отображения может меняться в зависимости от выбранной ОС):

```
      Create playbooks symlink                               [ OK ]
      Create group_vars directory                            [ OK ]
      Create group_vars/all symlink                          [ OK ]
      Create host_vars directory                             [ OK ]
      Create certificates directory                          [ OK ]
      Create certificates symlink                            [ OK ]
      Create symlink to module:ucs-storm                     [ OK ]
```

После этого установка подсистемы управления конфигурациями будет завершена.

При использовании веб-прокси после установки подсистемы управления конфигурации следует удалить из файла `/etc/environment` строки, добавленные в соответствии с разделом Подготовка веб-прокси на серверах с ролью operator и squadus_infra.

2.3.3.1 Ограничения по работе с подсистемой управления конфигурациями

В соответствии с разделом «Программные требования» на рабочем месте оператора необходимо установить пакеты дополнительного ПО.

В подсистеме управления конфигурациями не должно быть конфигурационных файлов самой подсистемы.

Конфигурационные файлы, установленные по умолчанию (например: `/etc/ansible/ansible.cfg`), необходимо удалить или заменить файлами из комплекта поставляемого ПО.

Подробнее по ссылке:
https://docs.ansible.com/ansible/latest/reference_appendices/config.html#the-configuration-file

2.3.4 Установка хранилища образов Docker

Установка производится на сервере с ролью `squadus_infra`. Перед началом установки необходимо проверить, что вход выполнен под пользователем root.

Этапы установки:

1. Скопировать файл `squadus_infra_<RELEASE>.run` на сервер `squadus_infra`.
2. Запустить скрипт установки:

```
bash squadus_infra_<RELEASE>.run
```

3. Согласиться на продолжение установки, нажав на клавишу «Y».

```
root@squadus_infra ~]# bash ./squadus_infra_<RELEASE>.run
Verifying archiveintegrity...100%                All good.
Uncompressing Squadus Infrastructure Node Package <RELEASE>100%
#
# Copyright (c) New Cloud Technologies, Ltd., 2013-2024 #
# You can not use the contents of the file in any way without New Cloud
Technologies, Ltd. written permission.
# To obtain such a permit, you should contact New Cloud Technologies, Ltd.
at http://ncloudtech.com/contact.html
# Welcome to Squadus Infrastructure Installer version <RELEASE>

This script is meant to be used on Infrastructure Server (see manualfor
default)
Do you want to continue? [y/N] Y
Check if the script is run with superuser privileges        [ OK ]
Make sure that the operating systemis compatible            [ OK ]
Ensurethat yum-utils is installed                           [ OK ]
```


Администратору отобразится следующее (список отображения может меняться в зависимости от выбранной ОС):

```
      Ensure that docker-ce repository is availiable                [ OK ]

      Ensure that docker is installed                               [ OK ]
      Ensure that jq package is installed                           [ OK ]
      Ensure that docker dir exists                                 [ OK ]
      Ensure that docker daemon config exists                       [ OK ]
      Check if docker daemon needs to be restarted                  [ OK ]
      Ensure that docker is started                                 [ OK ]
      Ensure that docker is enabled                                 [ OK ]
      Check if docker is availiable                                 [ OK ]
      Ensure that registry image is available                       [ OK ]
      Check if container with registry is available                 [CHANGE]
      Ensure that registry configuration directory exists           [ OK ]
      Ensure that docker-registry env file exists                   [ OK ]
      Check if old registry data directory exists                   [CHANGE]
      Ensure that registry data directory exists                    [CHANGE]
      Ensure that container with registry is available              [CHANGE]
      Wait for docker-registry to start                             [ OK ]
      Ensure that docker-registry is running                        [ OK ]
      Extracting registry archive...                                [ OK ]
      Remove dangling and outdated images                           [ OK ]
```

После этого установка хранилища образов Docker (docker_registry) будет завершена.

При использовании веб-прокси после установки хранилища образов Docker (docker_registry) следует удалить из файла `/etc/environment` строки, добавленные в соответствии с разделом Подготовка веб-прокси на серверах с ролью operator и squadus_infra.

2.3.5 Установка дополнительного ПО

В соответствии с документом «Системные требования» на сервере с ролью `operator` необходимо установить пакеты дополнительного ПО.

Рекомендуется использовать «чистую» ОС для предотвращения появления ошибок, связанных с использованием конфигурационных файлов.

Конфигурационные файлы, установленные по умолчанию (например: `/etc/ansible/ansible.cfg`), необходимо удалить или заменить файлами из комплекта поставляемого ПО.

Для установки пакетов необходимо обеспечить серверу с ролью `operator` выход в интернет.

Запрещается установка последних версий дополнительного ПО, доступных в репозитории. Перед установкой следует ознакомиться с требованиями к версиям ansible-core и модулям Python.

2.4 Подготовка конфигурационных файлов

Все операции с конфигурационными файлами выполняются на сервере с ролью `operator`.

2.4.1 Порядок размещения и заполнения файлов конфигурации

Этапы установки:

1. Перейти в каталог `~/install_squadus` с помощью команды:

```
root@squadus_infra~]# cd ~/install_squadus
```

2. Скопировать файл `contrib/squadus/ansible.cfg` в корневой раздел директории установки с помощью команды:

```
[root@squadus_infra~]# cp contrib/squadus/ansible.cfg
```

3. Выбрать наиболее подходящий тип установки:

– standalone (установка без поддержки отказоустойчивости);

– cluster (установка с поддержкой отказоустойчивости).

Предзаполненные файлы с примерами заполнения параметров установки располагаются по пути

```
~/install_squadus/contrib/squadus/[cluster | standalone]_hosts.yml
```

4. Скопировать заготовку файла `hosts.yml` в директорию `~/install_squadus/`:

```
cp contrib/squadus/<тип установки>_hosts.yml ./hosts.yml
```

5. Заполнить заготовку файла `hosts.yml`, указывая FQDN, по которым серверы доступны. Следует учитывать, что роли `squadus_ha` и `squadus_apps` не должны совпадать, если хостов в `squadus_apps` более одного.

6. Перенести заготовку файлов параметров `group_vars` с помощью команды:

```
cp -r contrib/squadus/group_vars/squadus_setup ./group_vars/
```

При необходимости можно переименовать `squadus_setup` на произвольное имя, но тогда необходимо изменить таким же образом имя группы `squadus_setup` в файле inventory.

8. Открыть файл `main.yml` из каталога размещения и отредактировать значения параметров по комментариям. Примеры параметров для минимальной настройки можно найти в самих файлах, а также в разделе «Настройка минимальных параметров установки».

9. Скопировать ssl-ключи для внешнего домена в каталог `certificates`. Подробнее см. в разделе «Размещение ssl-сертификатов для шифрования».

2.4.2 Конфигурирование файла hosts.yml

Для определения роли сервера необходимо добавить его доменное имя или IP-адрес в соответствующую секцию в шаблоне файла `hosts.yml`. После назначения роли серверу при установке будут выполнены команды Ansible. В файл `hosts.yml` вносятся только полностью определенные имена доменов (FQDN).

Преднастроенный файл `hosts.yml` (скопированный в соответствии с п. 3 раздела «Порядок размещения и заполнения файлов конфигурации») содержит примеры заполнения в следующем формате: `squadus-jibri-1.installation.example.net:`

где: – `squadus-jibri-1` — имя сервера для подгруппы `squadus_meet_jibri`;

– `installation.example.net` — имя домена установки.

Запись в файле `hosts.yml` при использовании группы серверов отличается записью имени сервера: `squadus-apps-[1:3].installation.example.net:`

где: `squadus-apps-[1:3]` — группа серверов `squadus_apps:`.

В кластерной конфигурации используется один или несколько серверов для одной роли.

Пример заполнения файла `hosts.yml` для кластерной конфигурации:

```
all:
  children:
    squadus:
      children:
        squadus_apps:                              # Группа серверов squadus_apps:
          hosts:
            squadus-apps-[1:3].installation.example.net:    # Имя DNS-сервера

        squadus_converter:
          hosts:
            squadus-doc-converter-[1:3].installation.example.net:

        squadus_db:
          hosts:
            squadus-db-[1:3].installation.example.net:
```

В конфигурации standalone для всех ролей используется один и тот же сервер.

Пример заполнения файла `hosts.yml` для конфигурации standalone:

```
all:
  children:
    squadus:
      children:
        squadus_apps:
          hosts:
             squadus-sa-1.installation.example.net:

        squadus_converter:
          hosts:
             squadus-sa-1.installation.example.net:

        squadus_db:
          hosts:
             squadus-sa-1.installation.example.net:
```

Объединение ролей может применяться в кластерной установке, если ресурсы организации ограничены. Подробнее о выделении ресурсов для установки см. в документе «Архитектура»

Порядок заполнения файла `hosts.yml` зависит от выбранной архитектуры устанавливаемой системы и настроек DNS-записей.

2.4.2.1 Ограничения по работе с файлом inventory

В файл `hosts.yml` вносятся только доменные имена. Часть логики установщика использует их для формирования доменных имен и адресов сервисов.

2.4.3 Конфигурирование файла main.yml

Для первичной установки системы необходимо скопировать предзаполненный файл конфигурации из директориии `~/install_squadus/contrib/squadus/`. Порядок подготовки файла `main.yml` определен в разделе «Порядок размещения и заполнения файлов конфигурации».

При повторной установке необходимо открыть с помощью текстового редактора файл расположенный в директории `~/install_squadus/group_vars/squadus_setup/main.yml` и изменить значения для обязательных переменных, перечисленных в таблице 6.

Описание переменных из конфигурационного файла `main.yml` представлено в таблице 6.

	В целях обеспечения безопасности все пароли и ключи, приведенные в таблице 6 и далее, должны быть заменены на новые.

Таблица 6 — Основные переменные

Параметр	Описание	Тип	Значение по умолчанию
ansible_user	Имя пользователя, от которого выполняется установка. Пользователь должен иметь доступ по ssh к хостам системы	Str	-
jibri_recorder_password	Пароль, используемый в подсистеме записи конференций	Str	-
jibri_auth_password	Пароль для внутренней авторизации сервиса записи конференций	Str	-
jicofo_auth_password	Пароль для аутентификации jicofo (компонент видеоконференций)	Str	-
jicofo_component_secret	Внутренний пароль для работы jicofo (компонент видеоконференций)	Str	-
jitsi_jwt_secret	JWT-пароль для работы jitsi (компонент видеоконференций)	Str	-
jitsi_jwt_app_id	Идентификатор JWT приложения	Str	-
jvb_auth_password	Аутентификационный пароль для работы jvb (компонент видеоконференций)	Str	-
jvb_component_secret	Внутренний пароль для работы jvb (компонент видеоконференций)	Str	-
manganum_mongodb_password	Пароль для базы данных, используемой компонентом manganum. Должен ссылаться на пароль сервиса squadus	Str	-
minio_access_key	Ключ доступа к хранилищу S3	Str	-
minio_secret_key	Секретный ключ для доступа к хранилищу S3	Str	-
mongodb_root_password	Пароль привилегированного пользователя в базе данных MongoDB	Str	-
mongodb_secured_key	Секретный ключ для установки MongoDB	Str	-
redis_password	Пароль к базе данных Redis	Str	-
squadus_domain	Указывается внешнее доменное имя системы для доступа к ПО Squadus	Str	-
squadus_mongodb_password	Пароль для базы данных, используемой сервисом squadus	Str	-
jitsi_use_keepalived	Включение и настройка сервиса keepalived для работы в кластерном режиме	Bool	-

Параметр	Описание	Тип	Значение по умолчанию
tls_ca_filename	Имя файла цепочки промежуточных сертификатов CA для внешнего домена	Str	ca.crt
tls_cert_filename	Имя файла сертификата для внешнего домена	Str	server.crt
tls_key_filename	Имя файла ключа для внешнего домена	Str	server.nopass.key
squadus_use_keepalived	Включение и настройка сервиса keepalived для работы в кластерном режиме	Bool	-
scandium_mongodb_password	Пароль для базы данных, используемой сервисом управления конференциями	Str	-
squadus_jwt_secret	JWT секрет для подключения ПО Squadus для сервиса управления конференциями	Str	Vagi2uk2CheCahbohphe
tennessine_mongodb_password	Пароль для базы данных, используемой компонентом tennessine. Должен ссылаться на пароль сервиса squadus	Str	-
zinc_mongodb_password	Пароль для базы данных, используемой компонентом zinc. Должен ссылаться на пароль сервиса squadus	Str	-
turnserver_cli_password	Пароль для доступа к администраторскому командному интерфейсу (CLI) - указано в файле дистрибутива readme	Str	RcBaN5mKibWe25h6NWiN
turnserver_secret	Внутренний пароль для работы API	Str	oogieyahneiBieneei8ey

Для генерации паролей и salt рекомендуется использовать утилиту pwgen. Безопасный пароль необходимо генерировать с помощью команды:

```
pwgen <длина пароля> 1
```

где `<длина пароля>` — должна быть не меньше 20 символов.

