MAILION

Руководство по установке

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

MAILION

РУКОВОДСТВО ПО УСТАНОВКЕ

1.8.1

На 89 листах

Москва

2024

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.

MAILION

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

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

Таблица 1 – Сокращения и расшифровки

Сокращение	Расшифровка
A - запись	Address, одна из ключевых ресурсных записей, используется для связи домена с IP-адресом сервера
DNS	Domain Name System, система доменных имён
FQDN	Fully Qualified Domain Name, полное доменное имя, иногда также называемое абсолютным доменным именем. Это доменное имя, которое указывает точное местоположение домена в древовидной иерархии системы доменных имен (DNS). Включает в себя имена всех родительских доменов иерархии DNS
MX	Mail Exchanger, тип DNS-записи, предназначенный для маршрутизации электронной почты с использованием протокола SMTP
PTR - запись	Pointer, противоположность A-записи для DNS. Связывает IP-адрес сервера с его каноническим именем (доменом). Применяется для фильтрации почты.
Standalone	Конфигурация установки ПО «Mailion» без отказоустойчивости
ДУ	Директория установки
ООО	Общество с ограниченной ответственностью
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

Mailion – корпоративная почтовая система нового поколения на базе микросервисной архитектуры, обеспечивающая обмен электронными сообщениями, планирование рабочего времени, интеллектуальный поиск информации и работу с адресными книгами. Система отличается высокой отказоустойчивостью, способна на быстрое самовосстановление и масштабируемость в зависимости от нагрузок.

В состав продукта входят:

– Почтовая система Mailion для обмена электронными сообщениями, совместной работы с календарями, хранения адресных книг и индексации данных;
– Универсальное приложение Mailion для работы с электронной почтой, календарями, контактными книгами, интеллектуального поиска информации и управления задачами в веб-браузерах и на операционных системах Windows, Linux, macOS;
– «Надстройка для Microsoft Outlook» для работы с почтой, календарем и контактами Mailion в интерфейсе приложения Microsoft Outlook.

Подробное описание возможностей продукта приведено в документе «Mailion. Функциональные возможности».

1.2 Структура ПО «Mailion»

Структура ПО «Mailion» представляет собой набор сервисов, обеспечивающих работу системы и взаимодействие между подсистемами ПО «Mailion».

Сервисы (представленные в виде установочных ролей) описаны в приложении Описание ролей Ansible

Общая логическая схема ПО «Mailion» приведена на рисунке (см. Рисунок 1).

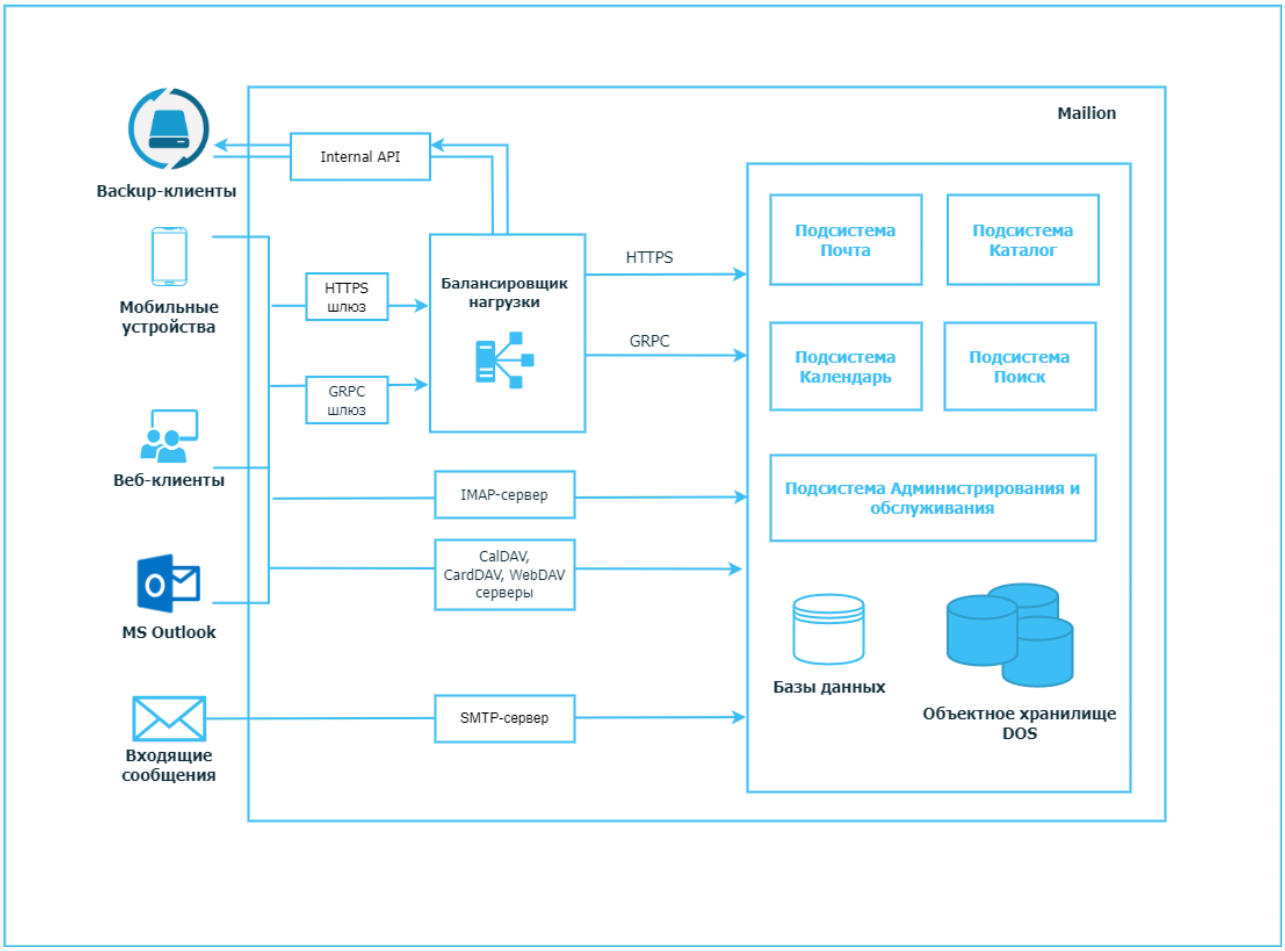


Рисунок 1 – Общая логическая схема ПО «Mailion»

1.3 Требования к квалификации персонала

Администратор ПО «Mailion» должен соответствовать следующим требованиям:

