ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

Программное обеспечение

«МойОфис Комплект Средств Разработки (SDK)»

Сервер совместного редактирования

3.6

Руководство по установке

На 99 листах

Версия документа: 1

Дата публикации: 25.11.2025

Москва
2025

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

Товарные знаки «МойОфис» и «MyOffice» 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

В настоящем документе применяют следующие сокращения с соответствующими расшифровками (табл. 1).

Таблица 1 — Сокращения и обозначения

Сокращение, термин	Расшифровка и определение
API	Application Programming Interface, интерфейс программирования приложений
Auth SSO	Single Sign-On, подсистема единого входа (аутентификации и авторизации)
CA	Certificate Authority, удостоверяющий центр для подтверждения подлинности ключей шифрования
CDN	Content Delivery Network, сеть доставки содержимого (в данном случае одна из ролей Auth SSO сервера)
CO	Система редактирования и совместной работы
CU	Converter Unit, сервис конвертирования разных форматов файлов
DNS	Domain Name System, система доменных имен
DU	Document Unit, синоним DCS
ETCD	Распределенная система хранения конфигурации
FCM	Firebase Cloud Messaging, сервис уведомлений мобильных приложений Google, ранее назывался GCM
FQDN	Fully Qualified Domain Name, полностью определенное имя домена
GCM	Google Cloud Messaging, сервис нотификаций мобильных приложений Google, заменен сервисом FCM
Inventory	Файл, содержащий набор управляемых хостов для автоматизации установки и управления конфигурацией для сервиса Ansible
PGS	Система хранения данных
SMTP	Simple Mail Transfer Protocol, протокол передачи почтовых сообщений
SSH	Secure Shell, «безопасная оболочка»
UI	User Interface, пользовательский интерфейс
URL	Uniform Resource Locator, единый указатель ресурса
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
УЦ	Удостоверяющий центр

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

«Сервер совместного редактирования (ССР)» — интегрируемая серверная система и клиентские веб-приложения, предназначенные для просмотра и совместного редактирования текстовых и табличных документов в прикладных ИТ-системах. Сервер встраивается в хранилища сторонних производителей, поддерживающих возможность взаимодействия с внешними клиентами по протоколу WOPI.

Данное решение предоставляет возможность открыть документ из внешнего хранилища документов на просмотр или редактирование в iframe и при необходимости сохранять редактируемый документ обратно в хранилище. В качестве примера интеграции было использовано хранилище NextCloud (гарантируется работоспособность на версии 26) с включенным расширением OfficeOnline (рис. 1).

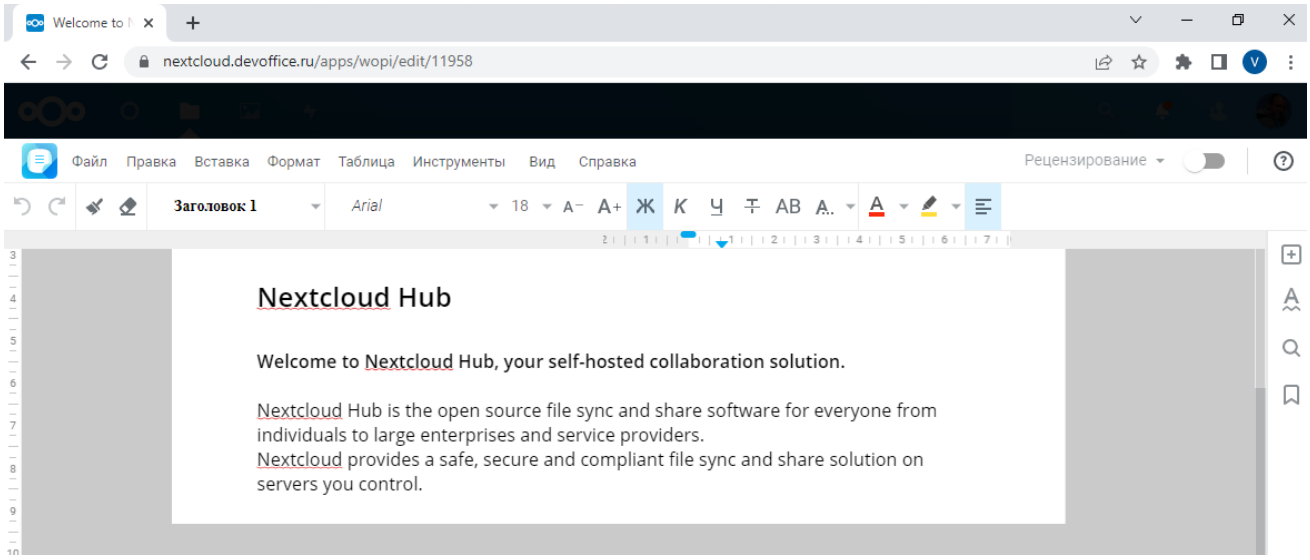

Рисунок 1 — Открытие документа в хранилище NextCloud

1.2 Перечень изменений с обновлением версии

Изменения в версии 3.6

1. Добавлена возможность настройки Keepalived + HAProxy для обеспечения отказоустойчивости и высокой доступности сервиса. По умолчанию данный функционал выключен.
2. Добавлена возможность запустить установку с очисткой только серверных компонентов (компонентов внутренней разработки). Для включения следует определить переменную `cleanup_srv_containers: true` в `group_vars/co_setup/main.yml`, либо запустить установку с аргументом `-e '{"cleanup_srv_containers": true}'`.
3. Добавлена возможность запуска дополнительной проверки, позволяющее на ранней стадии выявить наличие проблем, которые могут помещать успешному завершению установки продукта. Проверка наличия и валидности TLS сертификатов — выполняется по умолчанию.
4. Устранена проблема при загрузке статических файлов, в результате которой CDN-манифесты, хранящихся в ETCD содержали некорректные ссылки.
5. Добавлена возможность принудительной повторной загрузки статических файлов. Для включения функциоанала следует добавить переменную `bundles_upload_force_install: true` в `group_vars/co_setup/main.yml`, либо запустить установку с аргументом `-e '{"bundles_upload_force_install": true}'`. Если фукция не активна, при повторном запуске установки, загруженные ранее статические файлы будут пропущены.
6. Конфигурация Redis переведена на использование aclfile, в котором хранится информация о default пользователе. Устранены проблемы в автоматизации установки Redis, приводившие к ошибкам при запуске установки продукта повторно.
7. Значение переменных `co_domain_module` и `co_external_domain` формируется автоматически на основе значений переменных `domain_env` и `domain_name`. Переменные `co_domain_module` и `co_external_domain` исключены из файла `group_vars/co_setup/main.yml`.
8. Добавлен мониторинг состояния сервисов продукта с помощью blackbox exporter. В Grafana был создан панель «[DO] CO Service Status», для контроля состояния сервисов.

1.3 Описание архитектуры

Общая архитектурная схема для Сервера совместного редактирования (далее — ССР) приведена на рисунке 2.

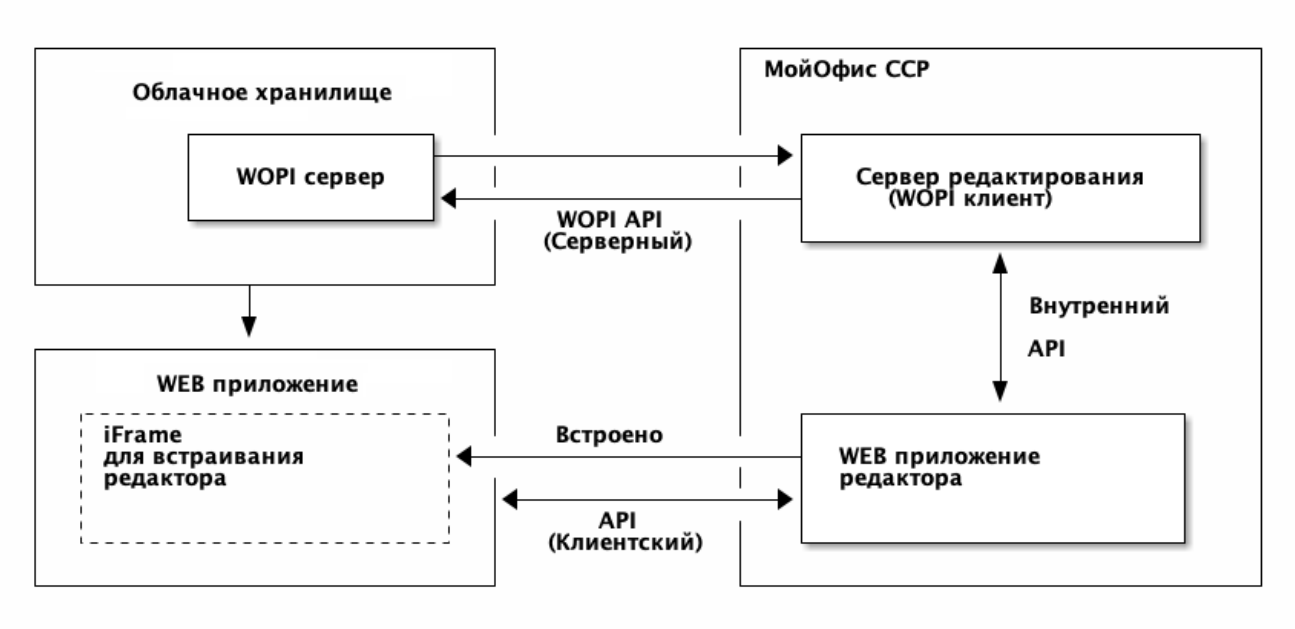

Рисунок 2 — Общая архитектурная схема ССР

1.4 Состав дистрибутива

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

– исполняемый файл co_ansible_bin_3.6-ces.run, предназначенный для установки подсистемы управления конфигурациями;
– исполняемый файл co_infra_3.6-ces.run, предназначенный для установки хранилища образов Docker.

1.5 Программные и аппаратные требования

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

1.6 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.
2. Работа с подсистемой виртуализации:
   - 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. Работа с системой автоматизации развертывания Ansible.
7. Практический опыт администрирования на уровне эксперта:

- СУБД ArangoDB;
- файловой системы GlusterFS;
- SSO-сервиса Keycloak;
- СУБД PostgreSQL;
- поисковой системы Elasticsearch;
- Redis;
- обработчика сообщений RabbitMQ;
- сервера конфигурации ETCD.

1.7 Типовые схемы установки

Структура сервиса может быть представлена двумя типами установки:

– standalone (на один виртуальный сервер или на несколько виртуальных серверов в рамках одного физического сервера);
– кластерная (все роли устанавливаются на разные виртуальные или физические серверы).

1.7.1 Standalone

Конфигурация без отказоустойчивости используется для разработки или демонстрации возможностей продукта.

Установка в минимальной конфигурации использует три сервера:

– сервер с ролью `operator` для управления процессом установки;
– сервер с ролью `co` для установки редакторов и дополнительного ПО;
– сервер NextCloud для размещения и хранения базовых библиотек и файлов.

1.7.2 Кластерная установка

Отказоустойчивая конфигурация, используемая для типовой установки продукта.

Для сохранения уровня отказоустойчивости не рекомендуется совмещать серверные роли между собой. Совмещение допускается в отдельных случаях для экономии ресурсов.

2 ПОДГОТОВКА К УСТАНОВКЕ

2.1 Подготовка ОС

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

Для установки на ОС Astra необходимо выполнить операции, изложенные в разделе «Конфигурирование ОС Astra Linux».

2.1.1 Конфигурирование ОС Astra Linux

2.1.1.1 Уровни защиты

Основные отличия между вариантами защищенности ОС Astra Linux SE 1.7 приведены в таблице 1.