Для генерации хешей паролей необходимо использовать утилиту htpasswd. Хеш генерируется с помощью команды:

```
htpasswd -bnBC 12 "" <пароль> | tr -d ':\n'
```

Для конфигурации дополнительных переменных необходимо открыть с помощью текстового редактора файл `extra_vars.yml`, расположенный в директории: `~/install_squadus/group_vars/squadus_setup`.

2.4.3.1 Настройка веб-прокси для запуска playbook

При использовании веб-прокси сервера следует заполнить переменную из таблицы 7 аналогично переменным, представленым в разделе Конфигурирование файла main.yml.

Таблица 7 — Настройка использования веб-прокси

Параметр	Описание	Тип	Значение по умолчанию
squadus_os_environment	Содержит адрес и порт веб-прокси сервера, а так же параметры авторизации: имя пользователя и пароль.	Dict	{}

Пример заполнения переменной типа dict:

```
squadus_os_environment:
  http_proxy: \
"http://WEB_PROXY_LOGIN:WEB_PROXY_PASSWD@WEB_PROXY_ADDR:WEB_PROXY_PORT"
  https_proxy: \
"https://WEB_PROXY_LOGIN:WEB_PROXY_PASSWD@WEB_PROXY_ADDR:WEB_PROXY_PORT"
```

2.4.4 Конфигурирование файла extra_vars.yml

Настройка дополнительных параметров производится в файле `extra_vars.yml`. Данные параметры изменять не обязательно. Настройка дополнительных параметров установки приведена в таблице 8.

Таблица 8 — Настройка дополнительных параметров установки

Параметр	Описание	Тип	Значение по умолчанию
excalidraw_whiteboard_enabled	Включение виртуальной доски для рисования в видеоконференциях	Bool	false
jitsi_sip_enabled	Установка и настройка сервиса для интеграции со сторонней SIP системой	Bool	false
jigasi_sip_server	Адрес SIP сервера, с которым проводится интеграция	Str	-
jigasi_sip_port	Порт сервера SIP	Int	-
jigasi_sip_transport	Транспортный протокол, используемый сервером SIP, с которым проводится интеграция	Str	-
jigasi_auth_password	Внутренний пароль для сервиса jigasi	Str	-
jigasi_sip_password	Пароль для доступа к SIP серверу, с которым проводится интеграция	Str	-
jitsi_readonly_username_enabled	Разрешает или запрещает изменение отображаемого имени пользователя при подключении к конференциям	Bool	false
ntp_servers	Список NTP серверов для синхронизации времени	List	- "centos.pool.ntp.org"

Параметр	Описание	Тип	Значение по умолчанию
squadus_enable_ unbound	Устанавливает внутренний кеширующий DNS-сервер	Bool	true
unbound_access_ control	Словарь, описывающий сетки, которые имеют доступ к DNS-серверу	Dict	-
unbound_forward_ addresses	Список адресов серверов, к которым DNS-сервер будет перенаправлять запросы, если не может ответить самостоятельно	List	- “8.8.8.8” - “8.8.4.4”
zirconium_enabled	Включение интеграции с DLP-системой	Bool	false

Пример корректно настроенных параметров:

```
excalidraw_whiteboard_enabled: true

jitsi_sip_enabled: true
jigasi_sip_server: "10.1.1.51"
jigasi_sip_port: 5160
jigasi_sip_transport: "udp"
jigasi_auth_password: "wepeez3euQueik7pohke2cixohciePhu"
jigasi_sip_password: "Uzaingai6iuwo8aesuw9aThe6Jie7Ru5"

squadus_enable_unbound: true

unbound_access_control: network1:"192.168.1.0/24"

unbound_forward_addresses:
-"8.8.8.8"
-"9.9.9.9"

ntp_servers:
  - "ntp01.your-domain.ru"
  - "ntp02.your-domain.ru"
  - "ntp03.your-domain.ru"
```

2.4.5 Установка системы для работы более 1000 пользователей

При установке ПО Squadus для использования 1000 и более пользователей необходимо с помощью текстового редактора открыть файл, расположенный в следующей директории `inventory/group_vars/squadus/main.yml` и вручную добавить с новой строки переменную:

```
tennessine_status_debounce_time: 7000
```

2.5 Создание и размещение сертификатов

2.5.1 Создание SSL-сертификатов

Требования к сертификатам:

1. При создании сертификата следует учитывать, что SAN должен содержать необходимые доменные имена (см. полный список в разделе «Внешние DNS-записи»).
2. Допускается использование Wildcard SSL-сертификата.
3. Для корректной работы сертификат должен быть подписан авторизованным сертификационным центром.
4. Сертификаты должны обязательно соответствовать формату PEM и содержать «BEGIN CERTIFICATE». Сертификаты OpenSSL формата PEM с заголовком «BEGIN TRUSTEDCERTIFICATE» не поддерживаются.

2.5.2 Размещение SSL-сертификатов для шифрования

Порядок размещения сертификатов:

1. Разместить сертификат внешнего домена:

```
[root@squadus_infra ~]# vim certificates/server.crt
```

2. Разместить ключ внешнего домена:

```
[root@squadus_infra ~]# vim certificates/server.nopass.key
```

3. Разместить цепочку сертификатов промежуточных центров сертификации (CA) внешнего домена:

```
[root@squadus_infra ~]# vim certificates/ca.pem
```

При использовании самоподписанных сертификатов следует: вручную создать каталог `extra` в директории `certificates` и разместить файл `extra/ca.crt` УЦ выпустившего сертификат

В конце файла не должно быть пустой строки. Рекомендуется прочитать файл с помощью утилиты CAT. В результате отобразится следующее:

```
[root@squadus_infra ~]# cat certificates/external_server.cert.pem
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
[root@squadus_infra ~]#
```

Для создания самоподписанного (selfsigned) Wildcard SSL сертификата можно воспользоваться скриптом из поставки. После запуска приведенной команды генерируются все необходимые сертификаты и ключи для домена `example.net`, а также автоматически копируются в директорию `certificates`.

```
bash contrib/scripts/gen_self_signed_cert.sh example.net
```


2.6 Настройка DNS

2.6.1 Создание DNS-записей на сервере с ролью operator

Для всех серверов, перечисленных в файле `hosts.yml` в соответствии с разделом «Конфигурирование файла hosts.yml» необходимо создать DNS-записи. Для создания записей необходимо использовать DNS-сервер вашей организации.

При отсутствии DNS-сервера организации необходимо создать записи на сервере с ролью `operator` в файле `/etc/hosts`.

Пример содержимого файла `/etc/hosts` сервера с ролью `operator` для установки типа standalone:

```
192.168.1.100 squadus-sa-1.installation.example.net
```

Пример содержимого файла`/etc/hosts` сервера с ролью `operator` для кластерной установки:

```
192.168.1.100 squadus-apps-1.installation.example.net
192.168.1.101 squadus-apps-2.installation.example.net
192.168.1.102 squadus-apps-3.installation.example.net
192.168.1.103 squadus-doc-converter-1.installation.example.net
192.168.1.104 squadus-doc-converter-2.installation.example.net
192.168.1.105 squadus-doc-converter-3.installation.example.net
```

Количество записей соответствует количеству используемых физических или виртуальных серверов.

DNS-сервер организации должен содержать аналогичные записи в соответствии с требованиями собственной настройки.

2.6.2 Внутренние DNS-записи

Все DNS-записи, используемые для работы самой системой внутри контура установки, формируются через «.» (точку) относительно вписанного в файл inventory имени сервера, и создаются в unbound автоматически на основе переменной `ansible_default_ipv4`.

Это поведение можно переопределить, если заполнить все адреса вручную на основе примеров в файле групповых переменных `extra_vars.yml` (файл копируется на этапе подготовки к установке, см. раздел «Конфигурирование файла hosts.yml») или если не использовать unbound и заполнить все необходимые записи во внешнем DNS-сервере. При подобном варианте необходимо создать «A» записи для каждого доменного имени сервера, и записи CNAME для любых поддоменов каждого доменного имени сервера.

Например, «A» запись для `squadus-apps-1.installation.example.net` со значением `192.168.1.2` и CNAME запись для `*.squadus-apps-1.installation.example.net` со значением `squadus-apps-1.installation.example.net`.

2.6.3 Ограничения по использованию доменного имени

При выборе доменного имени и SSL-сертификата следует учитывать, что в настоящее время в качестве основного домена (`domain_name`), на котором будет работать система, могут быть использованы домены только второго уровня.

2.6.4 Внешние DNS-записи

В таблице 9 приведены необходимые внешние DNS-записи, необходимые для работы системы. Данная таблица сформирована на основании следующих условий:

– для переменной `domain_module` со значением `{service}.{domain}` (т .е. формирование ссылок указывается через точку к указанному домену);

– ansible-переменные `squadus_go_domain`, `squadus_preview_domain`, `jitsi_main_domain`, `scandium_main_domain`, `turnserver_realm` и `squadus_im_domain` (далее — FQDN-шаблоны) не переопределены (подробнее в разделе «Изменение внешних DNS-записей») и имеют значения по умолчанию.

Если выбран другой метод формирования и/или FQDN-шаблоны переопределены, необходимо соотнести его со значениями, представленными в таблице 9.

Используемые DNS-записи могут быть переопределены с помощью FQDN-шаблонов.

Таблица 9 — Сведения о внешних DNS-записях

Имя записи	FQDN-шаблон	Тип записи	Значение	Комментарии
im	squadus_im_ domain	A	IP для приложения Squadus	VRRP для squadus_ha при отказоустойчивой установке, IP-адрес сервера с ролью squadus_apps при установке без отказоустойчивости
go	squadus_go_ domain	A	IP для приложения Squadus	VRRP для squadus_ha при отказоустойчивой установке, IP-адрес сервера с ролью squadus_apps при установке без отказоустойчивости
meet	jitsi_main_ domain	A	IP сервера с ролью squadus_ha	VRRP для squadus_ha при отказоустойчивой установке, IP-адрес сервера с ролью squadus_apps при установке без отказоустойчивости
scc	scandium_main_ domain	A	IP сервера с ролью squadus_ha	VRRP для squadus_ha при отказоустойчивой установке, IP-адрес с ролью squadus_meet_apps

Имя записи	FQDN-шаблон	Тип записи	Значение	Комментарии
				при установке без отказоустойчивости
preview	squadus_preview_domain	A	IP сервера с ролью squadus_ha	VRRP для squadus_ha при отказоустойчивой установке, IP-адрес сервера с ролью squadus_apps при установке без отказоустойчивости
turn	turnserver_realm	A	IP сервера с ролью squadus_meet_jvb	IP-адрес первого сервера группы squadus_meet_jvb
editor	squadus_wte_editor_domain	A	IP сервера с ролью squadus_ha	VRRP для squadus_ha при отказоустойчивой установке, IP-адрес сервера с ролью squadus_apps при установке без отказоустойчивости

2.6.5 Организация работы сервисов разрешения имен

Во время установки производится настройка и запуск локального кеширующего DNS-сервера unbound на серверах с ролью `squadus_apps`. Unbound используется для запросов только внутри продукта и подключается для контейнеров и самих серверов через соответствующие параметры групповых переменных. По умолчанию серверы будут перенастроены на работу через unbound и не будут принимать параметры серверов разрешения имен по DHCP. Поэтому рекомендуется направить unbound на внутренние DNS-серверы компании, если такая необходимость есть. По умолчанию unbound настроен на переадресацию запросов на адреса 8.8.8.8 и 8.8.4.4.