1. Знание основ сетевого администрирования:
   – сетевая модель OSI и стек протоколов TCP/IP;
   – IP-адресация и маски подсети;
   – маршрутизация: статическая и динамическая;
   – протокол обеспечения отказоустойчивости шлюза (VRRP);
2. Опыт работы с подсистемами виртуализации на уровне эксперта:
   – работа с подсистемой контейнерной виртуализации (Docker/Podman);
   – работа с одной из подсистем серверной виртуализации на базе гипервизоров Hyper-V, VMware vSphere ESXi, KVM;
   – навык администрирования операционной системы (ОС) Linux с помощью консоли;
   – опыт работы со службой доменных имен (DNS):

– знание основных терминов (DNS, IP-адрес и так далее);
– понимание принципов работы DNS (корневые серверы, TLD-серверы, серверы имен доменов, разрешающий сервер имен и так далее);
– знание типов записи и запросов DNS;

3. Знание видов архитектуры, а также основных компонентов инфраструктуры открытых ключей (PKI), к которым относятся:

– закрытый и открытый ключи;
– сертификат открытого ключа;
– регистрационный центр (RA);
– сертификационный центр (CA);
– хранилище сертификатов (CR);

4. Практический опыт администрирования на уровне эксперта:

– Redis;
– NATS;
– Prometheus;
– MongoDB;
– Postfix.

5. Опыт работы с подсистемой централизованного управления Ansible.
6. Опыт работы со стандартными офисными приложениями.

1.4 Системные требования

Перечень системных требований к аппаратному и программному обеспечению приведен в Аппаратные требования и Программные требования.

1.4.1 Аппаратные требования

Ниже представлены описание ролей групп серверов, стандартные расчеты аппаратной части, расчет на 10 000 тысяч пользователей, требования к сетевой и дисковой подсистеме.

1.4.1.1 Описание групп сервера

В таблице 2 приведено обоснование выделение машин под группы сервера.

Таблица 2 – Описание групп сервера

Имя группы сервера	Обоснование выделения машин
ucs_frontend	Веб-сервера Mailion и прокси-сервисы клиентских протоколов. Хранят также веб статический контент. Должны быть выделены, так как являются пограничными серверами между внешними сетями и внутренними службами системы или могут быть размещены за пограничным web application firewall
ucs_mail	Сервера, выполняющие приём и отправку писем. Являются точкой, граничащей между внешними сетями и внутренними службами. Рекомендуется не совмещать с веб и прокси серверами, чтобы при отказе или атаке не терять работоспособность в полном объёме. Могут быть размещены за пограничным web application firewall
ucs_apps	Сервера основной группы микросервисов, реализующих основной функционал системы
ucs_balancers	
ucs_calendar	
ucs_catalog	Сервера группы микросервисов, реализующих функционал Каталога. Рекомендуется разделение с остальными ролями для обособления в части безопасности. Нагрузка на эту группу повышенная, так как не только пользователи, но и приложения имеют различные уровни доступа, что постоянно проверяется внутри системы
ucs_converter	Сервера группы подготовки предпросмотра документов, конвертации разных форматов в форматы, готовые для отображения в браузере. Отделены от основной функциональности для обеспечения толерантности к отказу, так как работают напрямую с пользовательскими данными, в которых сложно выполнить предпроверку корректности этих данных и отсутствия уязвимостей
ucs_search	Сервера группы поискового движка, обеспечивающего поиск по письмам, вложениям, каталогу, справке. Индексирование данных ресурсоёмкая задача. Чтобы не делать один огромный сервер, поисковые данные могут быть шардированны, чтобы запросы обрабатывались сразу несколькими экземплярами поиска
ucs_etcd	Сервера группы очередей и хранилищ данных о работе региона. Не имеют тенденции к масштабированию, потому выделены отдельно. Требуют очень быстрые и никем не занятые, с точки зрения обращений, диски
ucs_mq	
ucs_mongodb	Сервера группы баз данных. Требовательны к ресурсам и к гарантиям их наличия
ucs_redis_cache	Сервера группы кэширующих баз данных. Выделены для гарантии обеспечения требуемых ресурсов
ucs_redis_data	
dispersed_object_store	Сервера группы объектного хранилища. Основное хранилище всей системы
ucs_infrastructure	Сервер группы инфраструктуры. Служит для хранения образов инсталляции, сбора журналов доступа и ошибок работы системы, метрик, обеспечивает мониторинг всей системы. Должен быть обособлен для внешнего наблюдения за системой. Его работа не блокирует работу системы

1.4.1.2 Стандартные расчеты аппаратной части

Минимальные требования для установки ПО «Mailion» без отказоустойчивости (Mailion «Standalone») приведены в таблице 3.

> ⚠ Режим и последующая настройка параметров на оборудовании без поддержки отказоустойчивости предоставляется в целях демонстрации функциональности ПО «Mailion». **Данный режим не поддерживается и к использованию не рекомендуется.**

Таблица 3 – Минимальные требования (установка без отказоустойчивости)

Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
Mailion «Standalone»					1	12	16	-	50
ИТОГО:					**1**	**12**	**16**	**0**	**50**

Минимальные требования для установки ПО «Mailion» для отказоустойчивой (кластерной) установки приведены в таблице 4.

Таблица 4 – Минимальные требования (отказоустойчивая установка)

Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ucs_frontend	6	6	10	10	2	12	12	20	20
ucs_mail									
ucs_apps	8	8	10		2	16	16	20	
ucs_catalog									
ucs_calendar									
ucs_balancers									
ucs_converter									
ucs_search	16	18	10	15	3	48	54	30	45
ucs_etcd									
ucs_mongodb									
ucs_redis_cache									
ucs_mq									
ucs_redis_data									
dispersed_object_store	3	4	20	4	4	12	12	80	16
ucs_infrastructure	4	8	100		1	4	8	100	

Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ИТОГО:					**12**	**92**	**102**	**250**	**81**

Рекомендованные требования для установки ПО «Mailion» на отказоустойчивом оборудовании приведены в таблице 4.

Таблица 5 – Рекомендованные требования (отказоустойчивая установка)

Имя роли сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ucs_frontend	4	4	10		2	8	8	20	
ucs_mail	4	4		10	4	16	16		40
ucs_catalog	8	8	10		2	16	16	20	
ucs_apps	8	8	10		2	16	16	20	
ucs_calendar									
ucs_balancers									
ucs_search	4	8		30	3	12	24		90
ucs_converter	4	8		30	3				
ucs_etcd	8	16		30	3	24	48		90
ucs_mongodb									
ucs_mq									
dispersed_object_store	4	4	60	10	4	16	16	240	40
ucs_redis_data	8	8		10	3	24	24		30
ucs_redis_cache									
ucs_infrastructure	4	8	200		1	4	8	200	
ИТОГО:					**26**	**144**	**184**	**510**	**290**

1.4.1.3 Расчёт требований для 10 000 пользователей

Расчет требований для 10 000 пользователей ПО «Mailion» приведен в таблице 6.