Таблица 1 — Уровни защищенности ОС Astra Linux SE 1.7

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 — ОС Astra Linux SE 1.7 «Орел»;
– Усиленный уровень — ОС Astra Linux SE 1.7 «Воронеж»;
– Максимальный уровень — ОС Astra Linux SE 1.7 «Смоленск»

Текущий уровнень 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
on /
```

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
```

2.1.1.2 Настройка усиленного уровня защищенности («Воронеж»)

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

1. Пользователю astra необходимо установить максимальный уровень целостности — 63 (соответствует администратору ОС). Для проверки уровня целостности пользователя необходимо выполнить следующую команду:

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

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

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

3. Установка Ansible и работа PGS невозможна при включенном режиме замкнутой программной среды. Для проверки статуса режима необходимо выполнить следующую команду:

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

4. При статусе ACTIVE перед началом установки на всех серверах следует выполнить команды:

```
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 2.

Таблица 2 — 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
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`.

2.1.1.3 Работа с репозиториями Astra

После установки ОС Astra для предотвращения установки обновлений несовместимых с текущей версией продукта рекомендуется переключить используемый репозиторий.

Stable-репозиторий, использующийся при установке ОС, не содержит предыдущие версии пакетов и содержит только последние версии пакетов текущей версии ОС. Для использования ранних версий пакетов следует переключить используемый stable-репозиторий на frozen-репозиторий.

Уточнить текущую версию ОС можно с помощью команды:

```
cat /etc/astra/build_version
```

Пример ответа:

```
1.8.1.16
```

Для проверки текущего репозитория следует выполнить команду:

```
cat /etc/apt/sources.list
```

Пример ответа:

```
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-extended/
1.8_x86-64 main contrib non-free non-free-firmware
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-main/
1.8_x86-64 main contrib non-free non-free-firmware
```

Порядок действий по изменению репозитория:

1. Открыть на сайт производителя ОС и найти актуальный для вашей версии frozen-репозиторий. Для версии ОС Astra Linux 1.8 страница с репозиториями https://wiki.astralinux.ru/pages/viewpage.action?pageId=302043111

2. Открыть файл `/etc/apt/sources.list` с помощью текстового редактора и заменить stable-репозиторий на frozen-репозиторий.

Пример файла с frozen-репозиторием:

```
deb https://download.astralinux.ru/astra/frozen/1.8_x86-64/1.8.1/uu/1/\
extended-repository/ 1.8_x86-64 main non-free non-free-firmware contrib
deb https://download.astralinux.ru/astra/frozen/1.8_x86-64/1.8.1/uu/1/\
main-repository/ 1.8_x86-64 main contrib non-free non-free-firmware
```

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 сервера с ролью operator

2.3.1 Установка ОС и 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.

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.

Все скрипты, запускаемые в процессе подготовки, следует выполнять от имени пользователя `root`. При запуске скриптов от другого пользователя, скрипты необходимо выполнять без sudo, за исключением запуска `co_infra.run`.

При запуске скриптов от другого пользователя с использованием sudo создаваемые каталоги `install_co` и `venv` отправятся в домашнюю директорию `root`.

2.3.2 Установка подсистемы управления конфигурациями

Установка выполняется на сервере с ролью operator. Порядок действий при установке:

1. Скопировать файл co_ansible_bin_3.6-ces.run в корневую директорию пользователя (где 3.6-ces — имя версии).

2. Запустить скрипт установки:

```
bash co_ansible_bin_3.6-ces.run
```

3. Дать согласие на продолжение установки, нажав на клавишу «Y». Пример запроса:

```
Do you want to continue?      [y/N] y
```

4. После завершения установки на экране пользователя будет отображен список выполненных операций и сообщения. Необходимо убедиться, что список содержит сообщения `[ OK ]` или `[CHANGE]` — это свидетельствует об успешной установке.

При получении сообщения `[FAIL]` необходимо обратиться в техническую поддержку.

После выполнения скрипта установки будет создана директория `~/install_co`.

2.3.3 Автоматическая установка дополнительного ПО

Установка дополнительного ПО может быть выполнена автоматически с помощью скрипта установки venv_setup.sh, расположенного в директории `~/install_co/contrib`.

Для запуска автоматической установки необходимо выполнить команду:

```
bash ~/install_co/contrib/venv_setup.sh
```

После выполнения скрипта будет создана директория `~/venv`. Для использования директории следует выполнить команду:

```
source ~/venv/bin/activate
```

Все последующие операции, связанные с ПО Python и Ansible, необходимо выполнять с включенной директорией `~/venv`.

2.3.4 Установка в сети без выхода в интернет

2.3.4.1 Общие требования

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

Для установки продукта в локальной сети, без прямого выхода в интернет, необходимо на сервере с ролью operator и целевых серверах обеспечить:

– доступность всех стандартных репозиториев ОС или их зеркал во внутренней сети для установки ПО.

– обеспечить доступность репозиториев pip или их зеркал в локальной сети.

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`.

2.3.4.2 Подготовка к установке на ОС Ubuntu в сети без выхода в интернет

Для установки продукта на ОС Ubuntu в сети без выхода в интернет необходимо на сервере с ролью operator и целевых хостах обеспечить доступ к репозиториям Docker (https://download.docker.com/linux/ubuntu/) или зеркалу в локальной сети.

Пакеты ПО Docker устанавливаются из репозиториев ОС для всех поддерживаемых ОС, кроме Ubuntu 22.04.

При установке на ОС Ubuntu в закрытой сети без доступа к https://download.docker.com/linux/ubuntu/ нужно переопределить переменные репозитория Docker и его ключа GPG.

> Для других ОС установка пакетов docker будет выполнена из стандартных репозиториев операционных систем (их зеркал).

Порядок подготовки ОС Ubuntu:

1. Подготовка сервера с ролью operator.

При запуске `co_infra_3.6.run` необходимо указать дополнительные параметры. Пример команды:

```
bash co_infra_3.6.run -- --docker-custom-repo --docker-custom-repo-url \
"deb [arch=amd64] https://<docker-custom-repo-address>/docker/ jammy stable" \
--docker-custom-repo-gpgkey "https://<docker-custom-repo-address>/docker/gpg"
```

где:

- `--` — передача последующих аргументов встроенному исполняющему скрипту.
- `--docker-custom-repo` — ключ, указывающий применить значения последующих параметров
- `--docker-custom-repo-url` — значение указывается в кавычках, имеет формат полной строки, описывающей репозиторий для скачивания пакетов docker. Строка будет записана в новый файл `/etc/apt/sources.list.d/docker-custom-ce.list`
- `--docker-custom-repo-gpgkey` — значение указывается в кавычках, URL для скачивания GPG ключа репозитория.

2. На целевые сервера других ролей устанавливается ПО Docker. Для ОС Ubuntu необходимо обеспечить доступ к стандартным репозиториям Docker (https://download.docker.com/linux/ubuntu/) или зеркалу в локальной сети.

При использовании собственного репозитория с пакетами docker в файл `install_co/group_vars/co_setup/main.yml` следует добавить следующие переменные:

```
docker_custom_repo_url: "deb [arch=amd64] https://<docker-custom-repo-address>/
jammy stable"
docker_custom_repo_gpgkey: "https://<docker-custom-repo-address>/gpg"
```

Переменные указываются в формате, аналогичном аргументам в пункте 1 настоящего раздела, и содержат одинаковые значения. При выполнении установки на каждый сервер будет добавлен собственный репозиторий и пакеты Docker будут устанавливаться из него.

2.3.5 Установка хранилища образов Docker

Установка выполняется на сервере с ролью operator. Порядок действий при установке:

1. Скопировать файл co_infra_3.6-ces.run на сервер с ролью operator (где 3.6 — имя версии).
2. Запустить скрипт установки:

```
bash co_infra_3.6-ces.run
```

3. Дождаться проверки целостности файла и его распаковки.

Пример вывода:

```
Verifying archive integrity...      100%        MD5 checksums are OK. All good.
Uncompressing Co Infrastructure Node Package [RELEASE]      100%
```

4. Дать согласие на продолжение установки, нажать на клавишу «Y».

```
Do you want to continue?  [y/N] y
```

5. После завершения работы исполняемого файла на экране пользователя будет отображен список выполненных операций. Необходимо убедиться, что список содержит сообщения `[ OK ]` или `[CHANGE]` — это свидетельствует об успешной установке.

При получении сообщения `[FAIL]` необходимо обратиться в техническую поддержку.

Для использования других систем контейнеризации необходимо обратиться в техническую поддержку.

2.3.6 Настройка зависимостей Python

На сервере с ролью operator зависимости Python указаны в файле `~/install_co/contrib/ces/requirements.txt`.

Для использования зависимостей из файла необходимо выполнить команду:

```
pip3 install -r ~/install_co/contrib/ces/requirements.txt
```

При установке модулей Pyhton с помощью скрипта venv_setup.sh настройка зависимостей выполняется автоматически.

2.4 Подготовка конфигурационных файлов

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

2.4.1 Интеграция по протоколу WOPI

В файле переменных `~/install_co/group_vars/co_setup/main.yml` необходимо указать домен сервиса Nextcloud в переменной `openresty_csp_allowed_frame_ancestors`, например:

```
openresty_csp_allowed_frame_ancestors:
  - "nextcloud.example.net"
```

Примечания:

1. Интеграция с мессенджерами в режиме WOPI недоступна.

2. Интеграция с WOPI тестировалась только для хранилища Nextcloud с плагином `https://apps.nextcloud.com/apps/officeonline`.

В конфигурационном файле `Nextcloud config/config.php` необходимо добавить переменную `'allow_local_remote_servers'=> true`.

На сервере Nextcloud в режиме администратора следует настроить интеграцию с Office Online. Указать адрес сформированный в соответствии с разделом «Внешние DNS-записи»:

```
https://docs[-<domain_env>.]<domain_name>
```

Для устранения ошибки, при которой копирование выделенного текста не работает в режиме просмотра документа, необходимо предоставить iframe доступ к Clipboard API следующим образом:

```
<iframe src="https://docs[-<domain_env>.]<domain_name>" \
allow="clipboard-read; clipboard-write"></iframe>
```

2.4.2 Порядок размещения и заполнения файлов конфигурации

Директория установки содержит предзаполненные файлы конфигураций, подготовленные для упрощения настройки системы. Необходимо скопировать шаблоны конфигурационных файлов `hosts.yml`, `main.yml` и конфигурационный файл `ansible.cfg`. Шаблоны для заполнения в зависимости от типа конфигурации представлены в таблице 3.

Таблица 3 — Шаблоны файлов конфигурации

Тип конфигурации	Расположение шаблона
Конфигурация без отказоустойчивости	contrib/ces/standalone/hosts.yml
	contrib/ces/standalone/group_vars/co_setup/main.yml
	contrib/ces/standalone/group_vars/co_setup/extra_vars.yml
Кластерная установка	contrib/ces/cluster/hosts.yml
	contrib/ces/cluster/group_vars/co_setup/main.yml
	contrib/ces/cluster/group_vars/co_setup/extra_vars.yml

Файл inventory использует формат .yml, синтаксис которого описан в документации Ansible.

Примеры команд копирования файлов в зависимости от типа установки.

Установка standalone:

```
cp -r ~/install_co/contrib/ces/standalone/* ~/install_co
```

Кластерная установка:

```
cp -r ~/install_co/contrib/ces/cluster/* ~/install_co
```

Вне зависимости от типа установки следует скопировать файл `~/install_co/contrib/co/ansible.cfg` в корневой раздел директории установки с помощью команды:

```
 cp ~/install_co/contrib/ces/ansible.cfg ansible.cfg
```

После выполнения копирования файлы будут размещены в двух каталогах:

– корневой каталог `~/install_co/` будет содержать файлы:

```
root@operator: ls -l ~/install_co/
hosts.yml
ansible.cfg
```

– каталог `~/install_co/group_vars/co_setup/` будет содержать файлы:

```
root@operator: ls -l ~/install_co/group_vars/co_setup/
main.yml
extra_vars.yml
```

После заполнения файлы конфигурации рекомендуется хранить отдельно на внешнем ресурсе. Файлы могут потребоваться при восстановлении и/или переустановке системы.

2.4.3 Конфигурирование файла hosts.yml

Для определения роли сервера необходимо добавить его FQDN 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: `co-etcd-1.installation.example.net:`

где:

– `co-etcd-1` — имя сервера для подгруппы `co-etcd`;

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

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

где: `co-etcd-[1:3]` — группа серверов `co-etcd`.

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

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