2.6.6 Формирование внешних доменных имен

При установке системы есть возможность указывать метод формирования доменных имен для продукта.

Шаблон, который формирует итоговый вариант всех DNS-записей, принимает на вход значения следующих переменных:

– `squadus_domain` — отображает основной домен, на котором будет работать система;

– `domain_module` — отображает способ формирования доменного имени сервисов ПО Squadus.

Пример работы шаблона приведен в таблице 10.

Таблица 10 — Примеры работы шаблона

domain_module	Имя ссылки	squadus_domain	Результат
{service}.{domain}	Auth	example.net	auth.example.net

Изменение принципа формирования доменных имен системы следует выполнять с учетом ограничений (подробнее в разделе «Ограничения по использованию доменного имени»).

2.6.7 Изменение внешних DNS-записей

Для изменения названия внешней DNS-записи необходимо добавить переменные для каждого сервиса в файл `main.yml` в директории `squadus_setup` из таблицы 11. По умолчанию переменные принимают значения, указанные в таблице 10. Часть переменных должна иметь одинаковое значение.

Например, переменная `praseodymium_preview_domain` должна наследовать значение переменной `squadus_preview_domain`. Меняя значение одной переменной, необходимо заменить значение второй переменной.

Пример переопределения переменной:

```
squadus_domain: "example.net"
squadus_preview_domain: "preview-new-domain.{{ squadus_domain }}"
praseodymium_preview_domain: "{{ squadus_preview_domain }}"
```

Исходя из указанных значений, переменная `squadus_preview_domain` примет следующий вид:

```
preview-new-domain.example.net
```

Таблица 11 — Переменные, формирующие названия DNS-записей

Переменная	Тип	Описание
jitsi_main_domain	Str	Запись DNS для сервиса meet
praseodymium_ preview_domain	Str	Запись DNS для сервиса praseodymium. По умолчанию запись принимает значение переменной

Переменная	Тип	Описание
		squadus_preview_domain. Обе переменные должны иметь одинаковое значение
scandium_main_domain	Str	Запись DNS для сервиса scc
squadus_deeplink_url	Str	Запись DNS для сервиса deeplink. По умолчанию запись совпадает с переменной squadus_go_domain. При переопределении переменной необходимо добавить префикс, схему в названии домена — https://
squadus_go_domain	Str	Запись DNS для сервиса go
squadus_im_domain	Str	Запись DNS для сервиса im
squadus_preview_domain	Str	Запись DNS для сервиса preview
squadus_wte_editor_domain	Str	Запись DNS для сервиса editor
turnserver_realm	Str	Запись DNS для сервиса turnserver

2.6.8 Проверка работы DNS на сервере с ролью operator

После настройки необходимо проверить доступность DNS на сервере с ролью `operator`.

При использовании внешнего DNS-сервера необходимо открыть файл `~/install_squadus/group_vars/squadus_setup/extra_vars.yml` с помощью текстового редактора и добавить адрес DNS-сервера, изменив IP-адрес:

```
## DNS Forwarder Configuration
# List of DNS servers that the queries will be forwarded to
# unbound_forward_addresses:
- "8.8.8.8"
- "8.8.4.4"
```

Для проверки соответствия доменного имени IP-адресу сервера необходимо:

1. Установить ПО с помощью команды:

```
apt install dnsuntils
```

или

```
yum install bind-utils
```

Выбор команды зависит от типа ОС.

2. После установки ПО выполнить следующую команду:

```
> dig A squadus-sa-1.installation.example.net
```

Пример ответа:

```
      ; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> A squadus-sa-
1.installation.example.net
      ;; global options: +cmd
      ;; Got answer:
      ;; opcode: QUERY, status: NOERROR, id: 45369
      ;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
      ;; OPT PSEUDOSECTION:
      ; EDNS: version: 0, flags:; udp: 65494;;
      QUESTION SECTION:
      ;squadus-sa-1.installation.example.net. IN A ;;
      ANSWER SECTION:
      *.squadus-sa-1.installation.example.net. 900 IN CNAME squadus-sa-
1.installation.example.net.
      squadus-sa-1.installation.example.net. 900 IN A 192.168.0.1
      ;; Query time: 23 msec
      ;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP) ;; WHEN: Tue Jan 10 15:56:32
      MSK 2023
      ;; MSG SIZE rcvd: 95
```

В ответе необходимо найти секцию `ANSWER SECTION` и проверить, что доменное имя соответствует IP-адресу.

```
      *.squadus-sa-1.installation.example.net. 900 IN CNAME squadus-sa-
1.installation.example.net.
      squadus-sa-1.installation.example.net. 900 IN A 192.168.0.1
```

2.7 Карта портов

Карта портов представлена в таблице 12.

Таблица 12 — Карта портов

Группа Ansible	Сервис	Прослушива-емый порт	Порт подключения	Куда обращается
All	cadvisor	9101/tcp	нет	нет
	node_exporter	9093/tcp		
	syslog-ng	514/udp, 601/tcp		
squadus_apps	envoy	8999/tcp	25/tcp	postfix
		8002/tcp	8002/tcp	pregen
		9094/tcp	8999/tcp	minio
		10000/tcp	8082/tcp	cvm
	boron	3039/tcp	27017/tcp	mongodb
		9544/tcp		
	tennessine	3009/tcp	27017/tcp	mongodb
		3040/tcp	4222/tcp	nats
		9545/tcp		
	cobalt	3034/tcp	27017/tcp	mongodb
		9532/tcp	4222/tcp	nats
		9549/tcp		
	copper	3011/tcp	27017/tcp	mongodb
			4222/tcp	nats
	argon	3041/tcp	27017/tcp	mongodb

Группа Ansible	Сервис	Прослушива-емый порт	Порт подключения	Куда обращается
		9546/tcp	4222/tcp	nats
			6379/tcp	redis
	zinc	3035/tcp	27017/tcp	mongodb
		9531/tcp	4222/tcp	nats
			3034/tcp	cobalt
	squadus	3070/tcp	3039/tcp	boron
		3301/tcp	3014/tcp	sodium
		9192/tcp	3009/tcp	tennessine
			3034/tcp	cobalt
			3011/tcp	cobalt
			3041/tcp	argon
			3035/tcp	zinc
			3010/tcp	krypton
			3037/tcp	lithium
			3013/tcp	chlorine
			3036/tcp	praseodymium
			3040/tcp	neon
			27017/tcp	mongodb
			4222/tcp	nats
			9999/tcp	scatter
			8003/tcp	envoy
			9000/tcp	envoy
			8082/tcp	envoy
			8009/tcp	synapse
	krypton	3010/tcp	27017/tcp	mongodb
		9534/tcp	4222/tcp	nats
		9540/tcp	3034/tcp	cobalt
	chlorine	3013/tcp	27017/tcp	mongodb
		9537/tcp	3034/tcp	cobalt
			3035/tcp	zinc
			3010/tcp	krypton
			4222/tcp	nats
	praseodymium	3036/tcp	3034/tcp	cobalt
		7509/tcp	3035/tcp	zinc
		9543/tcp	4222/tcp	nats
			9094/tcp	cvm
	neon	3040/tcp	3034/tcp	cobalt
		9542/tcp	4222/tcp	nats
			3010/tcp	krypton
			3013/tcp	chlorine
			3014/tcp	sodium
	sodium	3014/tcp	27017/tcp	mongodb
		9538/tcp	4222/tcp	nats
			3034/tcp	cobalt

Группа Ansible	Сервис	Прослушива-емый порт	Порт подключения	Куда обращается
			3011/tcp	copper
			3041/tcp	argon
			3010/tcp	krypton
			3013/tcp	chlorine
			3036/tcp	praseodymium
	radon	3047/tcp	27017/tcp	mongodb
		9547/tcp	4222/tcp	nats
			3010/tcp	krypton
			3034/tcp	cobalt
			3014/tcp	sodium
	iridium	3048/tcp	27017/tcp	mongodb
		9548/tcp	4222/tcp	nats
	bohrium	3008/tcp	3020/tcp	scandium
		3038/tcp	3035/tcp	zinc
		9540/tcp		
	lithium	3037/tcp	27017/tcp	mongodb
		9541/tcp	4222/tcp	nats
			3034/tcp	cobalt
	calcium	3049/tcp	27017/tcp	mongodb
		7049/tcp	4222/tcp	nats
		9549/tcp	3034/tcp	cobalt
	caddy	80/tcp	нет	нет
		443/tcp		
		2019/tcp		
		3300/tcp		
		8448/tcp		
squadus_converter	cvm	8082/tcp	8002/tcp	envoy
		9094/tcp	9096/tcp	envoy
	jod	9096/tcp	нет	нет
	pregen	8002/tcp	нет	нет
	envoy	8999/tcp	8002/tcp	pregen
		8002/tcp	9096/tcp	jod
		8082/tcp		
		9901/tcp		
		10000/tcp		
squadus_db	postgresql	5432/tcp	нет	нет
	mongodb	27017/tcp	нет	нет
		27019/tcp		
squadus_mail	opendkim	12301/tcp (доступ с bridge)	нет	нет
	postfix	25/tcp (доступ с bridge)	12301/tcp	opendkim
squadus_meet_apps	scandium	3020/tcp	27017/tcp	mongodb
		3030/tcp	3034/tcp	cobalt

Группа Ansible	Сервис	Прослушива-емый порт	Порт подключения	Куда обращается
		9539/tcp	4222/tcp	nats
			443/tcp	jitsiweb
	excalidraw	3002/tcp	нет	нет
	prosody	5222/tcp	3478/udp	turnserver
		5269/tcp	5349/tcp	turnserver
		5280/tcp	3020/tcp	scandium
		5347/tcp	2700/tcp	
	prosody_visitor_[1-8]	5222[1-8]/tcp		
		5269[1-8]/tcp		
		5280[1-8]/tcp		
		52801[1-8]/tcp		
		5347[1-8]/tcp		
	jicofo	8801/tcp	5222/tcp	prosody
			5222[1-8]/tcp	prosody_visitor_[1-8]
	jigasi-sip	20050-20099/udp	external sip port	external sip
	jitsiweb	82/tcp, 443/tcp	9099/tcp	jvb
			3002/tcp	excalidraw
squadus_meet_jvb	jvb	4443/tcp	нет	нет
		8901/tcp		
		4096/udp		
		10000/udp		
		9099/tcp		
	turnserver	3478/udp		
		5349/tcp		
squadus_meet_vosk	vosk	2700/tcp	нет	нет
		2701/tcp		
squadus_mq	nats	4222/tcp	нет	нет
		6222/tcp		
		8222/tcp		
squadus_redis		6379/tcp	нет	нет
		16379/tcp		
		6380/tcp		
		6381/tcp		
squadus_search	scatter	9999/tcp	50051/tcp	squash_search
	squash_search	50051/tcp	нет	нет
squadus_st	minio	9000/tcp	нет	нет
		43145/tcp		
squadus_infra	synapse	8449/tcp	8448/tcp	Caddy
		8448/tcp	5432/tcp	postgresql
		8008/tcp		
		8011/tcp		
		8009/tcp		

Группа Ansible	Сервис	Прослушива-емый порт	Порт подключения	Куда обращается
	caddy	80/tcp	9093/tcp	alertmanager
			3001/tcp	grafana
			9090/tcp	prometheuss
			8428/tcp	victoria-metrics
	CA	3002/tcp	нет	нет
	registry	5000/tcp		
	alertmanager	9093/tcp		
	blackbox_exporter	9115/tcp		
	pushgateway	9091/tcp		
	victoria-metrics	8428/tcp		
	postgres_exporter	9187/tcp	5432/tcp	postgresql
	redis_exporter	9121/tcp	6379/tcp	redis
			6380/tcp	
			6381/tcp	
	nats_exporter	7778/tcp	8222/tcp	nats
	jitsi_exporter	6071/tcp	8901/tcp	jvb
			8801/tcp	jicofo
	mongodb_exporter	9126/tcp	27017/tcp	mongodb
	grafana	3000/tcp	9090/tcp	prometheus
	mongo_backup	-	27017/tcp	mongodb
	minio_backup	-	9000/tcp	minio
	prometheus	9090/tcp	9093/tcp	alertmanager
			9115/tcp	blackbox_exporter
			6071/tcp	jitsi_exporter
			9126/tcp	mongodb_exporter
			9121/tcp	redis_exporter
			9187/tcp	postgres_exporter
			7778/tcp	nats_exporter
			8011/tcp	synapse
squadus_ha	caddy	80/tcp	443/tcp	Caddy
		443/tcp	3300/tcp	jitsiweb
		2019/tcp	443/tcp	jitsiweb
		3300/tcp	8449/tcp	Caddy
		8448/tcp		

3 УСТАНОВКА

3.1 Запуск установки

Установку можно выполнить двумя способами:

1. Для установки потребуется выполнить следующие действия:

– Запустить команду на подготовку серверов к установке:

```
ansible-playbook playbooks/common.yml --diff
```

После запуска этой команды будут запущены роли, указанные в документе «Архитектура» таблица «Описание общих ролей подсистемы Ansible».