Таблица 6 – Расчет требований для 10 000 пользователей

Примечания	Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
		на каждую роль					итого на группу			
Веб-сервера Mailion и прокси-сервисы клиентских протоколов, работающие в DMZ	ucs_frontend	**6**	**6**	**50**	**50**	**2**	**12**	**12**	**100**	**100**
ВМ, выполняющие приём и отправку писем, работающие в DMZ	ucs_mail									
Блок ВМ приложений, обеспечивающих основную функциональность	ucs_apps	**8**	**8**	**50**	**0**	**2**	**16**	**16**	**100**	**0**
	ucs_balancers									
	ucs_calendar									
Блок ВМ приложений Каталога	ucs_catalog									
Блок ВМ подсистемы предпросмотра документов	ucs_converter									
Блок ВМ поисковой подсистемы	ucs_search	**8**	**32**	**50**	**256**	**3**	**24**	**96**	**150**	**768**
ВМ группы очередей и хранилищ данных о работе региона	ucs_etcd	**16**	**32**	**50**	**201**	**3**	**48**	**96**	**150**	**603**
	ucs_mq									
ВМ группы баз данных	ucs_mongodb									

Примечания	Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
		на каждую роль					итого на группу			
ВМ группы хранилищ	dispersed_object_store	**4**	**8**	**3471**	**24**	**4**	**16**	**32**	**13883**	**95**
ВМ группы кэширующих баз данных	ucs_redis_cache ucs_redis_data	**8**	**8**	**0**	**50**	**3**	**24**	**24**	**0**	**150**
ВМ инфрастуктуры. Является хранилищем всех образов инсталяции, сервером мониторинга, логколлектором	ucs_infrastructure	**4**	**8**	**300**	**0**	**1**	**4**	**8**	**300**	**0**
					ИТОГО:	**18**	**144**	**284**	**14684**	**1716**

Параметры расчета приведены в таблице 7.

Таблица 7 – Параметры расчета

Параметр	Значения	Заполнить	Комментарий
Количество пользователей	10000	да	
Квота на ящик, Гб	1	да	
Избыточность данных DOS: d-сегменты	2	да	Количество сегментов самих данных, при использовании кодов Рида-Соломона, которые будут записаны в хранилище
Избыточность данных DOS: p-сегменты	1	да	Количество избыточных сегментов, при использовании кодов Рида-Соломона, которые будут записаны в хранилище
Фактор репликации данных DOS	3	да	Фактор репликации для индексов DOS (количество полных копий записи индекса)
Фактор репликации данных мета данных	3	да	Фактор репликации для мета данных (заголовки, участники, пр) СУБД Mailion
Процент заполнения квоты ящика	100,00%	нет	

Параметр	Значения	Заполнить	Комментарий
Избыточность данных DOS (d+p)	3	нет	Итоговая избыточность хранилища
Количество писем, шт	20971520	нет	

Дополнительные пояснения приведены в таблице 8.

Таблица 8 – Дополнительные пояснения

Данные, помеченные цветом	Пояснения
	для данных в ячейках, отмеченных этим цветом, нужно 2 или более блочных устройств. Рекомендуются физические устройства, которые не требуют резервирования на уровне RAID массива на хостовой системе
	все ресурсы указаны с расчётом работы ОС ВМ

1.4.1.4 Требования к дисковой подсистеме

Требования к дисковой подсистеме приведены в таблице 9.

Таблица 9 – Характеристики дисков

Тип диска	min IOPS read	min IOPS write	IOPS/GB read	IOPS/GB write	latency (clat) ms
HDD	300	150	1	1	<12
SSD	200000	80000	1700	700	<1

1.4.1.5 Требования к сетевой подсистеме

Между серверами (виртуальными машинами) должен быть канал в 1Гб/с и предельное время ожидания (Network latency) 5-7ms.

1.4.2 Программные требования

Требования к программному обеспечению для места оператора, на котором производится установка, приведены в таблицах 10, 11.

Таблица 10 – Требования к программному обеспечению для места оператора

Требование	Описания
Поддерживаемые браузеры	Перечень поддерживаемых браузеров приведен в документе «Mailion. Системные требования»
Python3	v. 3.6+

Требование	Описания	
Модули Python	jmespath	
	jinja2	необходима версия v.2.10 и выше (обновление для CentOS можно выполнить с любого репозитория OpenStack: http://mirror.centos.org/centos/7/cloud/x86_64/openstack-train/ или https://mirror.yandex.ru/centos/7/cloud/x86_64/openstack-train/)
	ansible	2.11 или новее, но до 2.12
	netaddr	python3-netaddr
	dnspython	
	hvac	
	pymongo	Не ниже версии 3.12
Дополнительные пакеты	mongodb-mongosh	Необходима версия 1.6.2 https://www.mongodb.com
	epel-release	Extra Packages Enterprise Linux, https://docs.fedoraproject.org/en-US/epel/

Перед установкой должен быть скачан и смонтирован образ Mailion

Таблица 11 – Требования к программному обеспечению для серверов, на которые производится установка

Требование	Описание
ОС	Перечень поддерживаемых ОС приведен в документе «Mailion. Системные требования»
Стандартные репозитории ОС	Подключение всех стандартных репозиториев ОС либо их зеркал во внутренней сети для установок в закрытом контуре
репозиторий epel (для Centos 7)	Подключение локальной копии репозитория для установок в закрытом контуре
Репозитории elrepo и docker-ce, ppa:canonical-kernel-team/ppa	Подключение репозиториев **elrepo** (http://elrepo.org) и **docker-ce** (https://download.docker.com/linux/centos/docker-ce.repo) для установки соответствующих пакетов ядра Linux и ПО **docker**, не входящих в состав поставки для установок в закрытом контуре
Доступ	Для каждого сервера, на котором выполняется установка, должен быть обеспечен SSH-доступ: − с sudo привилегиями (ALL=(ALL) NOPASSWD: ALL); − без пароля (доступ по ключу)
Рекомендации по версии ядра Linux	Требуется ядро mainline (обновляется по умолчанию, если не передан флаг **UPGRADE_KERNEL=false**). С более старыми версиями ядер (lts) работоспособность не гарантируется из-за особенностей **Docker** (требуется полная поддержка cgroup2 в ядре).