```
all:
  children:

    co:
      children:                                  # Перечень групп
        co_audit:                                # Подгруппа co_audit
          hosts:
            co-audit-[1:2].installation.example.net:  # FQDN сервера

        co_etcd:
          hosts:
            co-etcd-[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:

    co:
      children:
        co_audit:
          hosts:
            co-infra-1.installation.example.net:

        co_etcd:
          hosts:
            co-infra-1.installation.example.net:
```

Объединение ролей может применяться в кластерной установке, если ресурсы организации ограничены.

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

2.4.4 Конфигурирование файла main.yml

Для первичной установки системы необходимо скопировать предзаполненный файл конфигурации из директориии ~/install_co/contrib/ces/. 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_co/group_vars/co_setup/main.yml и изменить значения для обязательных переменных, перечисленных в таблице 5.

Описание переменных из конфигурационного файла main.yml представлено в таблице 4.

Таблица 4 — Основные переменные

Наименование переменной	Заполнение обязательно	Описание
ansible_user	-	Имя пользователя, с которым Ansible подключается к хостам по ssh Необходимо учитывать привилегии пользователя для подключения к хостам, у пользователя должны быть права sudo и возможность выполнять sudo без пароля
domain_env	-	Элемент доменного имени установки, предназначеный для разграничения доступа к сервисам.

Наименование переменной	Заполнение обязательно	Описание
		Устанавливается в соответствии с разделом Создание DNS-записей
domain_name	+	Зарегистрированный домен установки СО
ca_main_config.auth_keys.services.key	+	Ключ для настройки внутреннего центра сертификации, для генерации сертификатов межсервисного взаимодействия СО. Сгенерировать ключ для доступа к CFSSL API с помощью команды: `openssl rand -hex 16`
clickhouse_user_default_password	+	Пароль пользователя `default` для Clickhouse стека мониторинга `pwgen 20 1`
clickhouse_user_otel_password	+	Пароль пользователя `otel` для Clickhouse `pwgen 20 1`
co_observability_logs_retention_days	-	Время хранения логов в стеке observability, значение в днях
co_observability_metrics_retention_days	-	Время хранения метрик, значение в днях. Формат записи — "120d"
Конфигурация Docker		
docker_daemon_parameters: insecure-registries	+	Установка реестра образов. Заменить на IP-адрес или FQDN имя сервера с ролью operator и порт 5000 (например ["10.1.2.3:5000"])
docker_image_registry	+	Установка реестра контейнеров. Заменить на IP-адрес или FQDN имя сервера с ролью operator и порт 5000 (например 10.1.2.3:5000)
docker_registry_username	-	Имя пользователя для доступа к docker_registry. Значение по умолчанию "couser"
docker_registry_password	+	Пароль для доступа к docker_registry. Длина пароля не менее 8 симовлов
cu_pool_size	-	Количество conversion units(оставить без изменения)

Наименование переменной	Заполнение обязательно	Описание
du_pool_size	-	Количество document units (оставить без изменения)
Конфигурация ETCD		
etcd_browser_password	+	Пароль пользователя для веб-доступа к etcd
etcd_browser_username	-	Имя пользователя для веб-доступа к etcd
Конфигурация Grafana		
grafana_admin_password	+	Пароль администратора grafana
Конфигурация ELK		
elasticsearch_admin_password	+	Пароль администратора elasticsearch
elasticsearch_admin_password_hash	+	Хеш пароля администратора elasticsearch
elasticsearch_kibana_password_hash	+	Хеш пароля пользователя elasticsearch Kibana
kibana_elasticsearch_password	+	Пароль пользователя elasticsearch Kibana
Конфигурация KEEPALIVED		
keepalived_openresty_enabled	-	Включает использование внутреннего балансировщика нагрузки HAProxy совместно с сервисом Keepalived для обеспечения отказоустойчивости и высокой доступности lb-core-auth компонента (значение: true или false)
keepalived_openresty_virtual_ip	-	Свободный IP-адрес в подсети серверов кластерной установки. При использовании переменной keepalived_openresty_enabled со значеним true. Пример значения: "valid_virtual_ip"
Конфигурация LCS		
lcs_license_key	-	Ключ сервера лицензирования
lcs_server_base_url	-	Ссылка для сервера лицензирования
Конфигурация RabbitMQ		
rabbitmq_federation_enabled	-	Включение федерации RabbitMQ (значение: true или false)

Наименование переменной	Заполнение обязательно	Описание
rabbitmq_users.root.password	+	Пароль для root пользователя RabbitMQ
rabbitmq_users.couser.password	+	Пароль для couser пользователя RabbitMQ
Конфигурация REDIS		
redis_password	+	Пароль для Redis команды AUTH
Конфигурация TLS		
tls_ca_filename	-	Сертификат центра сертификации. Имя сертификата по умолчанию: "ca.pem"
tls_cert_filename	-	Сертификат сервера. Имя сертификата по умолчанию: "ca.pem"
tls_key_filename	-	Имя файла закрытого ключа сертификата сервера. Имя файла ключа по умолчанию: "server.nopass.key"
Конфигурация Openresty		
openresty_api_password	+	Пароль пользователя для доступа к CO Manage API
Конфигурация Sentry		
chatbot_sentry_dsn	-	Отправка ошибок сервиса Chatbot в сервис Sentry
openresty_sentry_log_sentry_dsn	-	Sentry DSN для отправки ошибок в sentry
openresty_sentry_log_sentry_url	-	Sentry DSN ссылка для разрешения кросс доменных запросов
openresty_sentry_board_wopi_log_dsn	-	Sentry DSN для отправки ошибок в sentry от «МояДоска»
openresty_sentry_sso_log_dsn	-	SSO Sentry DSN для отправки ошибок в sentry
openresty_sentry_wfe_log_dsn	-	WFE Sentry DSN для отправки ошибок в sentry
openresty_wfe_loader_pending_ms	-	Задержка (ms) перед показом загрузчика в поле файлового менеджера

Наименование переменной	Заполнение обязательно	Описание
openresty_wfe_page_size	-	Количество элементов на странице в списке файлов в веб-файловом менеджере. Принимает целочисленные значения {число} 0 - рассчет количества по доступному на экране месту 1 - отключить ограничение
openresty_wfe_max_request_delay	-	Максимальная задержка (в секундах) перед запросом на обновление списка файлов в текущей папке после восстановления соединения
Настройка victoria_metrics		
victoria_metrics_alerts_enabled	-	Значение по умолчанию: false

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'
```

Дополнительные переменные перечислены в таблице 5. Для изменения значения необходимо открыть с помощью текстового редактора файл extra_vars.yml, расположенный в директории: `~/install_co/group_vars/co_setup`.

Таблица 5 — Дополнительные переменные

Наименование роли	Заполнение обязательно	Описание
unbound_forward_addresses	-	Список внешних или внутренних DNS, на которые будут отсылаться запросы из unbound

2.4.5 Автоматическое создание паролей

В релизе 3.5 для сохранения уровня безопасности устанавливаемой системы из примеров конфигурационных файлов (каталог `~/install_co/contrib/`) были исключены значения переменных, содержащих пароли.

Для автоматического создания паролей, уникальных для каждой установки продукта, в дистрибутив был добавлен скрипт `~/install_co/contrib/password_generator.py`, который генерирует пароли и заполняет переменные с учетом различных требований к длине пароля.

Рекомендуется размещать конфигурационный файл `main.yml` в каталоге `group_vars/co_setup/main.yml`. В случае размещения конфигурационного файла в другом каталоге необходимо указать путь до конфигурационного файла при запуске скрипта.

Синтаксис использования скрипта:

```
[запуск python и путь до скрипта][-i путь до конфигурационного файла][-аргументы запуска]
```

Таблица 6 — Примеры использования аргументов

Аргумент	Процесс
-m 1	Генерирует пароли для переменных и записывает в файл
-m 2	Генерирует пароли для переменных и выводит на экран без записи в файл

Пример:

Расположение скрипта `contrib/password_generator.py`, расположение конфигурационного файла `group_vars/co_setup/main.yml`, генерация переменных с записью в файл:

```
python contrib/password_generator.py -i group_vars/co_setup/main.yml -m 1
```

Таблица 7 — Переменные, заполняемые скриптом

Принадлежность переменных	Наименование переменной
Переменные компонента СО	ca_main_config.auth_keys.services.key clickhouse_user_default_password clickhouse_user_otel_password grafana_admin_password etcd_browser_password elasticsearch_admin_password kibana_elasticsearch_password rabbitmq_users.root.password rabbitmq_users.couser.password redis_password

Принадлежность переменных	Наименование переменной
	openresty_api_password docker_registry_password elasticsearch_admin_password_hash elasticsearch_kibana_password_hash

2.5 Создание и размещение сертификатов

2.5.1 Создание SSL-сертификатов

Для обеспечения защищенного соединения между пользователем и сервером CCP используется проверка SSL-сертификата. Организации необходимо установить SSL-сертификат на свой сервер, чтобы поддерживать безопасную сессию с браузерами пользователей.

SSL-сертификаты выпускаются доверенным центром сертификации. Браузеры, ОС и мобильные устройства поддерживают список корневых сертификатов доверенных центров сертификации.

В отдельных случаях (например для демонстрации продукта) допускается использование самоподписанного сертификата. Порядок создания самоподписанных сертификатов описан в приложении Г.

Для упрощения настройки файл переменных `~/install_co/group_vars/co_setup/main.yml` (подготовленный в соответствии с требованиями раздела «Порядок размещения и заполнения файлов конфигурации») содержит имена сертификатов по умолчанию (секция TLS cert and key filenames).

Необходимо использовать сертификаты, выданные центром сертификации для вашей организации, или создать группу новых самоподписанных сертификатов.

2.5.2 Размещение SSL-сертификатов для шифрования

Порядок размещения сертификатов:

1. Разместить сертификат внешнего домена:

```
~/install_co/certificates/server.crt
```

2. Разместить ключ внешнего домена:

```
~/install_co/certificates/server.nopass.key
```

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

```
~/install_co/certificates/ca.pem
```

2.6 Настройка DNS

2.6.1 Создание DNS-записей

DNS-записи продукта формируются с помощью переменных `<domain_env>` и `<domain_name>`. В зависимости от заполнения переменных существует два типа записей:

- Если переменная `<domain_env>` не задана, то все DNS-записи будут иметь вид: `<service>.<domain_name>`
- Если переменная `<domain_env>` задана, то все DNS-записи будут иметь вид: `<service>-<domain_env>.<domain_name>`

где `<service>` — имя сервиса из таблицы.

В соответствии с форматом записи домена необходимо добавить на DNS-сервер организации все записи из одной из таблиц 8 или 9 с примерами.

Таблица 8 — DNS-записи в формате <service>.<domain_name>

Префикс DNS-записи	Тип записи	Значение	Комментарий
auth.<domain_name>	A	IP-адрес сервера, указанного в группе co_lb_core_wopi	Адрес приложения авторизации и целевой страницы Auth SSO. Количество A записей должно соответствовать количеству серверов
cdn.<domain_name>	CNAME	auth.<domain_name>	Адрес CDN
coapi.<domain_name>	CNAME	auth.<domain_name>	Адрес COAPI
docs.<domain_name>	CNAME	auth.<domain_name>	Адрес приложения редакторов
files.<domain_name>	CNAME	auth.<domain_name>	Адрес приложения файлового менеджера
links.<domain_name>	CNAME	auth.<domain_name>	Адрес ссылок на документы
_https._tcp.<domain_name>	SRV	auth.<domain_name>	Опционально, для мобильных клиентов
***** — *при использовании балансировки в качестве значения указывается виртуальный IP-адрес, содержащийся в переменной* `keepalived_openresty_virtual_ip` *файла* `~/install_co/group_vars/co_setup/main.yml`			

Таблица 9 — DNS-записи в формате <service>-<domain_env>.<domain_name>

Префикс DNS-записи	Тип записи	Значение	Комментарий
auth-<domain_env>.<domain_name>	A	IP-адрес сервера, указанного в группе co_lb_core_wopi	Адрес приложения авторизации и целевой страницы Auth SSO. Количество A записей должно соответствовать количеству серверов
cdn-<domain_env>.<domain_name>	CNAME	auth-<domain_env>.<domain_name>	Адрес CDN
coapi-<domain_env>.<domain_name>	CNAME	auth-<domain_env>.<domain_name>	Адрес COAPI
docs-<domain_env>.<domain_name>	CNAME	auth-<domain_env>.<domain_name>	Адрес приложения редакторов
files-<domain_env>.<domain_name>	CNAME	auth-<domain_env>.<domain_name>	Адрес приложения файлового менеджера
links-<domain_env>.<domain_name>	CNAME	auth-<domain_env>.<domain_name>	Адрес ссылок на документы
_https._tcp-<domain_env>.<domain_name>	SRV	auth-<domain_env>.<domain_name>	Опционально, для мобильных клиентов
***** *— при использовании балансировки в качестве значения указывается виртуальный IP-адрес, содержащийся в переменной* `keepalived_openresty_virtual_ip` *файла* `~/install_co/group_vars/co_setup/main.yml`			

2.6.2 Внутренние DNS-записи для установки

Во время установки производится настройка и запуск локального кеширующего DNS-сервера (Unbound) на серверах группы co_etcd. Сервер служит для обработки запросов внутри установки и предназначен для работы контейнеров и серверов через соответствующие параметры групповых переменных. По умолчанию серверы, перечисленные в файле `hosts.yml`, будут перенастроены на работу через Unbound и не будут принимать параметры DNS-серверов по DHCP. По умолчанию Unbound настроен на маршрутизацию запросов на адреса 8.8.8.8 и 8.8.4.4.

Для работы с внутренними DNS-серверами Unbound необходимо настроить при подготовке конфигурационных файлов. Порядок действий:

- открыть файл `~/install_co/group_vars/co_setup/extra_vars.yml`
- расскомментировать переменную `unbound_forward_addresses`
- внести в список IP-адреса DNS-серверов организации.

Пример записи:

```
## DNS Forwarder Configuration
# List of DNS servers that the queries will be forwarded to
unbound_forward_addresses:
  - "192.168.0.100"
  - "192.168.0.200"
```

При использовании собственного DNS-сервера необходимо внести в его конфигурацию все FQDN-записи серверов, перечисленных в файле `hosts.yml`.