– Запустить команду на установку ПО Squadus:

```
ansible-playbook playbooks/squadus.yml --diff
```

После этого запускаются роли, указанные в документе «Архитектура» таблица «Роли, используемые для установки ПО Squadus».

2. Запустить объединенный playbook, который выполнит подготовку серверов и установку ПО Squadus:

```
ansible-playbook playbooks/main.yml --diff
```

При использовании на сервере с ролью operator ОС Astra версии 1.7.5 или ниже следует выполнять запуск playbook с ключем --skip-tags monitoring

3.2 Проверка корректности установки

Для проверки корректности установки сервера продукта необходимо выполнить следующие действия:

1. Запустить приложение ПО Squadus.
2. Использовать для входа учетные данные пользователя или администратора.
3. Выбрать контакт из списка и отправить ему сообщение.
4. Если сообщение успешно отправилось и было прочитано пользователем — система настроена корректно.

3.3 Запуск веб-интерфейса ПО

Пользователи получают доступ к веб-интерфейсу ПО Squadus с помощью веб-браузера или настольного приложения. Для запуска ПО Squadus с помощью веб-интерфейса необходимо:

1. Открыть браузер при активном сетевом подключении.
2. Ввести в адресную строку браузера адрес вида https://mydomain.ru/.
3. Нажать клавишу **Enter**.
4. Дождаться открытия страницы авторизации ПО Squadus.

3.4 Установка в составе других продуктов «МойОфис»

Установка в составе других продуктов «МойОфис» не выполняется.

4 ОБНОВЛЕНИЕ

4.1 Обновление с предыдущих версий

Данный дистрибутив предназначен для чистой установки.

Переход с одной версии на другую осуществляется аналогично установке новой версии. Порядок установки описан в разделе «Первичная установка».

4.2 Обновление сервера с ролью turn

Для обновления turn сервера с версии 1.5 на версию 1.6 следует в файл `hosts.yml` добавить группу `squadus_meet_jvb` и указать доменное имя или IP-адрес первого сервера.

Пример:

```
 squadus_meet_jvb:
        hosts:
          squadus-jvb-1.installation.example.net:
      squadus_meet_turn:
        hosts:
          squadus-jvb-1.installation.example.net
```

4.3 Обновление SSL-сертификатов

Для обновления ранее установленных сертификатов необходимо разместить новые сертификаты в директории `certificates` согласно порядку размещения, описанном в разделе «Размещение ssl-сертификатов для шифрования», заменив старые файлы на новые.

После выполнения шагов, описанных в разделе «Размещение ssl-сертификатов для шифрования», необходимо выполнить установку новых сертификатов с помощью команды:

```
      ansible-playbook -playbooks/squadus.yml --diff -t
postfix,caddy2,turnserver,prosody,jibri
```

При использовании самоподписанных сертификатов следует: вручную создать каталог `extra` в директории `certificates` и разместить файл `extra/ca.crt` УЦ выпустившего сертификат

5 ДОПОЛНИТЕЛЬНЫЕ ПАРАМЕТРЫ УСТАНОВКИ

5.1 Аутентификация в docker registry

По умолчанию в docker registry, устанавливаемом на сервер группы `squadus_infra`, включена аутентификация по логину и паролю для доступа к docker image. Переменные, отвечающие за аутентификацию указаны в таблице 13.

Таблица 13 — Настройка минимальных параметров аутентификации docker registry

Параметр	Описание	Тип	Значение по умолчанию
docker_registry_endpoint	FQDN docker registry	Str	http://{{ docker_image_registry }}
docker_registry_password	Пароль пользователя	Str	oEeUL8kvCkkuxUia8ZaL
docker_registry_username	Имя пользователя	Str	admin

Для отключения аутентификации docker registry необходимо:

- удалить вышеперечисленные переменные из ansible playbook;
- на сервере группы `squadus_infra` удалить файлы `env`, `.htpasswd` выполнив команды:

```
rm -f /srv/docker/registry/conf/env
rm -f /srv/docker/registry/conf/.htpasswd
```

- после выполнения команд перезапустить контейнер docker registry для применения изменений:

```
docker restart docker-registry
```

Для смены пароля, используемого по умолчанию, необходимо:

- изменить пароль в ansible playbook;
- изменить файл `.htpasswd` на сервере группы `squadus_infra` используя утилиту htpasswd.

Пример команды:

```
htpasswd -Bbc /srv/docker/registry/conf/.htpasswd USERNAME PASSWORD
```

где:

`USERNAME` — имя пользователя;

`PASSWORD` — пароль.

5.2 Возможные проблемы в работе docker registry

1. Отсутствует DNS-запись для сервера группы `squadus_infra`, при этом запросы доступа к docker registry возвращают ошибку 500.
2. Отсутствует доступ к 5000/tcp порту сервера группы `squadus_infra`.

3. Не совпадают логин и пароль для доступа к docker registry.
4. При смене пароля используется алгоритм хеш-функции, отличный от BCRYPT.

Пример команды:

```
htpasswd -Bbn admin oEeUL8kvCkkuxUia8ZaL
```

5.3 Настройка стенда ПО

Для настройки Squadus SAML необходимо подключение к контроллеру домена Active Directory Federation Service (далее — ADFS). Для этого следует перейти в доступный через поиск раздел администрирования SAML и заполнить поля (рис. 1).

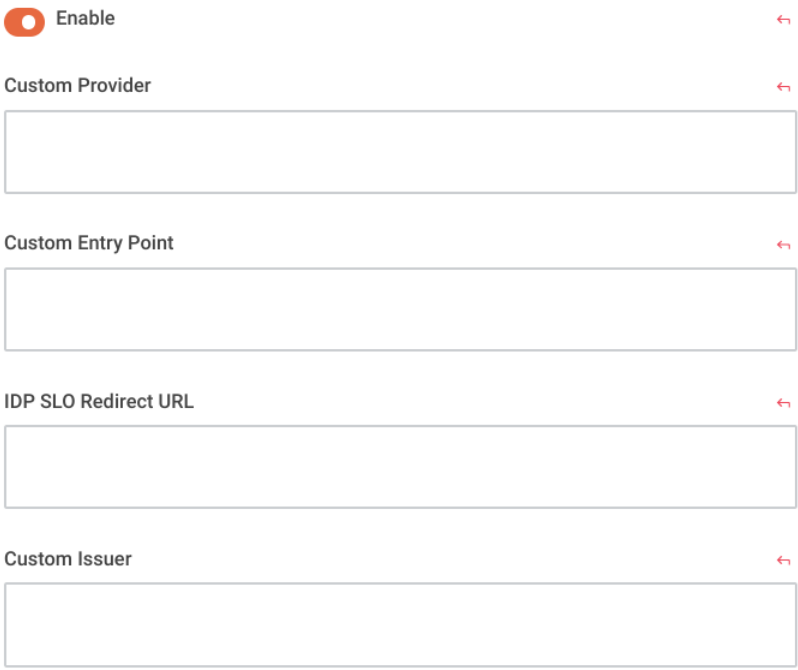

Рисунок 1 — Заполнение полей в SAML разметке

Поля, представленные на рисунке:

- Custom Provider — example-adfs;
- Custom Entry Point — https://mdcad-dc-01.ad.example.ru/adfs/ls/. Адрес контроллера ADFS;
- IDP Slow Redirect URL — https://mdcad-dc-01.ad.example.ru/adfs/ls/. Адрес контроллера ADFS;
- Custom Issuer — https://im.example.ru/_saml/metadata/example-adfs. Ссылка для сбора метаданных стенда. Часть example-adfs заполняется самостоятельно, как и в первом пункте Custom Provider (пункты должны совпадать);
- Private Key Component — приватный ключ. Ключ передается администратором ADFS в формате Base64 (PEM).

5.3.1 Добавление стенда на стороне ADFS

Чтобы добавить стенд на стороне ADFS, необходимо выполнить следующие действия:

1. Открыть панель администрирования ADFS (рис. 2):

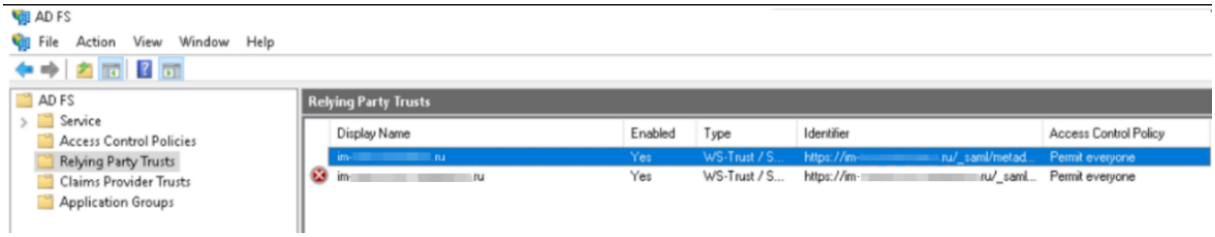

Рисунок 2 — Панель администрирования ADFS

2. В разделе **Relying Party Trust** в правом углу выбрать **Add Relying Party Trust** (рис. 3):

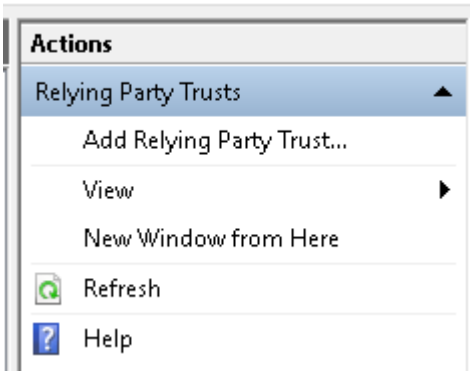

Рисунок 3 — Выбор действия Add Relying Party Trust

3. В первом пункте выбрать **Claims aware > Start**.

4. Далее добавить ссылку, сформированную в поле **Custom Issuer** в Squadus (рис. 4):

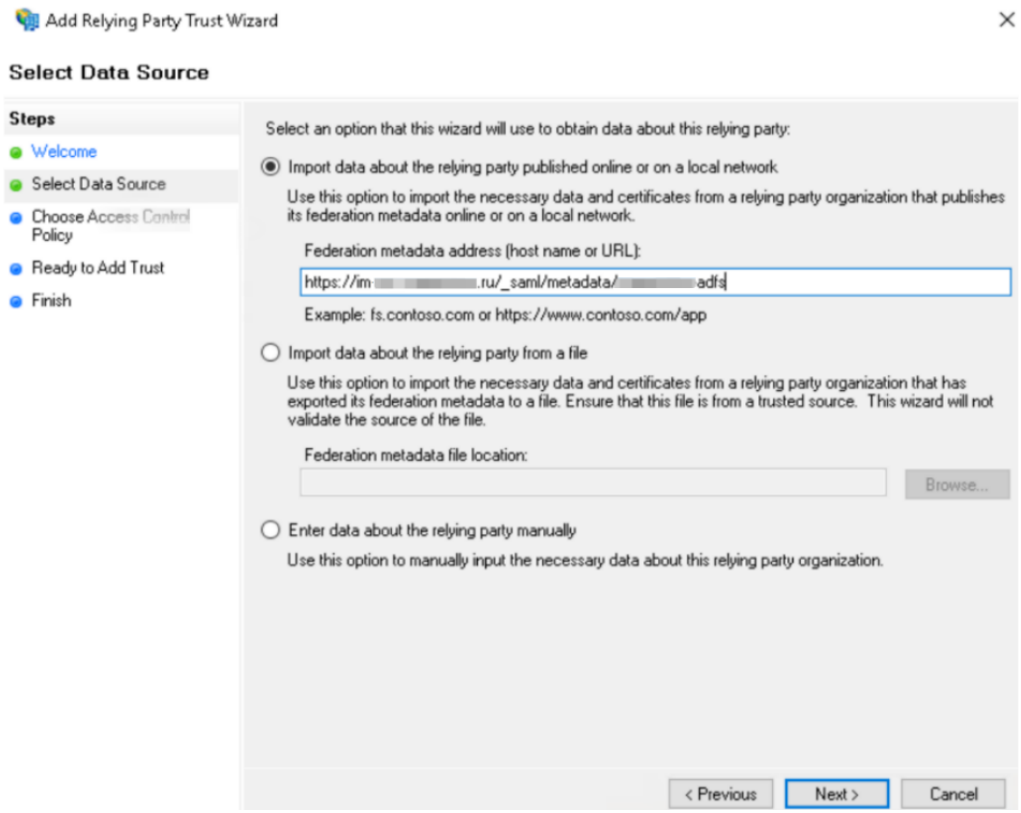

Рисунок 4 — Добавление ссылки

5. В последующих окнах необходимо нажать на кнопку **Next**.