1.5 Требования к работе DNS

1.5.1 Организация работы сервисов разрешения имен

Во время установки производится настройка и запуск локального кэширующего DNS-сервера (**unbound**) на машинах группы **ucs_etcd**. Он используется для запросов только внутри инсталляции и подключается для контейнеров и самих серверов через соответствующие параметры групповых переменных. С настройками инсталлятора по умолчанию серверы будут перенастроены на работу через **unbound** и не будут принимать параметры серверов разрешения имен по **DHCP**. Поэтому важно направить **unbound** на внутренние DNS-серверы компании, если есть такая необходимость. По умолчанию **unbound** настроен на перенаправление запросов на адреса 8.8.8.8 и 1.1.1.1.

1.5.2 Разрешение имен на машине оператора

Перед установкой необходимо убедиться, что на машине оператора доступен и подключен DNS-сервер, в котором созданы записи, согласно разделу Настройка внешних DNS-записей.

Должны быть доступны DNS-записи для машин группы **ucs_db**. При необходимости на машине оператора необходимо отредактировать файл `/etc/hosts` и внести в него соответствующие сопоставления имен и адресов. Пример приведен ниже.

Здесь и далее: **<install_domain_name>** - это доменное имя инсталляции, описанное в разделе Конфигурирование файла hosts.yml

```
192.168.0.1 ucs-db-1.<install_domain_name>
192.168.0.1 mongodb.ucs-db-1.<install_domain_name>
.......
192.168.0.n ucs-db-n.<install_domain_name>
192.168.0.n mongodb.ucs-db-n.<install_domain_name>
```

Проверить разрешение имени машины в адрес можно с помощью команды:

```
> dig A mongodb.ucs-db-1.<install_domain_name>
; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> A mongodb.ucs-db-
1.<install_domain_name>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- 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:
;mongodb.ucs-db-1.<install_domain_name>. IN A

;; ANSWER SECTION:
mongodb.ucs-db-1.<install_domain_name>. 900 IN CNAME ucs-db-
1.<install_domain_name>.
ucs-db-1.<install_domain_name>. 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
```

Секция **ANSWER SECTION** показывает, что имя разрешается в адрес:

```
mongodb.ucs-db-1.<install_domain_name>. 900 IN CNAME ucs-db-
1.<install_domain_name>.
ucs-db-1.<install_domain_name>. 900 IN        A   192.168.0.1
```

1.5.3 Формирование внешних доменных имен инсталляций

При установке системы есть возможность указывать метод формирования доменных имен инсталляции. Шаблон, который формирует итоговый вариант всех DNS-записей, на которых будет работать инсталляция, принимает на вход два параметра:

- значение переменной: **mailion_external_domain** – отображает основной домен, на котором будет работать инсталляция;
- значение переменной: **mailion_domain_module** – отображает способ формирования доменного имени.

Пример работы шаблона приведен в таблице 12.

Таблица 12 – Примеры работы шаблона

mailion_domain_module	Имя ссылки	mailion_external_domain	Результат
{service}.{domain}	Auth	test.example.com	auth.test.example.com
{service}-{domain}	Auth	test.example.com	auth-test.example.com
{service}-xz-1.{domain}	Auth	test.example.com	auth-xz-1.test.example.com

Таким образом, можно гибко настраивать принцип формирования доменных имен инсталляции. Это может пригодиться, например, если имеется Wildcard SSL сертификат на доменное имя **example.com** и ***.example.com**, но нет на ***.test.example.com**. Можно

установить **mailion_domain_module** в значение **{service}-{domain}** и получить домены третьего уровня, которые подходят под текущий Wildcard SSL сертификат.

1.5.4 Необходимые DNS записи

1.5.4.1 Внешние DNS-записи

В таблицах 13, 14 приведены все необходимые внешние DNS-записи, требуемые для инсталляции. Данная таблица сформирована для параметра **mailion_domain_module** со значением **{service}.{domain}** (т.е. формирование ссылок через точку к указанному домену). Если выбран другой метод формирования, необходимо соотнести его со значениями в таблицах ниже.

Таблица 13 – Сведения о внешних DNS-записях

Имя записи	Тип записи	Значение	Комментарии
api	CNAME	@	
auth	CNAME	@	
autoconfig	CNAME	@	
avatars	CNAME	@	
caldav	CNAME	@	
carddav	CNAME	@	
db	CNAME	@	
@	A	<ucs_frontend_vip>	Значение должно быть равно VIP-адресу между серверами с ролью **ucs_frontend** или адресу самого сервера этой группы, если производится установка без отказоустойчивости
@	TXT	"v=spf1 mx a:relay.<mailion_external_domain> ~all"	Необходимо указать сформированное имя, с учетом значения в словаре **mailion_external_domain**
@	MX	10 <mx1>	MX-запись указывает на A-запись в которой содержится адрес первого сервера из группы **ucs_mail**
@	MX	10 <mx2>	MX-запись указывает на A-запись в которой содержится адрес второго сервера из группы **ucs_mail** (и т.д.)
grpc	CNAME	@	
imap	CNAME	@	
mail	CNAME	@	
mail._domainkey	TXT	"v=DKIM1; k=rsa; p=<DKIM_KEY>"	Значение **DKIM_KEY** определяется на этапе установки
mx1	A	<ucs_mail_mx[0]>	Внешний IP-адрес, по которому доступен первый сервер из группы **ucs_mail**
mx2	A	<ucs_mail_mx[1]>	Внешний IP-адрес, по которому доступен второй сервер из группы

Имя записи	Тип записи	Значение	Комментарии
			ucs_mail (и т.д.)
preview	CNAME	@	
relay	A	<ucs_mail_relay_vip>	Значение должно быть равно VIP-адресу между серверами с ролью ucs_mail или адресу самого сервера этой группы, если производится установка без отказоустойчивости
resources	CNAME	@	
secured	CNAME	@	
smtp	A	<ucs_mail_vip>	
_adsp._domainkey	TXT	"dkim=all"	

Таблица 14 – Сведения о внешних DNS-записях

Имя записи	Тип	Приоритет	Вес	Порт	Адрес
_autodiscover._tcp	SRV	0	0	443	<mailion_external_domain>.
_caldavs._tcp	SRV	0	0	6787	caldav.<mailion_external_domain>.
_carddavs._tcp	SRV	0	0	6787	carddav.<mailion_external_domain>.
_grpcsec._tcp	SRV	0	0	3142	grpc.<mailion_external_domain>.
_imap._tcp	SRV	0	0	143	imap.<mailion_external_domain>.
_imaps._tcp	SRV	10	0	993	imap.<mailion_external_domain>.
_smtps._tcp	SRV	10	0	465	smtp.<mailion_external_domain>.
_submission._tcp	SRV	0	0	587	smtp.<mailion_external_domain>.
_submissions._tcp	SRV	10	0	465	smtp.<mailion_external_domain>.

Примеры написания DNS-записей приведены в приложении Пример написания внешних DNS-записей.