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

2.6.3 Проверка работы DNS на сервере с ролью operator

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

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 co-infra-1.installation.example.net
```

Пример ответа:

```
; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> A co-infra-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:
;co-infra-1.installation.example.net. IN A ;;
ANSWER SECTION:
*.co-infra-1.installation.example.net. 900 IN CNAME co-infra-
1.installation.example.net.
co-infra-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.

```
*.co-infra-1.installation.example.net. 900 IN CNAME
co-infra-1.installation.example.net.
co-infra-1.installation.example.net. 900 IN A 192.168.0.1
```

3 ДОПОЛНИТЕЛЬНЫЕ ПАРАМЕТРЫ УСТАНОВКИ

В разделе представлены дополнительные параметры установки системы. Настройка перечисленных функций не обязательна.

Если специализированные требования к установке отсутствуют, необходимо перейти в раздел «Запуск установки».

3.1 Порядок обновления ядра Linux

При установке ОС на серверы кластера ядро может быть автоматически обновлено до минимальной требуемой версии. По умолчанию ядро обновляется на kernel-lt (LTS) в ОС Redhat-based (РЕД ОС «Муром» (версия ФСТЭК)). В ОС Debian-based (Ubuntu, Astra Linux Special Edition, Astra Linux Common Edition) по умолчанию ядро не обновляется. Поддержка других ядер не гарантируется, обратитесь в техническую поддержку за более подробной информацией.

Для отключения обновления в ОС Redhat-based (РЕД ОС «Муром» (версия ФСТЭК)) при запуске установки необходимо использовать следующую команду:

```
-e kernel_ml_enabled=false
```

Для обновления ядра до kernel-lt (LTS) в ОС Debian-based (Ubuntu, Astra Linux Special Edition, Astra Linux Common Edition) при запуске установки необходимо использовать следующую команду:

```
-e kernel_ml_deb_enabled=true
```

В ОС Альт 9/10 автоматическое обновление ядра не поддерживается.

3.2 Настройка дополнительных серверов для аудита

Настройка дополнительных Fluentd серверов для сбора событий выполняется с помощью текстового редактора в файле `~/install_co/group_vars/co_setup/main.yml`. Необходимо добавить в файл перечисленные команды, изменив IP-адреса и порты:

```
# LOG servers for the environment
fluentd_server_upstream_log_servers:
  - ip: "10.10.10.10"
    port: 24225
  - ip: "11.11.11.11"
    port: 24225
```

Данная настройка применяется только при использовании в установке роли log. Включение функции задается с помощью переменной, указанной в таблице 10.

Таблица 10 — Подключение серверов аудита

Расположение переменной	Наименование переменной	Тип переменной	Значение
group_vars/co_setup/ main.yml	common_fluent_ logging_enabled	boolean	true / false (по умолчанию)

3.3 Остановка и запуск системы с помощью консольных команд

Для работы с консолью ПО МойОфис администратору системы необходимо обеспечить ssh-доступ к серверу в контуре установки.

Сервисы CCP управляются с помощью Docker.

Просмотр списка сервисов на сервере подсистемы:

```
docker ps
```

Для остановки сервиса `<service_name>` из списка сервисов необходимо выполнить следующую команду:

```
docker stop <service_name>
```

Для перезапуска сервиса следует выполнить следующую команду:

```
docker restart <service_name>
```

Для остановки сервиса docker необходимо выполнить следующую команду:

```
systemctl stop docker
```

Для корректного завершения работы сервисов следует выполнить следующую команду:

```
shutdown <option>
```

Ноды сервисов рекомендуется выключать по очереди. Параметр <option> позволяет использовать дополнительные параметры выключения, в том числе таймер и опцию перезапуска.

Пример (немедленное выключение с остановкой сервисов):

```
shutdown –h now
```

Запуск подсистемы осуществляется при инициализации и запуске аппаратной части.

3.4 Настройка обработки журналов

Настройка обработки журналов (logrotate) в текущей версии ПО не автоматизирована и настраивается самостоятельно администратором.

3.5 Настройка ротации журналов событий в ElasticSearch

Для защиты диска от переполнения записи журнала событий старше 120 дней автоматически удаляются. Процедура использует политики удаления устаревших индексов в ElasticSearch.

Период автоматического удаления (в днях) задается при развертывании в файле `~/install_co/group_vars/all/main.yml` с помощью переменной co_logs_retention_days.

3.6 Настройка автоматического отключения неактивного пользователя

CCP позволяет автоматически отключать пользователей от редактируемого документа, в случае их бездействия.

Для настройки необходимо присвоить новые значения переменным, перечисленным в таблице 11.

Таблица 11 — Переменные для автоматического отключения неактивного пользователя

Наименование сервиса	Наименование переменной	Тип переменной	Размерность	Значение по умолчанию	Описание
etcd (CO)	config/dcm/romdocuments.ttlSecs	number	секунды	360	Время хранения кешированного файла документа на диске сервиса DCM
	config/dcm/dcm.du.edits.expireSecs	number	секунды	11000	Период работы в режиме редактирования без сохранения. При истечении времени выполняется перезапуск сервиса DU с разрывом сессии редактирования
	config/nps-du/Du.Env.	number	минуты	180	Время до автомати-

Наименование сервиса	Наименование переменной	Тип переменной	Размерность	Значение по умолчанию	Описание
	TimeInactivityMins				ческого разрыва сессии редактирования при бездействии пользователя

На этапе развертывания ССР присвоить новое значение возможно только для времени до автоматического разрыва сессии редактирования при бездействии пользователя. Для изменения значения переменной при запуске скрипта установки необходимо использовать следующую команду:

```
-e du_max_time_for_inactive_collaborator_mins=120
```

Порядок запуска скрипта установки описан в разделе «Установка».

3.7 Предзагрузка ресурсов WOPI

В релизе 3.1 добавлена возможность использования prefetches при использовании рендеринга на стороне сервера (SSR) для формирования html-страницы.

Для использования предзагрузки в корне директории сервера с ролью docs во время установки системы будет размещен файл prefetches.json.

Пример размещения файла:

```
https://docs-<domain_env>.<domain_name>/prefetches.json
```

Prefetches.json представляет собой список файлов, кэширование которых обеспечит быстрый запуск/загрузку приложения.

Имена файлов, представленных в prefetches.json генерируются во время установки

Пример содержимого файла prefetches.json:

```
[
  {
    "href": "main.d25f849e.css"
  },
  {
    "href": "main.68e367ba.js"
  },
  {
    "href": "wasm-53fbf4860ef6a3ee829b988bd4091c5b.wasm"
  }
]
```

Настройка SSR на стороне WOPI сервера выполняется администратором сервера самостоятельно. После настройки html-страница должна содержать следующие данные:

```
<link rel="prefetch" href="https://docs-<domain_env>.<domain_name>/main.
[number].css" />
<link rel="prefetch" href="https://docs-<domain_env>.<domain_name>/main.
[number].js" />
<link rel="prefetch" href="https://docs-<domain_env>.<domain_name>/wasm-
[number].wasm" />
```

3.8 Функция отправки ошибок

3.8.1 Установка и настройка Sentry

В продукте реализована функция отправки ошибок в сервис аналитики Kibana или сервис Sentry. По умолчанию ошибки отправляются в сервис аналитики Kibana.

Сервис Sentry не входит в комплект поставки ПО, его установка и настройка выполняется администратором самостоятельно. При настройке Sentry следует учитывать рекомендации, изложенные в разделе «Рекомендации по конфигурированию Sentry».

Для настройки функции отправки ошибок необходимо использовать переменные, указанные в таблице 12.

Если в настройках оба сервиса отключены, то отчеты об ошибках отправляться не будут.

Таблица 12 — Отправка ошибок

Наименование сервиса	Наименование переменной	Тип переменной	Значение	Описание
etcd (CO)	common/logger.analytics.enabled	boolean	true (по умолчанию) / false	Включение/отключение отправки данных в сервис аналитики Kibana
	config/wte/error.log.analytics.enabled	boolean	true (по умолчанию) / false	Отправка ошибок в сервис аналитики Kibana Ошибки отправляются только при включении переменной common/logger.analytics.enabled
	config/wte/error.log.sentry.dsn	string	""	Отправка ошибок в сервис Sentry
	config/wte/sentry.wfe.log.dsn	string	""	Отправка ошибок сервиса WFE в сервис Sentry

Наименование сервиса	Наименование переменной	Тип переменной	Значение	Описание
	config/wte/sentry .sso.log.dsn	string	""	Отправка ошибок сервиса SSO в сервис Sentry
	config/wte/ chatbot .sentry.dsn	string	""	Отправка ошибок сервиса Chatbot в сервис Sentry
	config/wfe/ routing/error .log.sentry.url	string	""	Hostname сервера Sentry, если сервер развернут в другом домене
	config/wte/ error.log .feedback.enabled	boolean	true (по умолчанию) / false	Включение/отключение поля обратной связи. Функция доступна после включения отправки ошибок в один из сервисов с помощью переменных: wte/error.log.sentry.dsn wte/error.log .analytics.enabled

При включении поля обратной связи с помощью переменной wte/error.log.feedback.enabled пользователь может оставить собственный комментарий к ошибке. Этот комментарий будет отправлен в зависимости от конфигурации:

– в Sentry и дополнит соответствующее событие ошибки;

– в сервис аналитики Kibana отдельным событием, с сохранением идентификатора eventId из оригинального события ошибки.

События ошибок сервиса аналитики дополняются идентификатором пользователя и идентификатором события.

3.8.2 Рекомендации по конфигурированию Sentry

1. Для сохранения безопасности следует ограничить доступ к серверу Sentry для группы пользователей, которым определены соответствующие процессы допуска к пользовательской информации.

Ограничение доступа к журналу событий не позволит использовать сервис для отладки развития атаки, а также для получения ID объектов/пользователей.

2. При настройке SSL и в DSN указать url с использованием https.

3. В настройках проекта следует включить Verify TLS/SSL для создания защищенного соединения с сервером Sentry.

4. В настройках проекта необходимо указать домен/или несколько доменов продукта, в меню Allowed Domains, для ограничения обращений к серверу от сторонних доменов.

3.8.3 Сбор пользовательской аналитики

В продукте реализован сбор пользовательской аналитики, по умолчанию функция выключена. После включения сохраняет действия пользователя при работе с сервисами продукта. Пользовательская аналитика собирается автоматически и направляется POST-запросами на `url:/api/v1/analytics/user_analytics`.

Для получения, обработки и хранения данных силами администратора системы следует развернуть дополнительный прокси-сервер, собирающий и обрабатывающий данные из POST-запросов.

Для управления функцией сбора пользовательской аналитики необходимо использовать переменную, указанную в таблице 13.

Таблица 13 — Управление пользовательской аналитикой

Наименование сервиса	Наименование переменной	Тип переменной	Значение	Описание
etcd (CO)	config/wte/ user.analytics .enabled	Boolean	true / false (по умолчанию)	включение/ отключение функции

3.9 Настройка системы для работы со сложными файлами

В CCP появились настройки для ограничения использования оперативной памяти при работе со сложными файлами.

Для системы с минимально возможными аппаратными ресурсами работа со сложными файлами ограничена одной операцией над сложным файлом в один момент времени. При увеличении количества операций в один момент времени могут возникать задержки в текущих операциях и ошибки в работе других операций (в том числе над другими файлами), с сохранением общей работы системы.

3.9.1 Настройка сервиса DU

Выделение дополнительных ресурсов сервису DU для открытия файлов на редактирование выполняется с помощью переменной `du_max_memory_heavy`.

Для увеличения количества открытых на редактирование файлов следует изменить в большую сторону значения переменным `du_pool_size` и `du_heavy_unit_count`.

Рекомендуется контролировать используемую сервисом DU память средствами мониторинга для сохранения стабильной работы системы.

Для изменения ограничения необходимо установить новые значения переменным, указанным в таблице 14.

Таблица 14 — Переменные для настройки сервиса DU

Наименование переменной	Тип переменной	Размерность	Значение по умолчанию	Описание
du_max_memory_heavy	string	гигабайты	"5GB"	Максимальное количество RAM для сложных файлов
du_pool_size	integer	количество сервисов	100	Количество сервисов DU для редактирования файлов
du_heavy_unit_count	integer	количество сервисов	2	Количество сервисов DU для редактирования сложных файлов

Управление функцией поддерживается на этапе развертывания CO. Изменение значения переменной выполняется при запуске скрипта установки.

Пример команды настройки функции:

```
ansible-playbook playbooks/main.yml -e du_heavy_unit_count=5
```

3.9.2 Настройка пользователя

Для конфигурации работы со сложными файлами на стороне пользователя необходимо использовать переменные, указаные в таблице 15.