5.3.2 Известные ограничения

Если у пользователя нет полей из Mapping переменных (например, почты) необходимо выполнить следующие действия:

– создать правила для Relying Party Trust для ранее созданного стенда;

– правой кнопкой мыши нажать на созданный ранее стенд **Edit Claim Issuance Policy** (рис. 5):

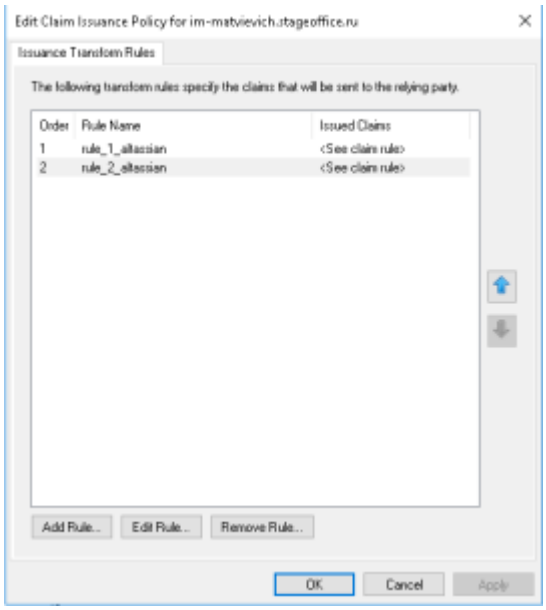

Рисунок 5 — Выбор ранее созданного стенда Edit Claim Issuance Policy

Правило 1:

```
      c:[Type
== "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"]
       => issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn", "http://schemas.xml
soap.org/ws/2005/05/identity/claims/emailaddress", "http://schemas.xmlsoap.org/ws
/2005/05/identity/claims/givenname", "http://schemas.xmlsoap.org/ws/2005/05/ident
ity/claims/surname"), query = ";objectSID,mail,givenName,sn;{0}", param =
c.Value);
```

Правило 2:

```
      c:[Type
== "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
       => issue(Type
= "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
= c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format
"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

Если добавить Relying Party Trust не получается из-за отсутствия поддержки TLS выше версии 1.0 на стороне ADFS, то следует рассмотреть рекомендации по внесению изменений от Microsoft, приведенные в соответствующих статьях.

Чтобы добавить фото пользователя из Active Directory, необходимо выполнить команду:

```
      c:[Type
== "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"]
       => issue(store = "Active Directory", types = ("thumbnailPhoto"), query
= ";thumbnailPhoto;{0}", param = c.Value);
```

5.4 Настройка вебинаров

5.4.1 Включение вебинаров

По умолчанию данная возможность отключена. Для включения необходимо выполнить следующие действия:

1. Задать переменной `jitsi_webinar_enabled` значение `true` в файле `group_vars/squadus/main.yml`

Пример заполнения:

```
      jitsi_webinar_enabled: true
```

2. Применить конфигурацию с сервера оператора.

```
      ansible-playbook playbooks/squadus.yml --tags caddy2,jitsi  --diff
```

3. В разделе **Администрирование** -> **Видеоконференции** -> **Флаги возможностей** включить **Создание видеоконференции в режиме вебинара**.

	Создавать вебинары могут только пользователи с правом **Доступ к созданию вебинаров**.

5.4.2 Проверка работоспособности вебинаров

Для проверки работоспособности необходимо выполнить следующие действия:

1. Запустить ПО Squadus.
2. Нажать на пиктограмму  и выбрать в открывшемся меню пункт **Создать вебинар** (рис. 6):

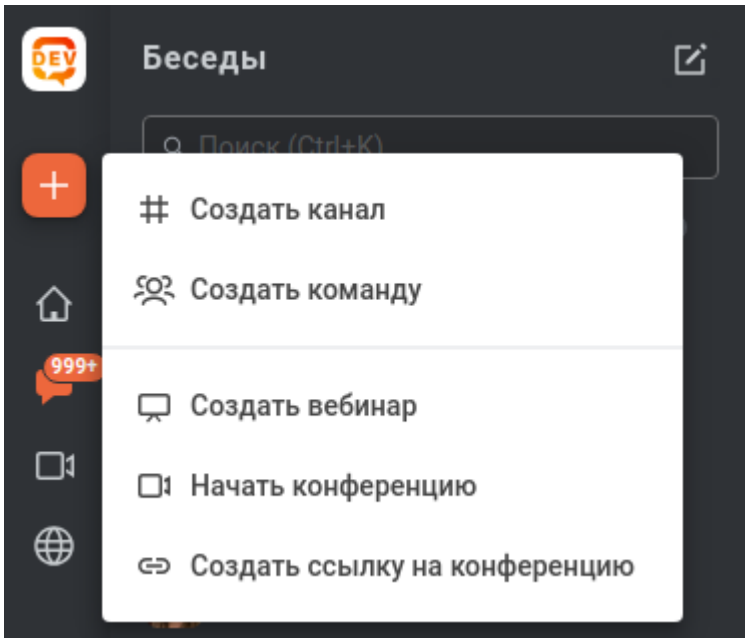

*Рисунок 6 — Меню **Создание***

3. В окне создания вебинара (рис. 7) необходимо указать **Тему** и присоединиться по указанной ссылке.

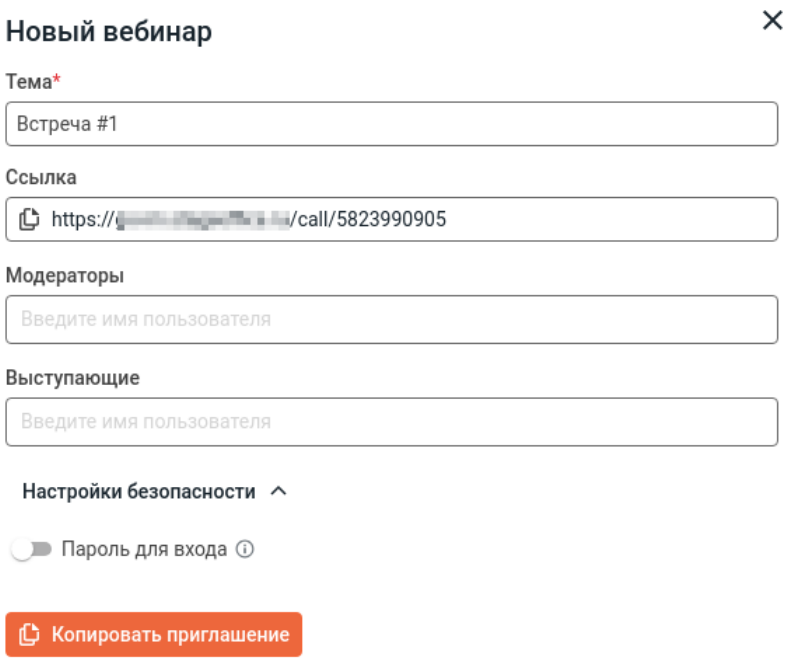

Рисунок 7 — Окно создания нового вебинара

5.5 Настройка push-уведомлений в режиме удаленного вызова процедур GRPC

Настройка push-уведомлений выполняется в ручном или автоматическом режиме.

Автоматическая настройка производится с использованием переменных из файла `group_vars/squadus_setup/main.yml`. Все параметры передаются в environment контейнера сервиса `squadus` и при перезапуске контейнера будут применены повторно.

Автоматическая настройка невозможна без повторного запуска `ansible-playbook` с последующим перезапуском контейнеров `squadus`. На время перезапуска сервисы будут недоступны.

Ручная настройка предполагает ввод параметров подключения через административную панель. При настройке перезапуск контейнеров не потребуется.

Для настройки push-proxy администратору стенда `squadus` будут переданы следующие данные:

– файл сертификата CA центра;
– файл сертификата клиента подписанный CA центром;
– файл с ключом для сертификата клиента;
– ID клиента;
– пароль клиента;
– список серверов для подключения по GRPC с указанием FQDN серверов, и порт подключения (по умолчанию используется порт 3031/tcp).

	Список серверов для подключения задан по умолчанию в переменной `myoffice_push_grpc_proxy_endpoints`

5.5.1 Ручная настройка

Перед началом настройки push-proxy необходимо убедиться, что пользователь обладает правами администратора.

Для включения настройки следует открыть административную панель и перейти в раздел **Администрирование** > **Push уведомления**.

В соответствии с рисунком 8 необходимо установить переключатель в правое положение **Включить**.

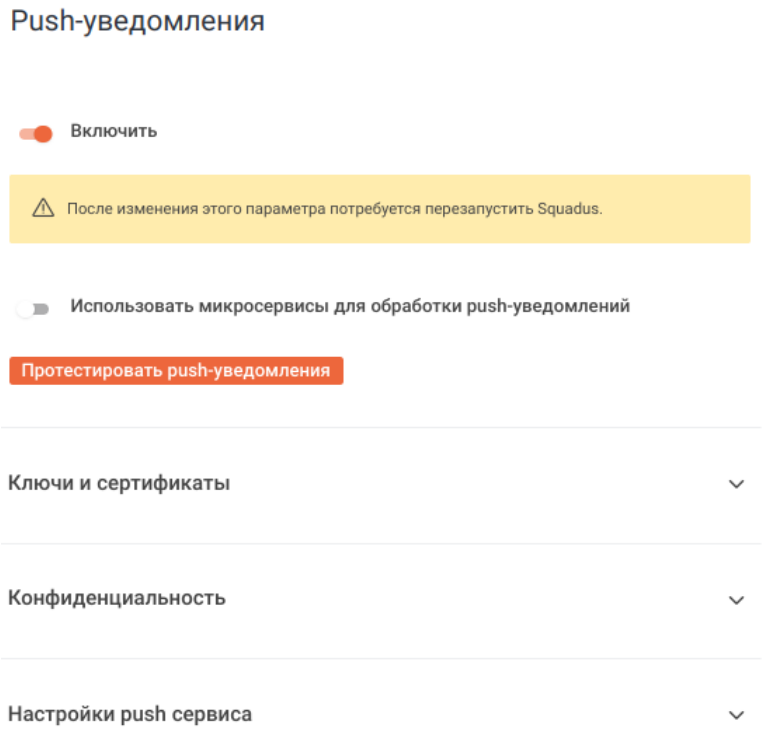

Рисунок 8 — Окно подключения push-уведомлений

После включения сервиса в списке параметров необходимо выбрать пункт **Настройки push сервиса**.

В открывшемся окне (рис. 9) следует указать значения для полей, описанных в таблице 14.

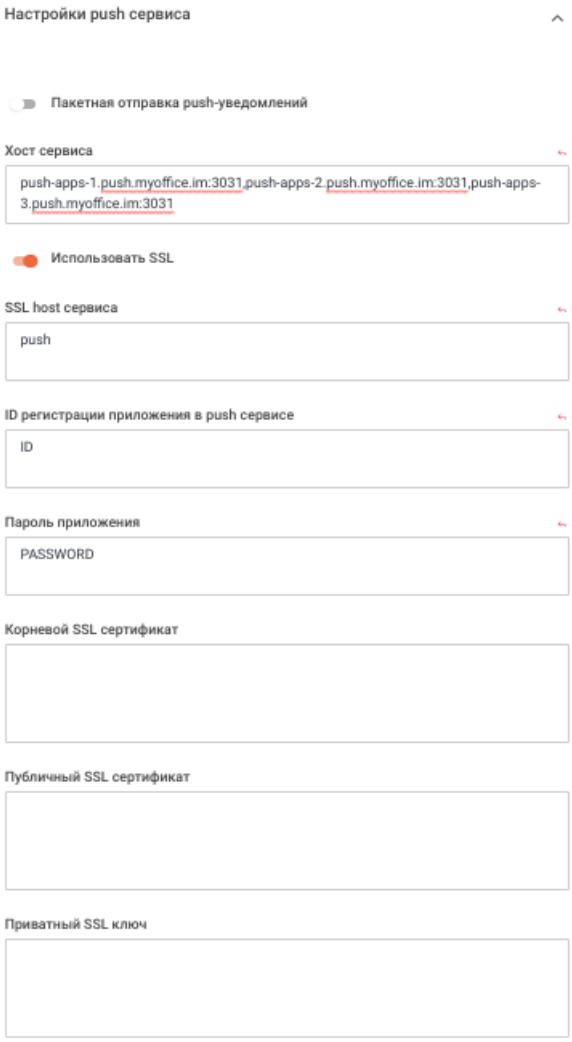

Рисунок 9 — Окно настройки push-сервиса

Таблица 14 — *Настройка полей push-сервиса*

Наименование поля	Примеры значений	Описание
Хост сервиса	push-apps-1.push.myoffice.im:3031, push-apps-2.push.myoffice.im:3031, push-apps-3.push.myoffice.im:3031	Список серверов push-proxy с указанием порта через двоеточие, разделенный запятой для отправки push-уведомлений
SSL-хост сервиса	push	Subject alternative name сертификата
ID регистрации приложения в push сервисе	-	ID для подключения
Пароль приложения	-	Пароль
Корневой SSL сертификат	-	Содержимое файла myoffice_ca.pem

Наименование поля	Примеры значений	Описание
Публичный SSL сертификат	-	Содержимое файла mycompany_client.crt
Приватный SSL ключ	-	Содержимое файла mycompany_client.nopass.key

После заполнения указанных полей необходимо нажать кнопку **Сохранить** в правом верхнем углу страницы.

5.5.2 Автоматическая настройка

Для настройки push-уведомлений в автоматическом режиме необходимо выполнить следующие действия:

1. Раскомментировать и изменить переменные, указанные в таблице 15.

Таблица 15 — Переменные для настройки push-уведомлений

Наименование переменной	Описание
myoffice_push_proxy_grpc_enabled	Включает режим проксирования к push-серверам через удаленный вызов процедур gRPC (значение true)
myoffice_push_grpc_proxy_endpoints	Список push-серверов
myoffice_push_proxy_tls_ca_filename	Сертификат центра сертификации, подписавшего используемые сертификаты
myoffice_push_proxy_tls_cert_filename	Клиентский сертификат для подключения к сервису push-уведомлений
myoffice_push_proxy_tls_key_filename	Ключ сертификата

2. Разместить полученные файлы в рабочей директории дистрибутива `certificates`.

3. Повторно запустить установку сервиса `squadus` с помощью команды:

```
[root@squadus_infra~]# ansible-playbook -i hosts.yml playbooks/main.yml\
 -l squadus_apps -t squadus
```

4. После завершения работы Ansible в административной панели ПО Squadus проверить применение настроек в соответствии с разделом «Ручная настройка».

5.5.3 Проверка работы сервиса

Для проверки необходимо выполнить следующие операции:

– перейти в чат с пользователем и совершить звонок;

– проверить телефон пользователя во время звонка на наличие push-уведомления.

Не используйте один и тот же логин пользователя при тестировании push-уведомлений. Отследить получение уведомлений с одним и тем же логином невозможно.

5.5.4 Устранение неполадок

При обновлении настроек push-proxy необходимо сохранить настройки и проверить работу push-уведомлений.

При отсутствии push-уведомлений следует перезапустить один из контейнеров группы `squadus_apps` для обновления и применения настроек.

Пример команды:

```
docker restart -t 120 squadus-1
```

5.6 Настройка виртуальной доски для совместного использования

В ПО Squadus реализована возможность использования виртуальной доски во время видеоконференций. Совместный доступ позволяет каждому участнику рисовать на виртуальной доске — процесс виден всем участникам в реальном времени. Результат можно сохранить в формате PNG или SVG непосредственно из конференции.

В данном релизе виртуальная доска не видна пользователям мобильных устройств.

Существует ограничение по одновременному использованию виртуальной доски — 20 пользователей.

5.6.1 Включение виртуальной доски

По умолчанию данная возможность отключена. Для включения необходимо выполнить следующие действия:

Задать переменной `excalidraw_whiteboard_enabled` значение `true` в файле `group_vars/squadus/main.yml`. Подробная информация приведена в разделе «Настройка дополнительных параметров установки».

```
excalidraw_whiteboard_enabled: true
```

Применить конфигурацию. Данное действие должно выполняться с подготовленного места оператора, которое должно соответствовать требованиям, описанным в разделе «Подготовка инфраструктуры установки».

```
ansible-playbook playbooks/squadus.yml --tags whiteboard --diff
```

После применения конфигурации в видеоконференциях появится возможность включения и совместного использования доски (рис. 10).

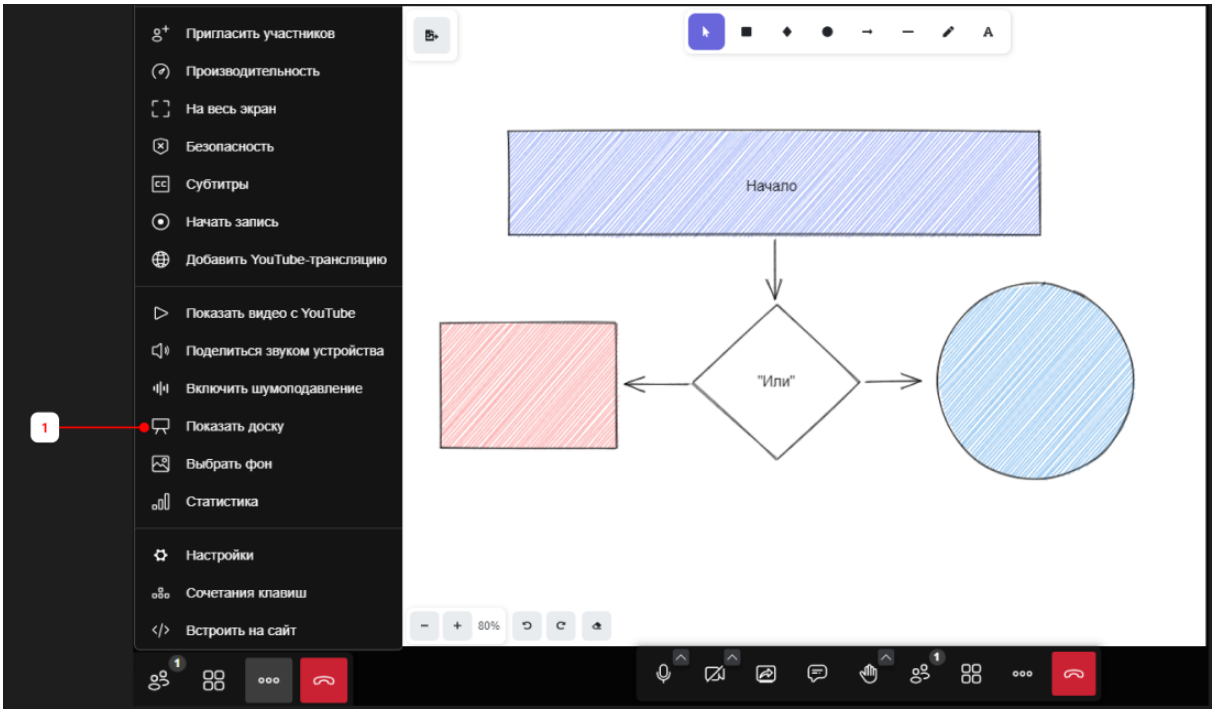

Рисунок 10 — Функция отображения доски для совместного использования

5.7 Настройка транскрибации речи (субтитры)

В ПО Squadus реализована возможность транскрибации аудиопотока видеоконференций в реальном времени. Такой режим позволяет распознавать речь участников и выводить результат в текстовом формате в окне конференции (рис. 11).

Включить данную функцию может любой участник конференции. Результат транскрибации виден только тому участнику, который включил данную функцию.

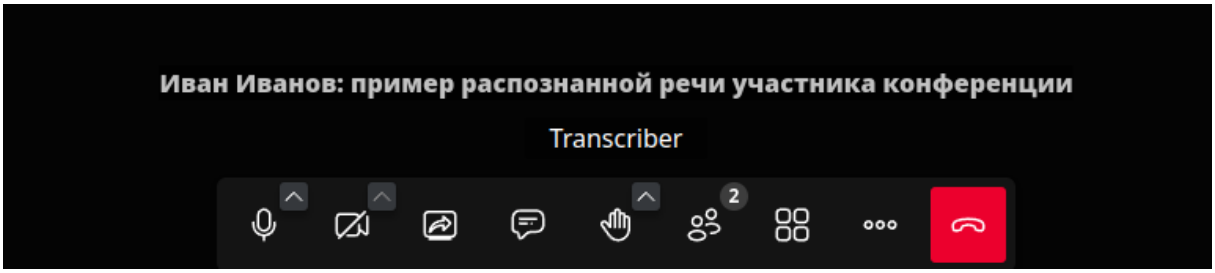

Рисунок 11 — Функция транскрибации

5.7.1 Системные требования

Модели для транскрибации являются высокоточными и могут использовать значительные ресурсы для функционирования. Рекомендуется использовать следующие параметры: не менее 4 vCPU и 16 Гбайт RAM для одной модели.

5.7.2 Включение транскрибации речи

По умолчанию транскрибация речи отключена. В текущей версии поддерживаются русский и английский языки. Но одновременно может использоваться только один из них.

Для установки модели для русского языка и включения транскрибации речи необходимо:

1. Предварительно загрузить в Docker-registry контейнеры языковых моделей из архивов. Архивы можно найти в поставке дистрибутива, в файлах-архивах `vosk_[LANG]_[X_X].tar`, где `[LANG]` — это идентификатор языка, а `[X_X]` — это версия ПО VOSK. Пример общего алгоритма загрузки приведен ниже:

```
      # загрузить образ файла-архива
      docker load -i vosk_ru_1_2.tar

      # поставить тег
      # предварительно заменить "docker_registry_fqdn" на актуальный fqdn хоста с Docker-registry, по умолчанию это "{{ groups['squadus_infra'][0] }}:5000"
      docker tag vosk-ru:1.2 docker_registry_fqdn/vosk-ru:1.2

      # выгрузить образ в Docker-registry
      docker push vosk-ru:1.2
```

2. В файле `inventory/group_vars/squadus/main.yml` задать переменной `vosk_enabled` значение `true`, а также определить переменную `vosk_hosts`.

```
      vosk_enabled: true
      vosk_hosts:
        vosk.example.net
          models:
            - language: "ru"
              listen_tcp_port: 2700
```

3. Добавить в файл inventory в раздел группы `squadus_meet_vosk` хост, на который планируется устанавливать модели VOSK.