1.5.4.2 Внутренние DNS-записи

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

Это поведение можно переопределить, если заполнить все адреса вручную на основе примеров в файле групповых переменных или если не использовать **Ansible** и заполнить все необходимые записи во внешнем DNS-сервере. При подобном варианте необходимо создать «A» - записи для каждого сервера, вписанного в файл **inventory**, а также CNAME адреса на все поддомены (“*”) к каждому серверу, вписанному в **inventory**.

Пример заполнения таких записей приведен в таблице 15.

Таблица 15 – Пример заполнения

Имя записи	Тип записи	Значение
infra-01	A	10.10.1.110
*.infra-01	CNAME	infra-01

unbound не должен быть доступен из внешней сети

Использование **unbound** необязательно. Если при заполнении файла с параметрами групповых переменных выставляется параметр **mailion_use_unbound: False**, то **unbound** будет установлен, но не будет принимать участия в работе ПО «Mailion».

1.6 Рекомендации

1.6.1 Рекомендации по использованию файловых систем

В соответствии с рекомендациями производителей операционных систем рекомендуется для ОС CentOS использовать файловую систему XFS.

1.6.2 Рекомендации по разметке дисков

При разметке дисков требуется учитывать следующее:

- все рекомендуемые аппаратные требования приведены в разделе Аппаратные требования, в соответствии с приведенными в разделе таблицами для разных типов установки будут разные требования по выделяемому дисковому пространству;
- для всех серверов рекомендуется оставлять не менее 20 Гб на корневой раздел для штатной работы ОС.
- для роли **ucs_infrastructure** или инсталляции в режиме «Standalone» рекомендуется выделить 50 Гб на корневой раздел, так как во время установки все образы инсталляции предварительно копируются в локальное хранилище docker (`/var/lib/docker/`);
- для всех серверов рекомендуется выделять отдельный раздел /srv, в который происходит установка компонентов системы, и переполнение которого не приведет к аварийной работе самой ОС. В этот раздел также могут быть направлены копии журналов работы компонентов, при соответствующей настройке лог-коллектора, что потребует дополнительного дискового пространства;
- для сервера роли **dispersed_object_store** рекомендуется выделять независимые диски HDD для серверной части и диски SSD под метаданные. Например:
    - **/srv/docker/dispersed_object_store/data/metadata/** – SSD, индексы документов и сегментов;

- **/srv/docker/dispersed_object_store/data/disk1/{blob,rocksdb}** – HDD1, бэкенд1 – блоб и индекс бэкенда;
- **/srv/docker/dispersed_object_store/data/disk2/{blob,rocksdb}** – HDD2, бэкенд2 – блоб и индекс бэкенда;

– распределение сегментов (data segments) + (parity segments):

- сумма data segments + parity segments не должна превышать количества независимых дисков в серверной части хранилища;
- не менее 2 + 1 независимых дисков в серверной части хранилища;
- для кластера из трех машин минимально допустимые значения – 2 (data segments) + 1 (parity segments) сегментов.

1.7 Ограничения

1.7.1 Ограничения при выполнении кластерной установки

При кластерной установке ПО «Mailion» можно выделить отдельный сервер для каждой роли или совместить несколько ролей на одном сервере. Необходимо учитывать, что некоторые серверные роли могут быть не совместимы с другими ролями.

Пример совместимости ролей приведен в таблице 16.

Таблица 16 – Совместимости ролей

Имя роли сервера	Совместимость с другими ролями сервера
ucs_calendar	Совместимы с другими ролями
ucs_balancers	
ucs_mq	
ucs_mail	Несовместимы с ролями **ucs_mongodb**, **ucs_etcd**, **ucs_redis_cache**, **ucs_redis_data**
ucs_apps	
ucs_catalog	
ucs_converter	
ucs_etcd	Несовместимы с ролями **ucs_apps**, **ucs_mail**, **ucs_converter**, **ucs_catalog**
ucs_mongodb	
ucs_redis_cache	
ucs_redis_data	
ucs_frontend	Несовместимы с другими ролями
ucs_search	
dispersed_object_store	
ucs_infrastructure	

Не рекомендуется совмещать серверные роли при установке

1.7.2 Ограничение по работе с файлом inventory

В файл `hosts.yml` вносятся только полностью определенные имена доменов (FQDN). Эти имена будут использоваться во время и после установки системы для обращения к внутренним сервисам. Часть логики установщика использует их для формирования доменных имен и адресов сервисов.

1.7.3 Ограничение по работе с Ansible

В подсистеме управления конфигурациями не должно быть предыдущих конфигурационных файлов самой подсистемы. В том числе конфигурационного файла, который по умолчанию устанавливается с пакетом (например, `/etc/ansible/ansible.cfg`). Такой файл требуется удалить либо перезаписать образцом из поставляемого ПО. Подробнее см. в https://docs.ansible.com/ansible/latest/reference_appendices/config.html#the-configuration-file.

Важно самостоятельно установить необходимые модули python из раздела Программные требования, так как они не являются частью поставки системы.

1.7.4 Ограничение по работе с системами виртуализации

Следующие системы виртуализации поддерживаются для обеспечения работы ПО «Mailion»:

- VMware;
- KVM.

1.7.5 Ограничение по работе с хостами MX

Каждый хост MX должен иметь PTR-запись для обеспечения правильной фильтрации писем антиспам-системой.

1.7.6 Ограничение при заполнении файлов переменных

При заполнении инвентарного файла имя **tier** (#SECTION 2) должно всегда начинаться с «ucs_».

1.7.7 Ограничение при использовании данных внешнего каталога

Необходимо использовать учетные данные внешнего LDAP-каталога для авторизации и отправки писем в ПО «Mailion». Если пользователь хочет отправить письмо на адрес **test@installation.net**, то письмо не отправится, так как на домене **installation.net** нет

почтового сервиса. Поэтому необходимо заменить доменную часть в Email при отправке письма.

Например, в ПО «Mailion» создан домен **ipa.example.installation.net**, на нем есть почтовый сервис и он связан с **example.ru** через поле **x_external_names** в базе данных. Соответственно, отправить письмо необходимо на адрес **test@ipa.example.installation.net**.

Важно. Если этот пользователь еще не был создан в ПО «Mailion» (а при отправке письма на почту из внешнего каталога в ПО «Mailion» создается пользователь, если он еще не был синхронизирован), то для того, чтобы была возможность в будущем под ним авторизоваться, необходимо использовать для входа не адрес **test@ipa.example.installation.net**, на который осуществлялась отправка письма, а **test@installation.net** по причине того, что такой Email заведен во внешнем каталоге.