Таблица 15 — Настройка пользователя для работы со сложными файлами

Наименование переменной	Тип переменной	Размерность	Значение по умолчанию	Описание
co/config/wte/ worker.init .timeout	integer	милли-секунды	200000	Время ожидания инициализации Worker
co/config/wte/ service.init .timeout	integer	милли-секунды	600000	Время ожидания инициализации WTE сервисов
co/config/wte/ document .processing .timeout	integer	милли-секунды	600000	Время ожидания обработки документа сервисом Core
co/config/wte/ document.load.timeout	integer	милли-секунды	180000	Время ожидания обработки и загрузки документа от сервиса DU

3.10 Настройка портов

3.10.1 Карта портов

Карта портов представлена в таблице 16.

Для обеспечения внешнего доступа к внутренним сервисам через интернет следует открыть порты 80 (HTTP) и 443 (HTTPS).

Таблица 16 — Карта портов

Группа Ansible	Сервис	Прослушиваемый порт	Порт подключения	Куда обращается
co	node_exporter	9100/tcp	-	-
	cadvisor	9101/tcp	-	-
	fluentd_agent	5140/udp, 5160/udp, 5165/udp, 5180/tcp, 24224/tcp, 5185/udp, 23100/tc	24225/tcp	fluentd_server
	docker	-	5000/tcp	docker-registry
	confd	-	2379/tcp	etcd
co_cvm, co_cu, co_dcm, co_du, co_jod, co_lb_core_wopi	haproxy	20002/tcp, 20004 - 20007/tcp, 20379/tcp, 33679/tcp	8443/tcp	openresty-lb-core-auth
			9094/tcp	cvm
			9096/tcp	jod
			5671/tcp	rabbitmq
			2379/tcp	etcd
			26379/tcp	redis_sentinel
co_lb_core_wopi	openresty-lb-core-auth	80/tcp, 443/tcp, 8080/tcp, 8443/tcp, 8888/tcp	20002/tcp, 20004 - 20007/tcp, 20379/tcp, 33679/tcp	haproxy
			5160/udp, 5165/udp	fluentd_agent
			9095/tcp	dcm
			30000 - 65535/tcp	du

Группа Ansible	Сервис	Прослушива-емый порт	Порт подключения	Куда обращается
co_etcd	etcd	2379/tcp, 2380/tcp	2380/tcp**	etcd
	etcd_browser	8001/tcp	2379/tcp	etcd
co_mq	rabbitmq	4369/tcp, 5671/tcp, 15671/tcp, 25672/tcp	-	-
co_cvm	cvm	9094/tcp	20002/tcp, 20005/tcp, 20006/tcp, 33679/tcp, 20379/tcp	haproxy
			6379/tcp	redis
			24224/tcp	fluentd_agent
			30000 - 65535/tcp	cu
co_cu	cu	30000 - 65535/tcp	24224/tcp, 5180/tcp	fluentd_agent
	sdd_cu	9097/tcp	24224/tcp	fluentd_agent
			6379/tcp, 33679/tcp	redis
			9097/tcp**	sdd_cu
			30000 - 65535/tcp	cu
co_dcm	dcm	9095/tcp	20002/tcp, 20004/tcp, 20005/tcp, 33679/tcp, 20379/tcp	haproxy
			6379/tcp	redis
			24224/tcp	fluentd_agent
			30000 - 65535/tcp	du
co_du	du	30000 - 65535/tcp	24224/tcp, 5180/tcp	fluentd_agent
			5671/tcp	rabbitmq

Группа Ansible	Сервис	Прослушива-емый порт	Порт подключения	Куда обращается
	sdd_du	9098/tcp	24224/tcp	fluentd_agent
			6379/tcp, 33679/tcp	redis
			9098/tcp**	sdd_du
			30000 - 65535/tcp	du
co_jod	jod	9096/tcp	20379/tcp	haproxy
			24224/tcp	fluentd_agent
co_dcm, co_lb_core_wopi	lsyncd**	9022/tcp	9022/tcp	lsyncd
co_imc	redis	6379/tcp, 16379/tcp	6379/tcp**	redis
	redis_sentinel	26379/tcp		
co_infra	ca	8890/tcp	-	-
	nginx	443/tcp, 6443/tcp*	9090/tcp	prometheus
			3000/tcp	grafana
			9093/tcp	alertmanager
			5601/tcp	kibana
			8001/tcp	etcd_browser
			9993/tcp***	alertmanager
			3002/tcp***	grafana
			8428/tcp***	victoria metrics
	prometheus	9090/tcp	9093/tcp	alertmanager
			9115/tcp	blackbox_ exporter
			9101/tcp	cadvisor
			2379/tcp	etcd
			9100/tcp	node_exporter
			9121/tcp	redis_exporter
			443/tcp, 8443/tcp	openresty-lb-core-auth

Группа Ansible	Сервис	Прослушива-емый порт	Порт подключения	Куда обращается
			9094/tcp	cvm
			9095/tcp	dcm
			9096/tcp	jod
			9097/tcp	sdd_cu
			9098/tcp	sdd_du
	grafana	3000/tcp	9090/tcp	prometheus
	alertmanager	9093/tcp	-	Внешние каналы коммуникации
	blackbox_ exporter	9115/tcp	-	-
	redis_exporter	9121/tcp	-	-
	elasticsearch	9200/tcp, 9300/tcp, 9600/tcp	-	-
	kibana	5601/tcp	9200/tcp	elasticsearch
	fluentd_server	23200/tcp, 24225/tcp	9200/tcp	elasticsearch
operator	docker-registry	5000/tcp	-	-
* — *только для установки типа standalone* ** — *только для установки типа cluster*				

4 УСТАНОВКА

4.1 Запуск установки

Запуск установки продукта выполняется на сервере с ролью operator с помощью команды:

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

Скорость установки зависит от выделенных вычислительных ресурсов. Для обеспечения непрерывности установки рекомендуется использовать дополнительное ПО Screen, Tmux.

4.2 Проверка корректности установки

Для проверки работоспособности установленного ПО и корректности установки необходимо запустить ПО «МойОфис Документы», выполнив следующие действия:

1. Открыть в поддерживаемом веб-браузере страницу установленного сервиса Nextcloud.

2. Войти в Nextcloud и открыть документ на редактирование.

4.3 Диагностика состояния подсистем

4.3.1 Диагностика состояния Nginx

Перечень проверок для диагностики состояния Ngnix указан в таблице 17.

Таблица 17 — Перечень проверок для диагностики Nginx

Тип проверки	Адрес	Примечание
Проверка статуса работы подсистем Auth/SSO и Core	https://<локальный-адрес-сервера>:8443/api/manage/core/status	Параметр «all» в ответе должен быть равен строке «OK»
	https://<локальный-адрес-сервера>:8443/api/manage/docs/status	
Проверка текущей конфигурации	https://<локальный-адрес-сервера>:8443/api/manage/config	
Просмотр журналов доступа и ошибок системы Auth/SSO (в случае отсутствия сервера с ролью co_log)	https://<локальный-адрес-сервера>:8443/api/manage/logs/error	В качестве альтернативы используется просмотр журналов событий на сервере с рольюco_lb_core_wopi, по умолчанию место расположения журнала событий: /srv/docker/openresty/logs/
	https://<локальный-адрес-сервера>:8443/api/manage/logs/access	
	https://<локальный-адрес-сервера>:8443/api/manage/logs/access_full	
Просмотр списка активных сессий и авторизованных пользователей подсистемы Auth/SSO	https://<локальный-адрес-сервера>:8443/api/manage/sessions	
	https://<локальный-адрес-сервера>:8443/api/manage/users	

Адрес сервера выбирается из указанных в группе `co_lb_core_wopi` файла `hosts.yml`.

Для обеспечения безопасности доступ к порту 8443, ограниченный на стороне Nginx, должен распространяться на локальный сервер и внутренние (частные) сети с адресами по стандарту RFC1918. Категорически запрещается открывать доступ к порту из публичных сетей.

4.3.2 Диагностика состояния Lsyncd

Диагностика состояния Lsyncd применяется только для кластерного режима установки (в standalone конфигурации lsyncd не используется).

Проверить синхронизацию необходимо в журнале событий с помощью команды:

```
docker logs --tail 10 lsyncd
```

Контейнер lsyncd должен быть запущен на всех узлах с ролью `co_lb_core_wopire_wopi`. Проверить статус его работы следует с помощью команды:

```
cat /srv/docker/lsyncd/conf/lsyncd/lsyncd.status
```

4.3.3 Диагностика состояния RabbitMQ

Проверка статуса федерации осуществляется с помощью веб-интерфейса сервиса RabbitMQ.

Таблица 18 — Данные для подключения

Данные	Пример значения	Описание
Адрес веб-интерфейса	mq-1.installation.example.net	Любой сервер группы `co_mq` Сервер указан в конфигурационном файле: `~/install_co/hosts.yml`
Имя пользователя	root	
пароль	Значение переменной `rabbitmq_users.root.password`	Переменная размещена в конфигурационном файле: `~/install_co/group_vars/co_setup/main.yml`

Порядок проверки, для примера сервера `mq-1.installation.example.net`:

1. Открыть страницу `https://mq-1.installation.example.net:15671` в браузере.
2. Авторизоваться на открывшейся странице. Имя пользователя — `root`. Пароль — значение переменной `rabbitmq_users.root.password`.
3. Открыть страницу `https://mq-1.installation.example.net:15671/#/federation`
4. Проверить, что на странице отображаются три очереди в состоянии running. Это свидетельствует о том, что федерация включена. При отключенной федерации переход по адресу не осуществится (в веб-интерфейсе нет соответствующей вкладки).

4.4 Системы мониторинга

4.4.1 Настройка подключения

В качестве системы мониторинга используется VictoriaMetrics с отображением информации и логирования с помощью Grafana. Для доступа к системам мониторинга и логирования СО необходимо использовать параметры, указанные в таблице 19.

Таблица 19 — Доступ к мониторингу СО

Адрес обращения при кластерной установке	Адрес обращения при установке standalone	Имя пользователя	Пароль из переменной СО
https://grafana-paas.<domain_env>:443	https://grafana-paas.<domain_env>:6443	admin	grafana_admin_password

Пример обращения к серверу:

```
https://grafana-paas.co-01.example.net:443
```

4.4.2 Аутентификация через Nginx

В релизе 3.5 добавлена базовая аутентификация через Nginx, установленный на сервере с ролью `co_infra`, к следующим сервисам:

– victoria_metrics;

– alertmanager.

По умолчанию имя пользователя и пароль будут аналогичны, используемым для авторизации в ETCD Browser. Значения параметров формируются их переменных `etcd_browser_username` и `etcd_browser_password`.

Для переопределения значений следует открыть в текстовом редакторе конфигурационный файл `group_vars/co_setup/main.yml` и добавить следующие переменные:

```
nginx_web_auth_user: "<имя пользователя>"
nginx_web_auth_user_password: "<пароль>"
```

4.4.3 Источники метрик

Prometheus собирает метрики от нескольких источников, перечисленных в таблице 20.

Таблица 20 — Источники метрик

Сервис	Порт
co_blackbox	9115
co_cadvisor	9101
co_etcd	2379
co_node_exporter	9100
co_redis_exporter	9121
co_srv_audit	9900
co_srv_cvm	9094
co_srv_dcm	9095
co_srv_fm	9091
co_srv_jod	9096
co_srv_nm	9092
co_srv_openresty	8443
co_srv_sdd_cu	9097
co_srv_sdd_du	9098

4.4.4 Настройка параметров метрик

Для изменения параметров метрик используются свойства из ETCD | config | common, перечень которых представлен в таблице 21.

Таблица 21 — Таблица настроек конфигурации метрик

Название настройки	Принимаемые значения	Значение по умолчанию	Описание настройки
management.metrics.use-global-registry	True / False	True	Сбор метрик стандартным методом приложения с Spring Boot Actuator
redis.lettuce.metrics	True / False	True	Сбор метрик Redis
redis.lettuce.metrics.histogram	True / False	True	Сбор метрик Redis для построения histogram. Используется только при включенной настройке: Сбор метрик Redis
management.metrics.enable Example: management.metrics.enable.co management.metrics.enable.co_units	True / False	Not set	Сбор метрик по шаблону. https://docs.spring.io/spring-boot/reference/actuator/metrics.html#actuator.metrics.customizing.per-meter-properties

Свойства добавляемые к метрикам при развертывании сервисов продукта представлены в таблице 22.

Таблица 22 — Свойства метрик

Метка	Описание метки	Значение метки	Сервис
applicaton	Серверный сервис	co_cvm	cvm
		co_dcm	dcm
		co_fm	fm
		co_jod	jod
		co_nm	nm
job	Задача сервиса мониторинга, которая собирает данные из сервиса	co_srv_cvm	cvm
		co_srv_dcm	dcm
		co_srv_fm	fm
		co_srv_jod	jod
		co_srv_nm	nm
		co_srv_sdd_cu	sdd_cu
		co_srv_sdd_du	sdd_du
		co_cadvisor	cadvisor
		co_etcd	etcd
		co_node_exporter	node_exporter
		co_redis_exporter	redis_exporter
		co_srv_audit	audit
		co_srv_openresty	openresty

4.4.5 Описание панелей

Описание для панелей, используемых в системе мониторинга для графического отображения текущего состояния, представлено в таблице 23.