```
      squadus_meet_vosk:
      hosts:
            vosk.example.net:
```

4. Применить конфигурацию:

```
      ansible-playbook playbooks/squadus.yml -t jicofo,jigasi,vosk,jitsiweb --diff
```

Для установки модели для английского языка, необходимо определить переменную `jitsiweb_transcription_preferred_language` со значением "en-US", а также задать переменной `vosk_hosts['vosk.example.net']['models'][0].language` значение `"en"`:


```
      jitsiweb_transcription_preferred_language: "en-US"
      vosk_enabled: true
      vosk_hosts:
        vosk.example.net
          models:
            - language: "en"
                listen_tc-p_port: 2700
```

5. Выполнить пункт 3 из раздела «Проверка работоспособности».

Для включения транскрибации необходимо в меню конференции выбрать пункт **Субтитры** (рис. 12), после чего появится одноименное модальное окно, в котором следует перевести переключатель в состояние **Вкл**.

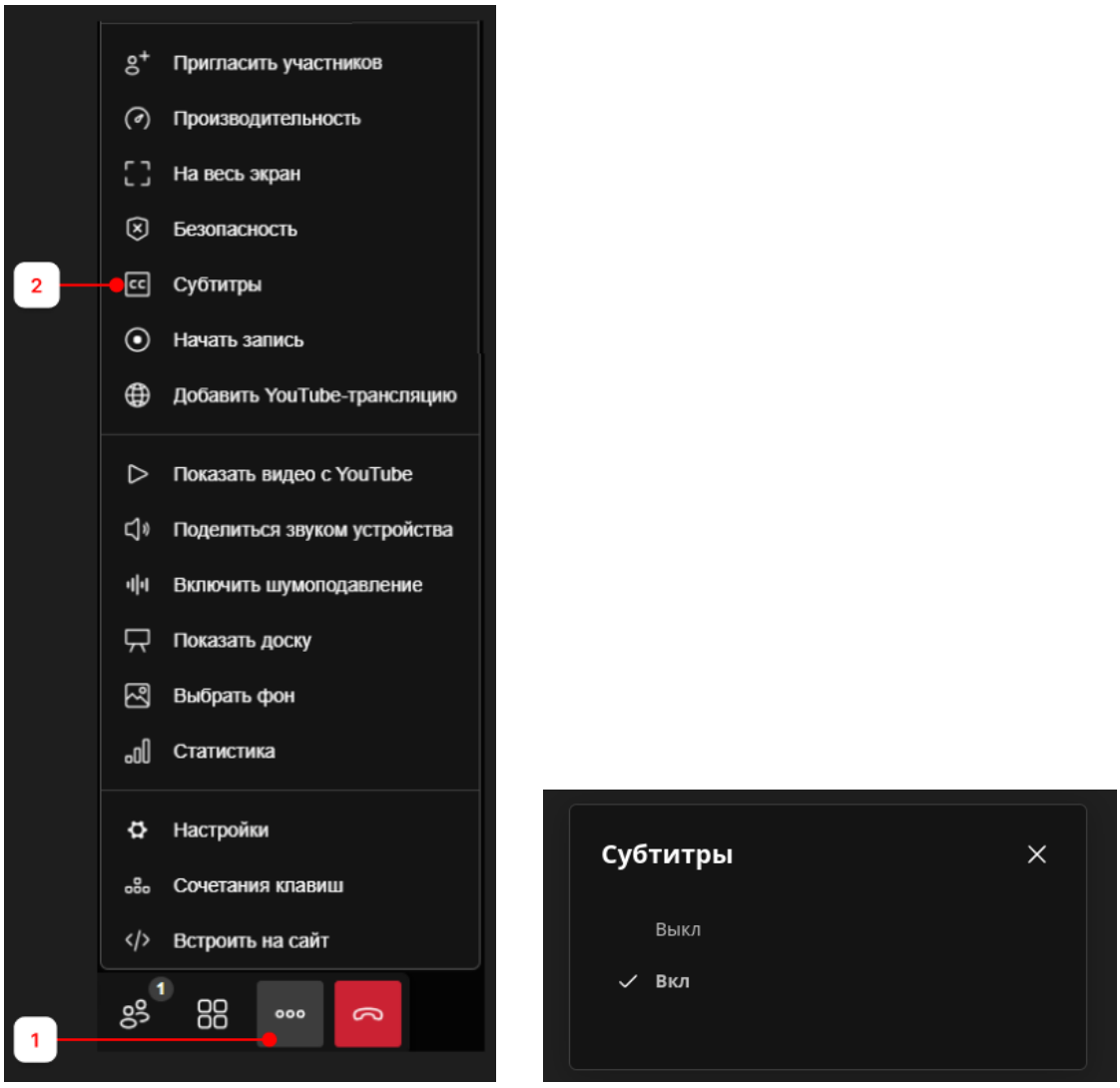

Рисунок 12 — Включение транскрибации

5.8 Режим федерации

5.8.1 Описание режима федерации

Режим федерации в Squadus — это возможность создавать комнаты/каналы между разными серверами Squadus и приглашать в комнаты пользователей из разных серверов. Взаимодействие серверов Squadus в режиме федерации основано на сервисе Matrix Synapse (который также может называться homeserver), и устанавливается на каждый сервер.

В качестве базы данных Matrix Synapse по умолчанию используется реляционная база данных с открытым кодом PostgreSQL. Squadus регистрируется как Application Service (служба приложений) в Matrix Synapse и взаимодействует с ним через Application Service API.

Все homeserver-серверы взаимодействует между собой через Server-Server API. Любое событие в федеративной комнате (отправка сообщения, реакция на сообщение, изменения названия комнаты, добавление нового пользователя и т.д.), произошедшее на одном сервере Squadus, проходит через эту цепочку и записывается в базу другого сервера Squadus.

Каждый аккаунт однозначно определяется логином и сервером, например, @alice:example.com. Комната определяется ее именем и сервером, например, #room:example.com. Matrix Synapse не хранит данные адреса почты, номера телефона, но хранит необратимые хеш-функции и осуществляет поиск именно по ним.

5.8.2 Настройка режима федерации

Для взаимодействия на сетевом уровне необходимо открыть доступ по протоколу TCP портам для входящего трафика, приведенным в таблице 16.

Таблица 16 — Порты для входящего трафика

Параметр	Описание	Тип	Значение по умолчанию
squadus_federation_bridge_int_port	Бридж порт для сервиса **squadus**	int	3300
synapse_client_int_port	Клиентский порт сервиса Synapse	int	8008
synapse_federation_int_port	Порт федерации сервиса Synapse	int	8448

Для установки Squadus в режиме федерации необходимо присвоить значения переменным, приведенным в таблице 17.

Таблица 17 — Переменные для настройки федераций

Параметр	Описание	Тип	Значение по умолчанию
squadus_postgresql_enabled	Включить установку базы данных PostgreSQL	bool	true
squadus_federation_enabled	Включить режим федерации Squadus	bool	true
synapse_ip_range_blacklist	Список запрещенных IP-адресов для приема сообщений	list	-
synapse_ip_range_whitelist	Список разрешенных IP-адресов для приема сообщений	list	-

Параметр	Описание	Тип	Значение по умолчанию
synapse_federation_domain_whitelist	Список разрешенных доменов для приема сообщений. Пример: im.example.com	list	-

Предварительно, необходимо установить библиотеку `psycopg2` (см. раздел «Программные требования»). Данная библиотека используется для управления конфигурацией сервиса базы данных PostgreSQL.

Для применения настроек на ранее подготовленном стенде следует запустить команду:

```
ansible-playbook playbooks/squadus.yml --tags federation --diff
```

5.9 Настройка отправки копий логов на внешний сервер

В Squadus реализована функция отправки копий логов на сторонний сервер в уже существующей системе заказчика. Настройка функции выполняется в следующем порядке:

1. Для настройки подключения необходимо в файле `~install_squadus/group_vars/squadus/main.yml` указать значения переменным, перечисленным в таблице 18.

Таблица 18 — Настройка отправки логов на сторонний сервер

Наименование переменной	Тип	Значение	Описание
syslog_ng_external_collector_ hostname	str	-	IP-адрес или домен стороннего сервера сбора логов
syslog_ng_external_port_ remote	int	-	Порт стороннего сервера сбора логов
syslog_ng_external_tier_send_ remote	bool	true / false (по умолчанию)	Включение/отключение функции отправки логов на сторонний сервер

Примечание — при отсутствии перечисленных в таблице 19 переменных следует добавить их вручную в файле `~install_squadus/group_vars/squadus/main.yml`.

2. После выбора сервиса необходимо в файле `~install_squadus/group_vars/squadus/main.yml` добавить переменную `external_collector:` со значением `true`.

Пример:

```
      syslog_ng_services:
...
  squadus_apps:
    argon: {}
    bohrium: {}
    boron: {}
...
    praseodymium: {}
    sodium: {}
    squadus:
      programm_name: "squadus-.*"
      external_collector: true
    squadus_jiratrigger: {}
    tennessine: {}
```

3. Для внесения изменений и запуска сервиса в новой системе после изменений файла `~install_squadus/group_vars/squadus/main.yml` необходимо выполнить установку системы в соответствии с разделом «Запуск установки».

5.10 Подключение к мониторингу

Для подключения к сервису мониторинга Grafana следует использовать параметры, указанные в таблице 19.

Таблица 19 — Параметры подключения к сервису мониторинга

Параметр	Значение
Адрес подключения	http://{{ `grafana_domain` }}
Имя пользователя	admin (по умолчанию)
Пароль	значение переменной `grafana_admin_password`

Значение переменной адреса подключения формируется следующим образом: `grafana_domain: "grafana.{{ groups['squadus_infra'][0] }}"`

А-запись для FQDN должна указывать на IP-адрес сервера группы ролей `squadus_infra`

5.11 Добавление стороннего корневого сертификата

В ПО Squadus реализована функция добавления стороннего корневого сертификата (далее — CA). Под сторонними подразумеваются самоподписанные CA или CA, полученные от третьих лиц.

Для работы с функцией необходимо открыть файл `~install_squadus/group_vars/squadus/main.yml` и в директории `install_squadus` указать значения переменным, представленным в таблице 20.

Таблица 20 — Добавление стороннего корневого сертификата

Наименование переменной	Тип переменной	Значение	Описание
prosody_extra_ca_enabled	boolean	true / false (по умолчанию)	Включение/ отключение функции поддержки сторонних CA
prosody_extra_tls_ca_directory	string	"/path/to/directory"	Директория, содержащая сторонние CA файлы в формате *.crt

Примечание — при отсутствии перечисленных в таблице 21 переменных следует добавить их вручную в файл `~install_squadus/group_vars/squadus/main.yml`.

Внесение изменений в существующей системе выполняется для подсистемы prosody с помощью команды:

```
ansible-playbook playbooks/squadus.yml -t prosody --diff -i hosts.yml
```

Для внесения изменений и запуска сервиса в новой системе после изменений файла `~install_squadus/group_vars/squadus/main.yml` необходимо выполнить установку системы в соответствии с разделом «Запуск установки».

5.12 Настройка межсетевого экранирования

Во время установки происходит настройка межсетевого экрана внутри контура системы. Необходимо обеспечить дополнительную защиту системы с внешней стороны системы (по отношению к контуру) (табл. 21).

Таблица 21 — Настройка межсетевого экранирования

Порт	Сервер с ролью	Примечание
80/tcp	squadus_ha	
443/tcp	squadus_ha	
4096/udp	squadus_meet_jvb	
10000/udp	squadus_meet_jvb	
3478[tcp|udp]	первый сервер группы squadus_meet_jvb	для работы turnserver
49152:65535/udp		
7443		SSL WebSocket порт для FreeSwitch

Остальные порты должны быть запрещены.

5.13 Настройка службы синхронизации времени NTP

Настройка синхронизации времени выполняется автоматически при применении `playbook-a playbooks/common.yml` в соответствии с разделом «Настройка дополнительных параметров установки». При необходимости пул NTP серверов можно переопределить с помощью переменной `ntp_servers`.

Необходимо учитывать, что корректная работа системы синхронизации времени крайне важна для корректной работы ПО Squadus. Стоит убедиться, что используемые NTP серверы доступны по UDP-порту 123 со всех узлов установки.

5.14 Централизованная установка настольных приложений

Централизованная установка настольного приложения Squadus для всех пользователей компьютера выполняется администратором. Такой тип установки использует дополнительное ПО SCCM (System Center Configuration Manager). Пользователь SCCM с ролью «Администратор» обладает правами на создание пакетов установок и распространение их содержимого на рабочие станции пользователей.

ПО разворачивается с помощью установщика msi "для всех пользователей" посредством обычной установки, с аргументом `MSIINSTALLPERUSER=""`.

Пример команды:

```
msiexec /i "SquadusMsiPath" /qn MSIINSTALLPERUSER=""
```

5.15 Настройка интеграции с DLP

По умолчанию интеграция с DLP отключена. Для включения интеграции необходимо выполнить следующие действия:

1. Задать переменной `zirconium_enabled` значение `true` в файле `group_vars/squadus_setup/extra_vars.yml`

Пример переменной в файле:

```
zirconium_enabled: true
```

2. Применить конфигурацию на сервере с ролью `operator`, выполнив команду:

```
ansible-playbook playbooks/squadus.yml --tags zirconium --diff
```

3. Включить и настроить интеграцию согласно документу «Руководству по администрированию».

5.16 Настройка postfix

Squadus отправляет почту с помощью MTA Postfix. Для отправки используется relayhost, представляющий собой адрес пограничного шлюза. Для настройки необходимо указать значения переменным, представленым в таблице 22.

Таблица 22 — Переменные для настройки postfix

Параметр	Описание	Тип	Значение по умолчанию
postfix_relayhost	IP-адрес сервера-ретранслятора	Str	"10.7.97.13"
postfix_relayhost_port	Порт сервера-ретранслятора	Int	25

Дополнительно потребуется настройка для сервиса подписывания DKIM.

Для создания DNS-записи вида `mail.domainkey.im.example.net` на сервере с ролью `operator` следует выполнить команду:

```
opendkim-genkey -s im.example.net -d im.example.net && cat
im.example.net.private
```

ПРИЛОЖЕНИЕ А

Порядок установки и настройки локального репозитория

1. Создать каталог для размещения репозитория с помощью команды:

```
sudo mkdir -p /srv/repo/alse/main
```

2. Примонтировать образ установочного диска (если на компьютере нет каталога /media/cdrom — то создать каталог /media/cdrom) с помощью команды:

```
[ -d /media/cdrom ] || sudo mkdir /media/cdrom
sudo mount /путь_к_ISO-образу /media/cdrom
```

3. Скопировать файлы из образа в каталог репозитория с помощью команды:

```
sudo cp -a /media/cdrom/* /srv/repo/alse/main
```

4. Отмонтировать ISO-образ диска с помощью команды:

```
sudo umount /media/cdrom
```

4.1 Если требуется, выполнить аналогичные действия для базового репозитория (диска со средствами разработки) с помощью команды:

```
sudo mkdir -p /srv/repo/alse/base
[ -d /media/cdrom ] || sudo mkdir /media/cdrom
sudo mount /путь_к_ISO-образу /media/cdrom
sudo cp -a /media/cdrom/* /srv/repo/alse/base
sudo umount /media/cdrom
```

5. Для обновления основного репозитория (основного диска) с помощью команды:

```
sudo mkdir -p /srv/repo/alse/update-main
[ -d /media/cdrom ] || sudo mkdir /media/cdrom
sudo mount /путь_к_ISO-образу /media/cdrom
sudo cp -a /media/cdrom/* /srv/repo/alse/update-main
sudo umount /media/cdrom
```

6. Для обновления базового репозитория (диска с обновлением средств разработки) с помощью команды:

```
sudo mkdir -p /srv/repo/alse/update-base
[ -d /media/cdrom ] || sudo mkdir /media/cdrom
sudo mount /путь_к_ISO-образу /media/cdrom
sudo cp -a /media/cdrom/* /srv/repo/alse/update-base
sudo umount /media/cdrom
```

ПРИЛОЖЕНИЕ Б

Замена стандартного репозитория на локальный

Замена стандартного репозитория на локальный выполняется на сервере с ролью `operator`. Перечисленный порядок действий используется в ОС Astra. Для замены репозитория необходимо:

1. Отключить внешние репозитории, запустив команду:

```
sed –i "s/^/#/" /etc/apt/sources.list
```

2. Добавить локальный внешний репозиторий, запустив команду:

```
tee –a /etc/apt/sources.list << EOF
deb http://$IP_ADDRESS:8081/repository/astra/ 1.7_x86-64 \
main contrib non-free
deb http://$IP_ADDRESS:8081/repository/astra-ext/ 1.7_x86-64 \
main contrib non-free
EOF
```

где `$IP_ADDRESS` — IP-адрес локального сервера для хранения файлов.

3. Обновить индекс репозитория, запустив команду:

```
apt update
```

4. Проверить доступность репозитория (произвести поиск произвольного пакета), запустив команду:

```
apt search pwgen
```

5. Убедиться, что в выводе команды присутствует название пакета pwgen. Вывод команды:

```
root@operator:~# apt search pwgen
Sorting... Done
Full Text Search... Done
pwgen/stable 2.08-1 amd64
Automatic Password generation
root@operator:~#
```

6. Настроить менеджер модулей (pip) на использование локального репозитория, запустив команду:

```
tee /etc/pip.conf << EOF
[global]
trusted-host = $IP_ADDRESS
index = http://$IP_ADDRESS:8081/repository/pypi-proxy/pypi
index-url = http://$IP_ADRESS:8081/repository/pypi-proxy/simple
EOF
```

где `$IP_ADDRESS` — IP-адрес локального сервера для хранения файлов.

ПРИЛОЖЕНИЕ В

Настройка сетевых соединений

Пример настройки сетевого соединения с помощью командной строки в ОС Astra.

1. Для проверки необходимо открыть файл с сетевыми настройками с помощью команды:

```
nano /etc/network/interfaces
```

В открывшемся окне редактора проверить наличие следующей строки:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*
```

1.1 Закрыть окно и вернуться к строке терминала.

1.2 Создать новое соединение с помощью команды:

```
sudo nano /etc/network/interfaces.d/eth0
```

Примечание: если на вашем сервере установлены другие редакторы (vim, vi) замените в команде `nano` на другой редактор.

2. В открывшемся окне редактора в зависимости от типа используемого для настроек ввести команду из пункта 2.1 или 2.2.

2.1 При использовании статического IP-адреса необходимо ввести:

```
echo "auto eth0
iface eth0 inet static
address 192.168.1.100
netmask 255.255.255.0
gateway 192.168.1.1" > /etc/network/interfaces.d/eth0
```

В примере используются произвольные настройки сетевого соединения. Необходимо заменить предложенные настройки (192.168.1.100, 255.255.255.0, 192.168.1.1) на настройки сетевого окружения созданных серверов.

2.2 При использовании DHCP в окне редактора необходимо ввести:

```
echo "auto eth0
iface eth0 inet dhcp" > /etc/network/interfaces.d/eth0
```

Для корректной работы необходимо закрепить IP-адреса за серверами с помощью настроек DHCP-сервера вашего шлюза (коммутатора).

3. После ввода переменных файл сохранить. Повторно открыть файл командой из пункта 1 для проверки.

4. Задать DNS-сервер

```
echo "nameserver 8.8.4.4" > /etc/resolv.conf
```

Адрес DNS-сервера 8.8.4.4 указан произвольно, если в локальной сети существует внутренний DNS-сервер, необходимо изменить адрес 8.8.4.4.

5. Применить настройки сетевого соединения

```
sudo systemctl restart networking
```

Повторить выполнение действия для каждого сервера, используемого для установки.

ПРИЛОЖЕНИЕ Г

Порядок создания самоподписанного сертификата

По умолчанию браузеры не доверяют самоподписанным сертификатам, рекомендуется использовать его только для внутренних целей или в целях тестирования.

1. Проверка или установка OpenSSL.

OpenSSL доступен по умолчанию во всех основных дистрибутивах Linux.

Для поиска установленного ПО OpenSSL и проверки версии необходимо выполнить команду:

```
$ openssl version
```

Если вывод с информацией о версии OpenSSL отсутствует — программа не установлена.

Для установки OpenSSL выполните следующую команду:

```
$ sudo dnf install openssl
```

или

```
$ sudo yum install openssl
```

Выбор команды зависит от типа ОС.

2. Создание SSL-сертификата.

Для создания самоподписанного сертификата SSL необходимо использовать следующую команду:

```
$ openssl req -x509 -nodes -days 365 -newkey rsa:4096 -keyout
server.nopass.key -out server.crt
```

С помощью команды будет создан самоподписанный сертификат, который будет действителен в течение 365 дней.

По умолчанию сертификат и файл ключа будут созданы в текущем каталоге (в каталоге, из которого выполняется команда).

Описание флагов использованных в команде приведено в таблице 23.

Таблица 23 — *Значения флагов команды*

Флаг	Описание
req	Выполнить запрос на подпись сертификата
-newkey rsa:4096	Создать ключ RSA длиной 4096 бит. Если не указано иное, по умолчанию будет создан ключ длиной 2048 бит
-keyout	Указать имя файла для хранения закрытого ключа
-out	Указать имя файла для хранения нового сертификата
-nodes	Пропустить шаг по созданию сертификата с парольной фразой
-x509	Создать сертификат формата X.509
-days	Указать время действия сертификата в днях

Описание полей при создании сертификата приведено в таблице 24.

Таблица 24 — Значения полей CSR

Поле	Описание
C =	Название страны (двухбуквенный код)
ST =	Название штата или провинции
L =	Название населенного пункта
O =	Полное название вашей организации
OU =	Название организационной единицы
CN =	Полное доменное имя

3. Создание закрытого ключа.

Закрытый ключ необходим для подписи вашего SSL-сертификата. Для создания и сохрания закрытого ключа необходимо выполнить команду:

```
$ openssl genrsa -out server.nopass.key
```

Значения флагов команды:

– `genrsa` — создать закрытый ключ RSA;

– `-out` — выходной файл.

По умолчанию закрытый ключ будет храниться в текущем каталоге (в каталоге, из которого выполняется команда).

4. Создание запроса на подпись сертификата (CSR).

CSR — информация, отправляемая в удостоверяющий центр. Для создания CSR необходимо выполнить следующую команду:

```
$ openssl req -new -key server.nopass.key -out server.csr
```

Описание флагов использованных в команде приведено в таблице 25.

Таблица 25 — Значения флагов команды

Флаг	Описание
req	Запрос на подпись сертификата
-new	Новый запрос
-key	Путь, где хранится ваш файл закрытого ключа
-out	Имя выходного файла

После запуска команды, представленной ниже, будет создан самоподписаный сертификат, который будет действителен в течение 365 дней.

```
$ openssl x509 -req -days 365 -in server.csr -signkey server.nopass.key \
-out server.crt
```

5. Проверка деталей сертификата выполняется с помощью команды:

```
$ openssl x509 -text -noout -in server.crt
```

ПРИЛОЖЕНИЕ Д

Пример параметров файла main.yaml

Пример корректно настроенных параметров:

```
ansible_user: "root"
jibri_recorder_password: "eChuoNgae0Ohz1ihahmoichu4heeshu4"
jibri_auth_password: "aCeephaobahjeexeWei0Aa8ceeboegiu"
jicofo_auth_password: "concentrationcompensationgivesreed"
jicofo_component_secret: "ieH1iedaejai0ob9piC1faeGhiel2ahM"

jitsi_jwt_secret: "aishi8ceYi6peid1Yeemaawahb2ve7we"
jitsi_jwt_app_id: "meet"
jitsi_main_domain: "meet.example.net"
jitsi_use_keepalived: false

jvb_auth_password: "solelyafternoonattorneyssomewhere"
jvb_component_secret: "moopheh1aixohcaequai5go4Awee4ou7"

manganum_mongodb_password: "{{ squadus_mongodb_password }}"

minio_access_key: "thi1shogeuThu0sheeShooqueukur8Ae"
minio_secret_key: "neecien8Gah0iudoh6Ooloong5oopaem"
mongodb_root_password: "processionmerryrapidmessage"
mongodb_secured_key: "elephantwisdomexceptionuse"

redis_password: "rakeproposebowpupilvirtue"

squadus_jitsi_enabled: true
squadus_domain: "example.net"
squadus_mongodb_password: "illegalongoingsurvivedesignation"
squadus_use_keepalived: false
scandium_mongodb_password: "chopohYuicoo2moo2uuphev2iechae4E"
scandium_squadus_jwt_secret: "chaevieT0oiz3ifoocev3eevainei4om"

tennessine_mongodb_password: "{{ squadus_mongodb_password }}"

tls_ca_filename: "ca.pem"
tls_cert_filename: "server.crt"
tls_key_filename: "server.nopass.key"
turnserver_cli_password: "RcBaN5mKibWe25h6NWiN"
turnserver_secret: "oogieyahneiBienei8ey"

zinc_mongodb_password: "{{ squadus_mongodb_password }}"—
```