1.8 Типовые схемы установки

ПО «Mailion» может быть представлено следующими типами установки:

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

2 ПЕРВИЧНАЯ УСТАНОВКА

2.1 Дистрибутив

Дистрибутив Mailion поставляется в виде файла образа ISO с именем `Mailion_[RELEASE].iso`.

После копирования инсталляционного архива необходимо проверить его контрольную сумму MD5 и SHA256, сверив ее с полученной от вендора ПО.

Образ дистрибутива предварительно монтируется командой:

```
mount Mailion_[RELEASE].iso /mnt/disk
```

В состав дистрибутива ПО «Mailion» входят:

1. Установщик рабочего места оператора (`mailion_ansible_bin_[RELEASE].run`).
2. Установщик окружения для проведения установки, включающий все необходимые образы и пакеты (`mailion_infra_[RELEASE].run`).
3. Файлы EULA (End-user license agreement).
4. Файлы TPL (Third-party license).

Где `[RELEASE]` - имя текущего релиза.

2.2 Подготовка к установке

В данном разделе приведена последовательность действий, которую необходимо произвести перед установкой Mailion.

2.2.1 Описание ролей Ansible для преднастройки серверов перед установкой

Ansible применяется для автоматизации настройки и развёртывания сервисов. Список ролей ansible для ПО «Mailion» приведен в таблице 17.

Таблица 17 – Описание общих ролей Ansible для преднастройки серверов перед установкой

Наименование роли	Описание
authorized_keys	Добавляет указанные ssh-ключи для выбранных пользователей на серверы группы **play_hosts**
hostname	Устанавливает **hostname** для выбранных серверов
SELinux	Проверяет режим работы **SELinux** и переключает его в режим «enforcing»3
packagemanager	Настраивает пакетный менеджер
locale	Устанавливает параметры **locale** на серверах
timezone	Устанавливает часовой пояс на серверах

Наименование роли	Описание
sshd	Производит настройку службы удаленного доступа **sshd**
chrony	Устанавливает и настраивает службу синхронизации времени **chronyd4**
timesyncd	Устанавливает и настраивает службу синхронизации времени **timesyncd5**
sysctl	Устанавливает требуемые параметры ядра на серверах
limits	Настраивает параметры ограничений на серверах
kernel_ml	Устанавливает пакет **kernel_ml** последнего доступного ядра
kernel_ml_deb	Устанавливает пакет **kernel_ml** последнего доступного ядра для ubuntu
rsyslog	Устанавливает и настраивает сервис сбора журналов
docker	Устанавливает и настраивает **Docker**, подключает к **docker registry**
unbound	Устанавливает и настраивает кэширующий DNS-сервер
iptables	Устанавливает и настраивает службы межсетевого экрана с параметрами, требуемыми для конкретной роли
resolv	Производит настройку файла **resolv.conf**
package_tools	Добавляет требуемые пакеты для работы ПО «Mailion» в целевую ОС

Роли, используемые для подготовки ПО «Mailion» описаны далее в таблице 18.

Таблица 18 – Описание ролей, используемых при подготовке ПО «Mailion»

Наименование роли	Описание
keepalived	Устанавливает и запускает службу, реализующую протокол VRRP
cAdvisor	Устанавливает сервис **cAdvisor**, осуществляющий сбор метрик работы контейнеров
node_exporter	Устанавливает сервис **node_exporter**, осуществляющий сбор метрик работы сервера
node_cert_exporter	Мониторинг срока действия сертификатов
node_filestat_exporter	Мониторинг появления дампов памяти
blackbox_exporter	Мониторинг доступности веб-интерфейса
syslog_ng	Устанавливает сервис централизованного сбора журналов работы системы
logrotate	Настраивает ротацию хранимых журналов работы системы
ca	Устанавливает и настраивает сервис внутреннего центра сертификации
alertmanager	Устанавливает и настраивает сервис оповещений о событиях мониторинга
devkalion	Устанавливает и настраивает сервис автообнаружения сервисов инсталляции для мониторинга
gesiona	Устанавливает и настраивает сервис, экспортирующий список сервисов инсталляции для сервиса мониторинга
prometheus	Устанавливает и настраивает сервис мониторинга
grafana	Устанавливает и настраивает сервис отображения данных мониторинга инсталляции
kunkka	Устанавливает и настраивает сервис отображения данных о запущенных контейнерах на каждом сервере и их конфигурационных файлов

Наименование роли	Описание
plugin_certificate	Роль, выписывающая сертификат для сборки клиентских приложений **outlook plugin**
etcd	Устанавливает базу данных **etcd**
hydra	Устанавливает и настраивает сервис обнаружения и балансировки нагрузки gRPC
nats	Устанавливает и настраивает **NATS**
nats_exporter	Сбор метрик мониторинга с **NATS**
mongodb	Устанавливает и настраивает документоориентированную СУБД
mongodb.mailion_migration	Устанавливает миграции данных сервисов в базах **MongoDB**
mongodb_exporter	Сбор метрик мониторинга с **MongoDB**
dorofej	Роль работы с модулем **Ansible**, реализующим первичную миграцию СУБД
redis	Устанавливает и настраивает кластер хранилищ **Redis**
theseus	Устанавливает и настраивает сервис работы с учетными данными
perseus	Устанавливает и настраивает сервис хранения контактов
erakles	Устанавливает и настраивает сервис работы с сущностями
odusseus	Устанавливает и настраивает сервис работы с регионами
talaos	Устанавливает и настраивает сервис работы с тенантами
daidal	Устанавливает и настраивает сервис работы с доменами
minos	Устанавливает и настраивает сервис работы с сессиями
ektor	Устанавливает и настраивает сервис работы со связями, сущностями
pasifae	Устанавливает и настраивает сервис подсказок при поиске
dispersed_object_store	Устанавливает и настраивает объектное хранилище, предоставляющее gRPC-интерфейс для хранения бинарных данных и метаданных
achill	Устанавливает и настраивает сервис работы с аватарками
jod	Устанавливает и настраивает сервис для конвертации документов
pregen	Устанавливает и настраивает сервис для конвертации документов
cvm	Устанавливает и настраивает сервис для конвертации документов
cu	Устанавливает и настраивает сервис для конвертации документов
sdd	Устанавливает и настраивает сервис для конвертации документов
meepo	Устанавливает и настраивает сервис генерации превью
mailbek	Устанавливает и настраивает сервис проксирования запросов к шардированным данным на экземплярах поисковой системы
dirbek	Сервис поиска по каталогу
helpbek	Устанавливает и настраивает поисковый сервис по имеющейся веб-документации инсталляции
tripoli	Устанавливает и настраивает единый индексно-поисковый сервис
rspamd	Устанавливает и настраивает сервис антиспама
zeus	Устанавливает и настраивает сервис, отвечающий за шаблонизацию и настройку работы с письмами
paranoid	Устанавливает и настраивает сервис, реализующий протоколы **Postfix Policy Delegation** и **Nginx HTTP Auth**