Таблица 23 — Описание для панелей

Название панели	Описание панели	Строка	Панель	Описание панели
Alerts	Информация о критических событиях	-	Current list of the alerts	Текущее состояние срабатывающих алертов
[DO] Basic User Scenarios Monitoring	Общая информация о пользовательских сценариях. Описание операций авторизации, файловых операций и возникающих ошибок	Availability	All Success Requests Rate	Процентное соотношение успешных запросов авторизаций
			Last Week	Процентное соотношение успешных запросов авторизаций за неделю
			Last 24H	Процентное соотношение успешных запросов авторизаций за 24 ч.
			Last 6H	Процентное соотношение успешных запросов авторизаций за 6 ч.
			Last 1H	Процентное соотношение успешных запросов авторизаций за 1 ч.
		Login Stats	Login 500 ratio	Процентное соотношение ошибочных

Название панели	Описание панели	Строка	Панель	Описание панели
				запросов авторизаций
			Login Requests Rate	Темп запросов авторизаций, распределённый по статусу
			Login latency 95%	Средняя длительность выполнения запросов авторизаций
			All FM Requests Error Ratio	Процентное соотношение ошибочных файловых запросов
			4xx response ratio within 1h window	Процентное соотношение ошибочных HTTP запросов со статусом 4xx за 1 ч.
		File List Stats	FileList Error 500 Ratio	Процентное соотношение ошибочных файловых запросов, связанных с получением списка файлов
			FileList Requests Rate	Темп файловых запросов, связанных с получением списка файлов, распределённый по статусу
			FileList Requests Latency	Средняя длительность выполнения файловых запросов,

Название панели	Описание панели	Строка	Панель	Описание панели
				связанных с получением списка файлов
			File GET API Error 500 Ratio	Процентное соотношение ошибочных GET API файловых запросов, связанных с получением списка файлов
		MakeDir Stats	MakeDir Error 500 Ratio	Процентное соотношение ошибочных файловых запросов, связанных с созданием папки
			MakeDir Requests Rate	Темп файловых запросов, связанных с созданием папки, распределённый по статусу
			MakeDir Requests Latency	Средняя длительность выполнения файловых запросов, связанных с созданием папки
		Upload Stats	Upload Error 500 Ratio	Процентное соотношение ошибочных файловых запросов, связанных с загрузкой документа
			Upload Requests Rate	Темп файловых запросов, связанных с загрузкой

Название панели	Описание панели	Строка	Панель	Описание панели
				документа, распределённый по статусу
			Upload Requests Latency	Средняя длительность выполнения файловых запросов, связанных с загрузкой документа
		Doc Create Stats	Create Doc Error 500 Ratio	Процентное соотношение ошибочных файловых запросов, связанных с созданием документа
			Create Doc Requests Rate	Темп файловых запросов, связанных с созданием документа, распределённый по статусу
			Create Doc Requests Latency	Средняя длительность выполнения файловых запросов, связанных с созданием документа
		Doc View Stats	View Doc Error 500 Ratio	Процентное соотношение ошибочных файловых запросов, связанных с открытием документа

Название панели	Описание панели	Строка	Панель	Описание панели
			View Doc Requests Rate	Темп файловых запросов, связанных с открытием документа, распределённый по статусу
			View Doc Requests Latency	Средняя длительность выполнения файловых запросов, связанных с открытием документа
		Doc Edit Stats	Open Error Ratio	Процентное соотношение ошибочных файловых запросов, связанных с открытием документа
			Docs Open Rate	Темп файловых запросов, связанных с открытием документа, распределённый по статусу
			Available Document Units	Текущее состояние DU юнитов для открытия документов (активные, всего)
		Doc Export/Print Stats	Export Doc Error 500 Ratio	Процентное соотношение ошибочных файловых запросов, связанных со скачиванием/печатью документа

Название панели	Описание панели	Строка	Панель	Описание панели
			Export Doc Requests Rate	Темп файловых запросов, связанных со скачиванием/печатью документа, распределённый по статусу
			Export Doc Requests Latency	Средняя длительность выполнения файловых запросов, связанных со скачиванием/печатью документа
		File Delete Stats	Delete File 500 Ratio	Процентное соотношение ошибочных файловых запросов, связанных с удалением документа
			Delete File Requests Rate	Темп файловых запросов, связанных с удалением документа, распределённый по статусу
			Delete File Requests Latency	Средняя длительность выполнения файловых запросов, связанных с удалением документа
		File Purge form Trash	Purge File 500 Ratio	Процентное соотношение ошибочных файловых запросов, связанных с

Название панели	Описание панели	Строка	Панель	Описание панели
				очисткой документа из корзины
			Purge File Requests Rate	Темп файловых запросов, связанных с очисткой документа из корзины, распределённый по статусу
			Purge File Requests Latency	Средняя длительность выполнения файловых запросов, связанных с очисткой документа из корзины
		Permissions Stats	Permissions 500 Ratio	Процентное соотношение ошибочных файловых запросов, связанных с выдачей прав на документ
			Permissions Requests Rate	Темп файловых запросов, связанных с выдачей прав на документ, распределённый по статусу
			Permissions Requests Latency	Средняя длительность выполнения файловых запросов, связанных с выдачей прав на документ

Название панели	Описание панели	Строка	Панель	Описание панели
[DO] CO Service Status	Актуальный статус сервисов продукта	-	RabbitMQ	Актуальный статус инстансов сервиса RabbitMQ
			Redis	Актуальный статус инстансов сервиса Redis
			Etcd	Актуальный статус инстансов сервиса Etcd
			Audit	Актуальный статус сервиса Audit
			Boards	Актуальный статус сервиса Boards
			Chatbot	Актуальный статус сервиса Chatbot
			CVM	Актуальный статус сервиса CVM
			DCM	Актуальный статус сервиса DCM
			JOD	Актуальный статус сервиса JOD
			FM	Актуальный статус сервиса FM
			NM	Актуальный статус сервиса NM
			Plugins	Актуальный статус сервиса Plugins
			SDD CU	Актуальный статус сервиса

Название панели	Описание панели	Строка	Панель	Описание панели
				SDD CU
			SDD DU	Актуальный статус сервиса SDD DU
			DPS	Актуальный статус сервиса DPS
			Gateway	Актуальный статус сервиса Gateway
[DO] Log Records	Фиксация логируемых сообщений	-	TimeLine	Количество логируемых сообщений за выбранный промежуток времени.
			RAW Logs	Список логируемых сообщений за выбранный промежуток времени.
[DO] Main errors. Search for errors, warnings	Основные ошибки, возникаемые в сервисах продукта. Поиск логируемых сообщений со статусом error, warning.	-	TimeLine	Количество ошибочных логируемых сообщений за выбранный промежуток времени.
			Errors, Warnings	Список ошибочных логируемых сообщений.
[DO] Profile Dashboard	Профиль нагрузки	-	Profile. Most frequent users operations from profile (SRV)	Профиль. Наиболее используемые пользовательские операции серверных компонент.

Название панели	Описание панели	Строка	Панель	Описание панели
			API Requests Rate	Темп файловых запросов и запросов авторизации.
			FS. Time for FS requests (no get/put/search)	FS. Длительность запросов к Системе Хранилища (без get/put/search)
			Profile. FS. Most frequent users operations from profile (FS)	Профиль. FS. Наиболее используемые пользовательские операции Системы Хранилища.
			SRV. Rest requests time (ms)	SRV. Время выполнения REST запросов (мсек) на стороне серверных сервисов.
			FS. Time for FS requests (no get/put/search) percentiles	FS. Время выполнения запросов (мсек) на стороне Системы Хранилища.
			SRV. Time for SRV clients requests	SRV. Время ожидания REST запросов со стороны клиента, разделённые по методам.
			FS. Count of requests from CO (java) by fscmd	FS. Количество запросов от серверных компонент (Java) в Систему Хранилища.

Название панели	Описание панели	Строка	Панель	Описание панели
			DCM. DU. Maximum collaborators per session	DCM. DU. Максимальное количество коллабораторов сессии редактирования.
			DCM. DU. Count of opening file on DU by mediatype	DCM. DU. Количество открытых файлов на DU распределённых по медиатипу документа.
[DO] Profile Dashboard (users)	Профиль нагрузки (распределение по пользователям)	-	Auth. Count of unique logins used for auth operation	Auth. Количество авторизаций пользователей, объединённых по уникальности логина.
			Auth. Count of not-unique logins used for auth operation	Auth. Количество всех авторизаций пользователей
			FM. Count of unique users used for FM operations	FM. Количество пользовательских операций, объединённых по уникальности логина
			NM. Auth. Maximum number of WS (tabs), opened by users at the same time on one node	NM. Auth. Максимальное количество открытых WebSocket соединений (вкладок браузера) одновременно на одной ноде
			DCM. Count of unique users	DCM. Количество пользователей,

Название панели	Описание панели	Строка	Панель	Описание панели
			opening document	объединённых по уникальности логина, которые открывают документ на редактирование
			DCM. ROM. Count of unique users that have opened ROM files	DCM. ROM. Количество уникальных пользователей, которые просматривают документ
			DCM. Count of unique users who has opened file on DU	DCM. Количество уникальных пользователей, которые редактируют документ
[DO] Doc Conversion Stats	Общая информация о сервисах для конвертации документов. Описание времени, темпа и количества запросов конвертаций	-	Services	Актуальный статус сервисов, используемых при конвертациях
			Conversions count from last cleanup	Количество конвертаций по сервисам (с момента деплоя с cleanup)
		H/W Usage	Memory Usage	Потребление памяти
			CPU Usage	Потребление CPU
		Conversion Stats	Conversions Success Rate	Темп успешных запросов конвертаций (по сервисам)
			Conversions Failure Rate	Темп ошибочных запросов

Название панели	Описание панели	Строка	Панель	Описание панели
				конвертаций (по сервисам)
			CVM HTTP Conversion Time	Время обработки запроса CVM конвертации
			JOD HTTP Conversion Time	Время обработки запроса JOD конвертации
			CVM Tomcat Threads	Количество активных Tomcat потоков в сервисе CVM
			JOD Tomcat Threads	Количество активных Tomcat потоков в сервисе JOD
			Available CU units	Текущее состояние CU юнитов для конвертаций (активные, всего)
			Available Pregen units	Текущее состояние Pregen юнитов для конвертаций (активные, всего)
			Current JOD Conversions	Текущее количество активных JOD конвертаций
			Time to find free CU	Время поиска CU для начала конвертации
			Redis EVALSHA Time	Время выполнения команды в Redis
[DO] Doc Open Stats	Общая информация о сервисах для открытия документов и	-	Services	Актуальный статус сервисов, используемых при открытии документа

Название панели	Описание панели	Строка	Панель	Описание панели
	режима коллаборации. Описание статуса сервисов, времени, темпа и количества запросов открытия документов	-	Opened docs count from last cleanup	Количество открытий документов по сервисам (с момента деплоя с cleanup)
		H/W Usage	Memory Usage	Потребление памяти
			CPU Usage	Потребление CPU
		Docs Open Stats	Docs Open Rate	Темп запросов открытия документов (по сервисам и статусу)
			Documents Distribution by Hosts	Распределение открытия документов по хостам
			Available Document Units	Текущее состояние DU юнитов для открытия документов (активные, всего)
			Top 10 Response Time by URI	Топ 10 файловых запросов, связанных с открытием документа, с самой высокой длительностью выполнения
			Top 10 Storage Requests Response Time	Топ 10 запросов к хранилищу, связанных с открытием документа, с самой высокой длительностью выполнения (по

Название панели	Описание панели	Строка	Панель	Описание панели
				названию и статусу)
			Time to find free DU	Время поиска DU для начала открытия документа
			Redis EVALSHA Time	Время выполнения команды в Redis
[DO] Requests Stats	Общая информация о HTTP запросах к сервисам. Количество ошибок приложения и дополнительная информация для детального поиска	Services Detail	Services Health Basic	Общие формулы вывода информации о статусах сервисов (по сервисам)
			Services Status	Актуальный статус серверных сервисов продукта
			DU Units Status	Актуальный статус количества поднятых DU
			CU Units Status	Актуальный статус количества поднятых CU
		Requests Detail	Requests Rate Basic	Общие формулы вывода информации о темпе выполнения HTTP запросов (по сервисам)
			Success Requests Rate	Темп успешных HTTP запросов
			Error Requests Rate	Темп ошибочных HTTP запросов

Название панели	Описание панели	Строка	Панель	Описание панели
			2xx Status Rate	Темп ошибочных HTTP запросов со статусом 2xx
			4xx Status Rate	Темп ошибочных HTTP запросов со статусом 4xx
			5xx Status Rate	Темп ошибочных HTTP запросов со статусом 5xx
		Exceptions Analysis	Exceptions Basic	Общие формулы вывода информации об ошибках в приложении
			Exceptions by Class Basic	Общие формулы вывода информации об ошибках в приложении с указанием класса, где произошла ошибка
			By Service	Информация об ошибках приложения (посервисам)
			By Service and Action	Информация об ошибках приложения (по сервисам и действиям)
[DO] UX	UX статистика клиентских запросов	-	UX. FM. Users Statistics	UX. FM. Пользовательская статистика. Распределение запросов пользователей по UserAgent.

Название панели	Описание панели	Строка	Панель	Описание панели
			UX. Collaboration Sessions Data	UX. Статистика открытых сессий коллаборации. Распределение открытых документов к количеству пользователей.
[DO] Web Analytics. Documents	Web Аналитика. Статистика Web клиентских сервисов	-	Web_Analytics.Documents.Open. Time for DocumentLayout by file size. (min/average/max)	Время загрузки структуры документа в зависимости от размера документа (мин./среднее/макс.)
			Web_Analytics.Documents.Open. File size by type	Количество открытых документов распределённых по размеру и типу документа
			Web_Analytics.Documents.Open. Durations — 95%	Средняя длительность загрузки сервисов.
[DO] File Manager API Stats	Информация о файловых запросах и авторизациях пользователей	Logins Stats	Logins 500 ratio	Процентное соотношение ошибочных запросов авторизаций ко всем запросам авторизаций
			Logins status amount within 5 min interval	Статус запросов авторизаций, разделённый по 5 мин. интервалу
			Logins Rate	Темп запросов авторизаций
			Logins Latency — 95%	Средняя задержка запросов

Название панели	Описание панели	Строка	Панель	Описание панели
				авторизаций пользователей
		FM Requests Stats	FM Requests Error Ratio	Процентное соотношение ошибочных запросов ко всем запросам, связанным с файловыми операциями и авторизациями пользователей
			FM Connection Threads	Количество активных потоков файлового сервиса
			NGINX Connectionss	Количество активных потоков сервиса авторизаций
			FM Requests Rate	Темп HTTP запросов файлового сервиса
			Top 10 Response Time by URI	Топ 10 файловых запросов с самой высокой длительностью выполнения
			Upload Requests Rate	Темп файловых запросов, связанных с загрузкой документа, распределённый по статусу
			Upload Requests Latency	Средняя длительность выполнения файловых запросов,

Название панели	Описание панели	Строка	Панель	Описание панели
				связанных с загрузкой документа
			FM Requests Latency by Status	Средняя длительность запросов файлового сервиса, распределённых по статусу
		Storage Requests Rate	Storage Requests Rate	Темп запросов к хранилищу, распределённых по названию и статусу
			Top 10 Storage Requests Response Time	Топ 10 запросов к хранилищу с самой высокой длительностью выполнения, распределённых по названию и статусу
[DO] Whiteboards Stats	Общая информация о HTTP запросах к сервису Boards (МояДоска). Количество ошибок приложения и дополнительная информация для детального поиска	App Stats	API Requests Rate	Темп запросов приложения Boards (МояДоска)
			API Requests Latency by Status	Средняя длительность запросов сервиса, распределённых по статусу
			Opened Sockets	Открытые сокеты приложения
		Docker Stats	CPU Usage	Потребление CPU
			Memory Usage	Потребление памяти

Название панели	Описание панели	Строка	Панель	Описание панели
			Network Rx	Передача данных (Получено)
			Network Tx	Передача данных (Передано)
		Go Stats	Total Reserved Memory	Среднее количество байт выделенной памяти среди всех процессов инстансов приложения
			Stack Memory Use	Среднее количество байт стековой памяти среди всех процессов инстансов приложения
			Other Memory Reservations	Среднее количество байт прочей памяти (не стек) среди всех процессов инстансов приложения
			Heap Memory	Среднее количество байт используемой памяти (heap) среди всех процессов инстансов приложения
			Allocation Rate, Bytes	Темп выделения памяти за промежуток времени, в байтах
			Heap Object Allocation Rate	Темп создания объектов за

Название панели	Описание панели	Строка	Панель	Описание панели
				промежуток времени
			Number of Live Objects	Количество «живых» объектов приложения
			Goroutines	Количество активных горутин
			GC min & max duration	Минимальная и максимальная длительность очистки сборщиком мусора (GC)
			Next GC, Bytes	Следующий запуск сборщика мусора (GC), в байтах
[DO] AuthN Dashboard	Информация о запросах авторизации, связанные с внешним SSO способом авторизации			
[DO] Gateway Dashboard	Информация о запросах, проксируемых и проходящих валидацию на стороне Gateway			
Docker Monitoring	Данные о состоянии активных Docker контейнеров			
JVM (Micrometer)	Official Dashboard 4701.Dashboard for Micrometer instrumented applications (Java, Spring Boot, Micronaut)			
Etcd	Officail Dashboard 3070. Etcd Dashboard for Prometheus metrics scraper			
Node Exporter Full	Officail Dashboard 1860.Nearly all default values exported by Prometheus node exporter graphed			
Redis	Official Dashboard 11835.Redis Dashboard for Prometheus Redis Exporter			

4.4.6 Оповещения мониторинга

Оповещения мониторинга (Alerts) срабатывают, когда метрики достигают определенного порога значений. Посмотреть все оповещения можно по ссылке:

```
http://<domain_env>:8880/api/v1/alerts
```

По умолчанию при срабатывании Alerts сервис Alertmanager в VictoriaMetrics не будет отправлять уведомления в виде электронных писем. Подробнее о настройке см. раздел «Настройка оповещений мониторинга».

Правила формирования оповещений представлены в таблице 24.

Таблица 24 — Оповещения CO

Группа правил	Название правила	Описание правила	Порог срабатывания правила	Длительность правила
co backend rules	failed logins exceeds 10% of total count	Соотношение неуспешных авторизаций ко всем авторизациям	Количество неуспешных авторизаций за 5 мин интервал достигло 10% от всех авторизаций	2 мин.
	500 bad request percentage too high	Темп запросов со статусом 500	Темп запросов со статусом 500 за 5 мин интервал достиг больше 2% от всех запросов	5 мин.
	jvm heap warning	Соотношение потребляемой памяти сервиса к максимальной (средства JVM)	Количество потребляемой памяти сервиса достигло больше 80% от максимально выделенной памяти этому сервису	5 мин.
	tomcat threads warning	Количество Tomcat потоков приближается к максимуму	В течение 15 мин. количество Tomcat потоков превысит максимальное количество	5 мин.

Группа правил	Название правила	Описание правила	Порог срабатывания правила	Длительность правила
	du pool is about to become completely occupied	Набор DU для открытия документов вскоре закончится	В течение 1 ч. количество занятых DU приблизится к максимуму	10 мин.
	docs open failures exceeds 10% of total count	Соотношение неуспешных открытий документов ко всем открытиям документов	Количество неуспешных открытий документов за 5 мин интервал достигло 10% от всех открытий документов	5 мин.
co blackbox rules	http(s) probe: status code	Входной балансировщик отвечает для сервисов CO	Ответ от сервиса CO приходит со статусом отличным от 200	5 мин.
	SSLCertExpiringSoon	Сертификат сервисов скоро истекает	До окончания сертификата осталось 7 дней	30 мин.
co main rules	target_liveness	Сервис CO работает	Сервис не работает в течение N мин (длительности правила)	3 мин.
	disk usage: root warning	Соотношение используемого места на диске хоста к максимальному	Количество доступного места достигает 80% < 95% от максимального, либо в течение 8 ч., если ничего не изменится, то количество свободного места станет меньше 0	30 мин.
	disk usage: srv warning	Соотношение используемого места на диске хоста сервисами	Количество доступного места сервисов SRV достигает 80% < 95% от	30 мин.

Группа правил	Название правила	Описание правила	Порог срабатывания правила	Длительность правила
		SRV к максимальному	максимального, либо в течение 8 ч., если ничего не изменится, то количество свободного места станет меньше 0	
	disk usage: root critical	Соотношение используемого места на диске хоста к максимальному	Количество доступного места достигает 95% от максимального, либо в течение 4 ч., если ничего не изменится, то количество свободного места станет меньше 0	30 мин.
	disk usage: srv critical	Соотношение используемого места на диске хоста сервисами SRV к максимальному	Количество доступного места сервисов SRV достигает 95% от максимального, либо в течение 4 ч., если ничего не изменится, то количество свободного места станет меньше 0	30 мин.
	oom kill detected	Произошёл сбой из-за нехватки памяти OOM (Out Of Memory)	Зафиксирован OOM от сервиса в течение 1 мин.	-
	high memory load	Соотношение потребляемой памяти хоста к максимальной (средства Docker)	Количество доступной памяти хоста стало меньше 5% от	30 мин.

Группа правил	Название правила	Описание правила	Порог срабатывания правила	Длительность правила
			максимальной памяти	
	CPU iowait too high	Длительность ожидания IO операций	Среднее время ожидания IO операций в течение 15 мин. достигло 30 сек	30 мин.
	High CPU Load	Нагрузка на CPU	Процентное соотношение загрузки CPU достигло 90%	-
	LA too high	Средняя нагрузка на CPU	Средняя нагрузка на CPU выше текущей нагрузки в 1.5 раз в течение N (длительность правила)	10 мин.

4.4.7 Настройка оповещений мониторинга

Для своевременного уведомления о возникающих неполадках, связанных с сервисами, на почту или webhook-сервер следует настроить оповещения мониторинга при установке системы. Включение и отключение автоматической настройки оповещений при установке выполняется с помощью переменной, указанной в таблице 25.

Таблица 25 — Настройка оповещений мониторинга

Наименование переменной	Расположение переменной	Тип переменной	Значение по умолчанию
victoria_metrics_alerts_enabled	/group_vars/	boolean	true

Дополнительные переменные для настройки сервиса Alertmanager должны быть определены в каталоге `inventory/group_vars/co_infra` в файле `main.yml`. Пример переменных для настройки:

```
```
alertmanager_inhibit_rules:
  - source_matchers: ['severity="critical"']
    target_matchers: ['severity="warning"']
    equal: ['environment', 'instance', 'event']
alertmanager_receivers:
  - name: "email"
    email_configs:
      - send_resolved: true
        to: "{{ alertmanager_email_alert_recipient | default('admin@example.com')
}}"
alertmanager_route:
  group_by: ['alertname']
  group_wait: "30s"
  group_interval: "5m"
  repeat_interval: "30m"
  receiver: "email"
  routes:
    - matchers:
        - 'environment="CO"'
      receiver: "email"
```
```

```
alertmanager_smtp_sender: "alert_sender@example.com"
alertmanager_smtp_smarthost: "smtp.relay.example.com:587"
alertmanager_smtp_auth_identity: ""
alertmanager_smtp_auth_user: "alert_sender@example.com"
alertmanager_smtp_auth_password: "SuperStrongPassword"
alertmanager_smtp_auth_secret: ""
alertmanager_smtp_require_tls: true # false
alertmanager_smtp:
  from: "{{ alertmanager_smtp_sender | default('alertmanager@example.com') }}"
  smarthost: "{{ alertmanager_smtp_smarthost |
default('smtp.example.com:465') }}"
  auth_identity: "{{ alertmanager_smtp_auth_identity | default('') }}"
  auth_username: "{{ alertmanager_smtp_auth_user | default('') }}"

  auth_password: "{{ alertmanager_smtp_auth_password | default('') }}"
  auth_secret: "{{ alertmanager_smtp_auth_secret | default('') }}"
  require_tls: "{{ alertmanager_smtp_require_tls | default(false) }}"
alertmanager_example_vars.yml
```

Важно использовать корректные структуры данных. Если в предоставленном примере значением переменной является список — следует использовать список, если используется словарь — следует использовать словарь. Необходимо убедиться, что названия всех свойств, используемых в конфигурации, соответствуют названиям, описанным в официальной документации, упомянутой выше.

5 ПОРЯДОК ОБНОВЛЕНИЯ

5.1 Очистка данных

При обновлении версии продукта или повторной установке возможно использование переменной `cleanup_all` со значением `true`, которая позволяет очистить все данные на сервере установки, кроме данных мониторинга.

5.2 Сохранение данных мониторинга

В продукте с версии 3.1 появилась возможность частичного сохранения данных мониторинга и журналов событий (расположеных в директориях /elasticserch, /kibana, /grafana, /prometheus). Сохранение выполняется автоматически.

Для удаления данных мониторинга необходимо установить значение true переменной, указанной в таблице 26.