Наименование роли	Описание
woof	Устанавливает и настраивает сервис, реализующий метод **search** протокола LDAP для резолвинга групповых адресов, алиасов, получения списка доменов со стороны **postfix**
ariadne	Сервис аутентификации для MTA
lmtp	Устанавливает и настраивает сервис, реализующий протокол **lmtp**
postfix	Устанавливает роль для развертывания почтового сервера (**MTA**)
nginx	Устанавливает и настраивает сервер nginx в режиме **smtp**
kongur	Устанавливает и настраивает сервис, отвечающий за работу календарных событий
mars	Сервис для взаимодействия со ПО Squadus (создание и редактирование чатов и конференций)
kex	Устанавливает и настраивает сервис проксирования запросов к внешним календарям
thoth	Устанавливает и настраивает сервис сохранения полей
ares	Устанавливает и настраивает сервис для взаимодействия с системами видеоконференций
othrys	Устанавливает и настраивает взаимодействия с внешними календарными серверами
elysion	Устанавливает и настраивает сервис выполнения асинхронных работ в календаре
mosquito	Устанавливает и настраивает сервис, предоставляющий абстракцию pub/sub над **AMQP**
viper	Устанавливает и настраивает сервис для сохранения писем в системе
razor	Устанавливает и настраивает сервис для отправки писем по шаблону с локализацией
weaver	Устанавливает и настраивает сервис для построения всего сообщения (его web-представления) или его части (для **IMAP**)
marker	Устанавливает и настраивает сервис для управления тегами
hog	Устанавливает и настраивает сервис для получения и сохранения настроек пользователей
beef	Устанавливает и настраивает сервис для сохранения и получения метаданных писем
mixer	Устанавливает и настраивает сервис для получения объектов веб-интерфейсом
atlas	Устанавливает и настраивает сервис для отправки почтовых сообщений
kronos	Устанавливает и настраивает сервис, предназначенный для регистрации задач на отложенное исполнение операций
clotho	Устанавливает и настраивает сервис для хранения истории изменений объектов и тегов
orpheus	Устанавливает и настраивает сервис проксирования аутентификации и поиска сущностей
iason	Устанавливает и настраивает сервис контроля за регистрацией внешних пользователей
cleanup	Производит полное удаление выбранных компонентов (при необходимости)
imap	Устанавливает и настраивает сервис, реализующий протокол **IMAP**
cox	Устанавливает и настраивает **proxy grpc** сервис
house	Устанавливает и настраивает веб-сервер

Наименование роли	Описание
ararat	Устанавливает и настраивает сервис для работы десктопных и мобильных клиентов с календарем по протоколу CalDAV/CardDAV
leda	Устанавливает и настраивает LDAP прокси сервер
sophokles	Устанавливает и настраивает сервис авторизации
dafnis	Устанавливает и настраивает сервис квот
iolaos	Устанавливает и настраивает сервис создания динамических групп
homeros	Устанавливает и настраивает сервис аудита действий пользователя.
adonis	Устанавливает и настраивает сервис для административных функций ministerium
etcd.etcd_backup	Настройка автоматического резервного копирования для **etcd**
mongodb.mongodb_backup	Настройка автоматического резервного копирования для **MongoDB**
sreindexer	Настройка инструмента для переиндексации поиска
nats.nats_backup	Настройка автоматического резервного копирования **NATS**
themis	Устанавливает и настраивает сервис для генерации ссылок или занятость пользователей

2.2.2 Подготовка инфраструктуры установки

Для подготовки инфраструктуры установки должны быть проведены следующие действия (последовательность не важна):

- Установка хранилища образов **Docker** (**docker_registry**) на машине **ucs-infrastructure**, см. раздел Установка хранилища образов Docker.
- Установка подсистемы управления конфигурациями (**Ansible**) на машине оператора, см. раздел Установка конфигурационных файлов Ansible.

2.2.2.1 Установка хранилища образов Docker (docker_registry)

Установка производится на сервере с ролью **ucs_infrastructure**. Перед началом установки проверить, что вход выполнен под пользователем **root**.

Для установки необходимо:

1. Скопировать файл `mailion_infra_[RELEASE].run` в домашний директорий пользователя.
2. Запустить скрипт установки:

```
bash mailion_infra_[RELEASE].run
```

3. Дождаться проверки целостности файла и его распаковки.

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

4. Согласиться на продолжение установки, нажать «**Y**».

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

5. Указать тип контейнерной виртуализации (**docker** или **podman**, см. варианты установки в разделе Запуск установки).

```
choose container_management_tool ('docker' or 'podman')*:
```

6. Во время установки на экране пользователя будет отображен список выполненяемых операций и их статус:

```
.....................................................          ........
Check if container with registry is available                  [  OK  ]
Ensure that registry configuration directory exists            [CHANGE]
Ensure that docker-registry env file exists                    [CHANGE]
Check if old registry data directory exists                    [  OK  ]
Ensure that registry data directory exists                     [CHANGE]
Ensure that container with registry is available               [CHANGE]
Ensure that docker-registry is running                         [  OK  ]
Extracting registry archive...                                 [  OK  ]
Remove dangling and outdated images                            [  OK  ]
.....................................................          ........
```

Необходимо убедиться, что элементы списка содержат статус **[OK]** или **[CHANGE]**, это свидетельствует об успешной установке компонента.

При получении статуса **[FAIL]** для любого из компонентов необходимо обратиться в техническую поддержку.

Установка хранилища образов **Docker** (**docker_registry**) будет считаться успешно завершенной в случае успешной установки всех компонент.

2.2.2.2 Установка конфигурационных файлов Ansible для развертывания ПО «Mailion»

Установка производится на рабочем месте оператора. Перед началом установки необходимо проверить следующие условия:

- вход выполнен под пользователем **root** или под пользователем **sudo** с привилегиями **yum** (**dnf7**);
- машина, на которой выполняется установка, соответствует требованиям, приведенным в разделе Системные требования;
- с выбранного сервера есть возможность доступа по SSH к другим серверам, на которых выполняется установка;

- система управления конфигурациями **Ansible** установлена, другие конфигурационные файлы **Ansible** не присутствуют в системе;
- необходимые модули установлены в системе, их версии соответствуют требованиям.

> ⚠ В подсистеме управления конфигурациями не должно быть предыдущих конфигурационных файлов самой подсистемы. В том числе конфигурационного файла, который по умолчанию устанавливается с пакетом (например, `/etc/ansible/ansible.cfg`). Такой файл требуется удалить либо перезаписать образцом из поставляемого ПО. Подробнее см. в разделе https://docs.ansible.com/ansible/latest/reference_appendices/config.html#the-configuration-file

Перед установкой важно самостоятельно установить необходимые модули python из раздела Программные требования, так как они не являются частью поставки системы.