Таблица 26 — Сохранение данных мониторинга

Наименование переменной	Тип переменной	Диапазон значений
force_cleanup_monitoring	boolean	false (значение по умолчанию)

Примеры использования переменной:

1. Для запуска ansible с сохранением данных мониторинга (остальные данные удаляются) следует выполнить следующую команду:

```
ansible-playbook -i hosts.yml playbook/main.yml -e cleanup_all=true
```

По умолчанию значение переменной `force_cleanup_monitoring = false`, при запуске ansible допускается не указывать повторно ее значение.

2. Для запуска ansible с полным удалением данных следует выполнить следующую команду:

```
ansible-playbook -i hosts.yml playbook/main.yml -e cleanup_all=true -e
force_cleanup_monitoring=true
```

При такой команде использование флага `-e force_cleanup_monitoring=true` переопределит значение по умолчанию с `false` на `true`.

5.3 Обновление на версию 3.3

При обновлении на версию 3.3 следует изменить файлы конфигурации в связи с удалением сервиса pregen.

Необходимые изменения:

1. Открыть конфигурационный файл `main.yml` и удалить следующие переменные:

```
pregen_pool_enabled
pregen_pool_size
pregen_heavy_unit_count
pregen_render_timeout
pregen_render_heavy_timeout
pregen_max_memory
pregen_max_memory_heavy
pregen_error_log_sentry_dsn
```

2. Открыть inventory файл `hosts.yml` и удалить строки вида:

```
co_pregen:
hosts:
co-infra-1.installation.example.net:
И внутри группы co_setup:
co_setup:
...
co-pregen-[1:2].installation.example.net:
```

6 ИЗВЕСТНЫЕ ПРОБЛЕМЫ И СПОСОБЫ РЕШЕНИЯ

6.1 Проблема установки модуля python3-libselinux

Описание проблемы:

В некоторых случаях в процессе работы установки на ОС Redos возможно появление следующей ошибки:

```
2023-01-01 12:00:00,001 p=28456 u=root n=ansible | fatal: [10.100.100.100]:
FAILED! => {"changed": false, "msg": "No package matching 'python3-libselinux'
found available, installed or updated",
"rc": 126, "results": ["No package matching 'python3-libselinux' found
available, installed or updated"]}
```

Решение:

Выполнить следующую команду и продолжить установку:

```
sed -i 's@python3-libselinux@libselinux-python3@'\
./_versions/3.1/collections/ansible_collections/nct/system/roles/python3/vars/R{E
D,edHat}.yml
```

6.2 Решение проблемы с логами

При остановке ротации (архивирования) логов сервисов Nginx необходимо обновить политики безопасности на серверах с ролью `openresty-lb-core-wopi`.

Обновления политики безопасности выполняются с помощью команды:

```
restorecon -R /srv/docker
```

После обновления политики необходимо проверить ротацию логов через 48 ч.

Например:

```
[root@jenny ~]# cd /srv/docker/openresty/logs/
[root@jenny logs]# ls
access_full.log access_full.log-20231224-1703378461.gz access.log-20231222-
1703205421.gz  error.log error.log-20231224-1703378461.gz
access_full.log-20231221-1703118661.gz  access_full.log-20231225-1703464201
access.log-20231223-1703290201.gz  error.log-20231221-1703118661.gz  error.log-
20231225-1703464201     access_full.log-20231222-1703205421.gz  access.log
access.log-20231224-1703378461.gz  error.log-20231222-1703205421.gz  nginx.pid

access_full.log-20231223-1703290201.gz  access.log-20231221-1703118661.gz
access.log-20231225-1703464201 error.log-20231223-1703290201.gz
```

6.3 Переполнение диска данными мониторинга

Описание проблемы:

Быстрое заполнение диска при установке standalone или для кластерной установки, на узле кластера с ролью co_infra.

Решение:

Быстрое заполнение диска может происходить при поступлении большого количества данных мониторинга или логирования, из-за неправильно настроенных политик их хранения.

По умолчанию данные мониторинга располагаются в директории `/srv/docker/prometheus/data`. Время хранения данных задается при установке СО с помощью переменной `prometheus_storage_tsdb_retention_time` (по умолчанию "21d", то есть 21 день).

При переполнении диска данными мониторинга база данных Prometheus может быть повреждена. Для восстановления работоспособности необходимо удалить директорию /srv/docker/prometheus/data. После удаления директории следует переустановить роль, ограничив ее опцией -limit, только для роли co_infra и указав сценарий playbooks/infra.yml. Пример команды:

```
ansible-playbook -i playbooks/infra.yml --tags prometheus --limit co_infra
```

Объем данных журнала событий зависит от количества узлов кластера, количества их контейнеров и уровня протоколирования различных сервисов (настраиваются с помощью Etcd). По умолчанию данные журнала событий располагаются в директории `/srv/docker/elasticsearch/data`. Время хранения данных задается при установке СО с помощью переменной `co_logs_retention_days` в файле `~/install_co/group_vars/all/main.yml`. Значение по умолчанию "120d", что означает — 120 дней.

В случае переполнения диска данными журнала событий, предусмотрено удаление более старые индексов вручную (структуры хранения и поиска данных в объеме 1 дня). Для этого на узле с ролью co_infra необходимо выполнить следующие команды:

```
# пароль вводить из переменной elasticsearch_opendistro_admin_password
curl -k --user admin https://localhost:9200/_cat/indices
# выбрать индексы, подлежащие удалению, начинающиеся с "co-"
curl -X DELETE -k --user admin https://localhost:9200/co-<YYYY.MM.DD>
```

Для уменьшения уровня логирования необходимо изменить значения переменных, приведенных в таблице 27.

Таблица 27 — Перечень переменных журнала мониторинга

Наименование переменной	Значение по умолчанию	Значение для уменьшения глубины лога
common_co_log_level	info	warn/error
chatbot_log_level	info	warn/error
cvm_cu_log_level	info	warn/error
cvm_log_level	info	warn/error
dcm_du_log_level	info	warn/error
dcm_log_level	info	warn/error
du_log_level	info	warn/error
du_nps_log_level	info	warn/error
sdd_log_level	info	warn/error

6.4 Ошибка при запуске/перезапуске контейнеров

Описание проблемы:

При запуске docker-контейнеров со статусом Exited появляется ошибка «Id already in use».

Решение:

1. Вывести список процесов с помощью команды:

```
for i in $(docker ps -a -f status=exited --format '.ID'); do ps aux | grep $i |
head -1; done
```

2. Остановить процесссы из списка с помощью следующей команды:

```
for i in $(docker ps -a -f status=exited --format '.ID'); do proc_id=$(ps aux |
grep $i | head -1 | awk '{print $2}'); kill $proc_id; done
```

3. Удалить каталоги с помощью команды:

```
for i in $(docker ps -a -f status=exited --format '.ID'); do rm -
rf /run/docker/containerd/$i*; done
```

4. Проверить имена каталогов, соответствующие ID Exited контейнеров в следующих директориях: /var/run/docker/runtime-runc/moby/ и /run/docker/runtime-runc/moby/.

5. Повторно выполнить удаление каталогов, заменив путь до конечного каталога, с помощью команды:

```
for i in $(docker ps -a -f status=exited --format "{{.ID}}"); do rm -
rf /var/run/docker/runtime-runc/moby/$i*; done
```

6. Запустить Exited контейнеры:

```
docker ps -a -f status=exited --format '.ID' | xargs --no-run-if-empty docker
restart
```

6.5 Настройка кэширования негативных ответов в Unbound

Описание проблемы:

Сервис Unbound использует кэш для хранения негативных ответов на DNS-запросы (например, если домен не существует или не может быть разрешен). По умолчанию ответы сохраняются в кэше на 60 минут, что может привести к задержке повторных попыток обработки запросов, если проблема с разрешением DNS-запросов существует непродолжительное время.

Решение:

Для ускорения обработки ошибок и повторных попыток разрешения DNS-запросов следует уменьшить время хранения негативных ответов, с помощью переменной `cache-max-negative-ttl` в конфигурации сервиса Unbound.

Порядок действий:

1. Откройте конфигурационный файл сервиса Unbound с помощью текстового редактора (путь по умолчанию: `/etc/unbound/unbound.conf`).
2. Установите переменной `cache-max-negative-ttl` значение 2 секунды (или иное значение):

```
cache-max-negative-ttl: 2
```

6.6 Настройка самоподписанного сертификата

Описание проблемы:

При использовании самоподписанных сертификатов возникают ошибки их применения.

Решение:

1. Подключиться к серверу из группы co_infra.
2. Открыть с помощью текстового редактора файл /srv/docker/main_ca/data/ucs-ca.pem
3. Добавить содержимое сертификата, указанного в переменной tls_ca_filename в файл.

4. Необходимо удалить на хостах инсталляции текущий внутренний CA сертификат следующей командой:

```
ansible co -b -m file -a "path={{ tls_main_dir }}/certs/\
{{ ca_main_hostname }}-main-ca.pem state=absent" -i hosts.yml
```

5. Запустить установку системы без очистки данных.
6. Выполнить перезапуск всех CO контейнеров на всех серверах с помощью команды:

```
ansible co -l 'co:!co_etcd:!co_mq:!co_imc:!co_infra' -b -m shell -a \
"docker ps -q | xargs --no-run-if-empty docker restart" -i hosts.yml
```

6.7 Бесконечная перезагрузка redis_6379

Описание проблемы:

Сервис Redis использует режим AOF, в котором сервис не изменяет уже существующие данные, а добавляет новые в конец. Ошибка связана с неверной записью данных, после которой сервис уходит в перезагрузку.

Пример ошибки:

```
Bad file format reading the append only file: make a backup of your AOF file,
then use ./redis-check-aof --fix <filename>
```

Решение:

Для решения следует выполнить одну из двух представленных команд:

1. Установка пакета redis-tools:

```
apt install redis-tools -y docker logs redis_6379 \
| tail | grep redis-check-aof -q && (echo y | redis-check-aof \
--fix /srv/docker/redis_6379/data/appendonly.aof )
```

2. Проверка данных сервиса на диске:

```
docker exec redis_6379 sh -c 'redis-check-aof --fix /data/appendonly.aof'
```

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/*
```

- Закрыть окно и вернуться к строке терминала.
- 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 одну из команд.

- 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.

- 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 28.

Таблица 28 — 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

Флаг	Описание
-days	Указать время действия сертификата в днях

Описание полей при создании сертификата приведено в таблице 29.

Таблица 29 — 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 сохранения 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 30.

Таблица 30 — Значения флагов команды

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

Флаг	Описание
-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
Описание ролей для серверов системы

В данном приложении представлен перечень ролей, используемых для установки системы.

Таблица 31 — Роли для кластерной установки

Наименование	Описание
lb-core-auth	Сервер балансировки нагрузки
infra	Сервер, объединяющий инфраструктурные роли сбора логов и мониторинга. Может содержать роль chatbot
etcd	Подсистема конфигурации с использованием Etcd
core-cvm	Сервис управления импортом, экспортом и индексированием документов
cu-pool	Пул контейнеров с конвертерами документов
core-dcm	Сервер управления редактированием, коллаборации и документного API
du pool	Пул контейнеров с модулями редактирования документов в режиме коллаборации
core-fm	Подсистема сервиса файлового API
core-nm	Подсистема сервиса push-уведомлений
imc	Сервер кеширования сессий и хранения промежуточных результатов в памяти
mq	Сервер очереди сообщений и подписок
core	При сокращенном составе ролей — совмещенные роли *-core-* для Сервера совместного редактирования (ССР)

Таблица 32 — Технические роли

Наименование	Описание
operator	Технологическая роль. Рабочее место, с которого производится установка всех компонентов
LB	Сервер балансировки нагрузки для всех компонентов (используется только при кластерной установке)

Приложение Е

Создание локальных DNS-записей

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` для установки типа standalone:

```
192.168.1.100 co-infra-1.installation.example.net
```

Пример содержимого файла /etc/hosts для кластерной установки:

```
192.168.1.100 co-etcd-1.installation.example.net
192.168.1.101 co-etcd-2.installation.example.net
192.168.1.102 co-etcd-3.installation.example.net
192.168.1.103 co-imc-mq-1.installation.example.net
192.168.1.104 co-imc-mq-2.installation.example.net
192.168.1.105 co-imc-mq-3.installation.example.net
```

Количество записей соответствует количеству используемых физических или виртуальных серверов.

При использовании `/etc/hosts` для создания DNS-записей необходимо добавить в файл `~/install_co/group_vars/co_setup/extra_vars.yml` все записи, перечисленные в `/etc/hosts` для работы локального кеширующего DNS-сервера (Unbound).

Пример записи:

```
unbound_local_zones:
      -  type: "transparent"
         zone: "installation.example.net"
         local_data:
              - domain: "co-etcd-1.installation.example.net"
                type: "A"
               ip: "10.1.2.3"
```