Для установки необходимо:

1. Скопировать файл `mailion_ansible_bin_[RELEASE].run` в домашнюю директорию пользователя.
2. Запустить скрипт установки:

```
bash mailion_ansible_bin_[RELEASE].run
```

3. Согласиться на продолжение установки, нажать на клавишу «**Y**».

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

4. Во время установки на экране пользователя будет отображен список выполненяемых операций и их статус:

```
.............................                                    ........
Create playbooks symlink                                         [  OK  ]
Create group_vars directory                                      [  OK  ]
Create group_vars/all symlink                                    [  OK  ]
Create host_vars directory                                       [  OK  ]
Create certificates directory                                    [  OK  ]
Create certificates symlink                                      [  OK  ]
.............................                                    ........
```

Необходимо убедиться, что элементы списка содержат статус **[OK]** - это свидетельствует об успешной установке компонента.

При получении сообщения **[FAIL]** для любого из компонентов необходимо обратиться в техническую поддержку.

Установка конфигурационных файлов **Ansible** будет считаться успешно завершенной в случае успешной установки всех компонент.

2.2.2.3 Установка ПО «Mailion» с машины оператора

К началу данного этапа директория инсталляции `~/install_mailion/` должна выглядеть следующим образом (см. Рисунок 2):

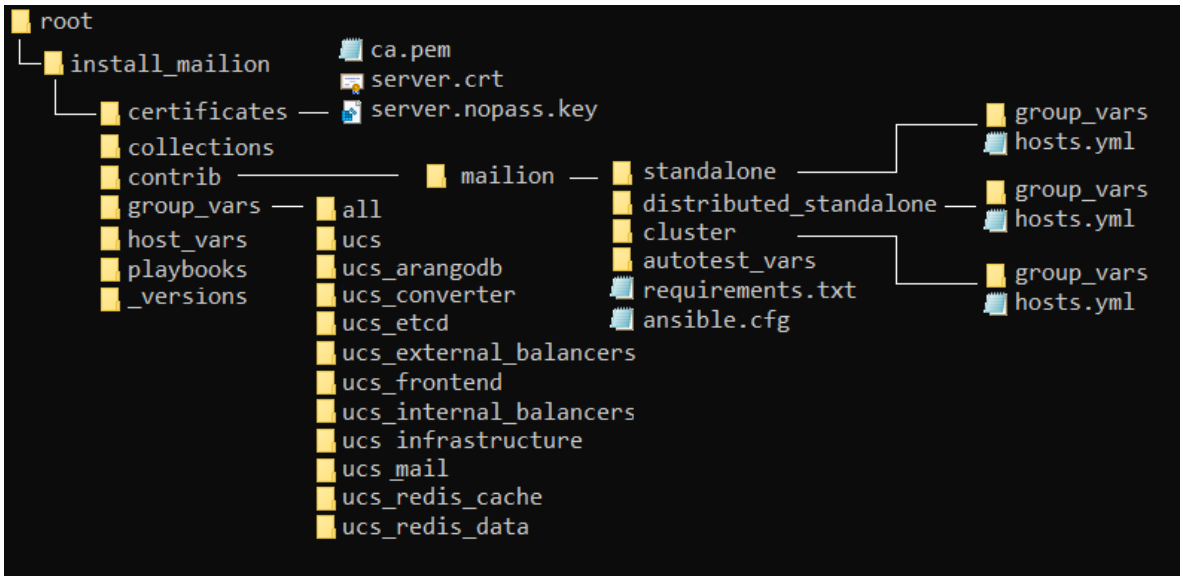


Рисунок 2 – Структура папок перед началом инсталляции

В инсталляторе представлены предзаполненные файлы конфигураций (установка описана в разделе Установка конфигурационных файлов Ansible), которые помогут в настройке необходимого функционала будущей системы. В директории `~/contrib/mailion/` находятся 3 директория, соответствующие возможным конфигурациям установки:

- `~/contrib/mailion/cluster` (кластерная конфигурация);
- `~/contrib/mailion/standalone` («Standalone»);
- `~/contrib/mailion/distributed_standalone` (распределенная конфигурация «Standalone»).

Так как целевое назначение системы – крупная отказоустойчивая инсталляция, в данном документе будет описана **кластерная конфигурация установки**.

При установке конфигурации **«Standalone»** необходимо воспроизвести аналогичные этапы установки, описанные в данном разделе. Отличие будет заключаться в названии папки, в которой находится конфигурационный файл для данной конфигурации.

Перед установкой необходимо перейти в каталог `~/install_mailion/` с помощью команды:

```
cd ~/install_mailion
```

Данный каталог будет являться корневой точкой установки

2.2.2.3.1 Копирование файла ansible.cfg

Необходимо скопировать конфигурационный файл ansible из папки `~/contrib/mailion/ansible.cfg` в корневой раздел директории установки с помощью команды:

```
cp contrib/mailion/ansible.cfg .
```

2.2.2.3.2 Конфигурирование файла hosts.yml

Для подготовки файла **inventory** (`~/hosts.yml`) необходимо произвести следующие действия:

1. Предварительно скопировать его из директория с заполненными шаблонами `~/contrib/mailion/<config>`, где `<config>` – конфигурация установки. Для конфигурации **cluster** следует воспользоваться следующей командой:

```
cp contrib/mailion/cluster/hosts.yml .
```

Для конфигурации **«Standalone»** необходимо использовать **hosts.yml** из директория **contrib/mailion/standalone**

Для распределенной конфигурации **«Standalone»** необходимо использовать **hosts.yml** из директория **contrib/mailion/distributed_standalone**

2. Открыть файл `hosts.yml` в редакторе и заменить все текстовые вхождения **«installation.example.net»** на доменное имя инсталляции (имя должно быть в нижнем регистре). Важно не менять данные имена до **«.installation.example.net»,** можно изменять только количество нод.

В файл `hosts.yml` вносятся только полностью определенные имена доменов (FQDN). Эти имена будут использоваться во время и после установки системы для обращения к внутренним сервисам. Часть логики установщика использует их для формирования доменных имен и адресов сервисов

3. Если на машине оператора планируется использовать несколько инсталляций Mailion, то необходимо заменить в файле `hosts.yml` имя группы **ucs_setup** (из ## SECTION 2) на имя текущей инсталяции (префикс **ucs_** следует оставить в

имени, например: **ucs_mailion**). Аналогичным образом нужно поменять значение переменной **tier** (см. рисунок 3).

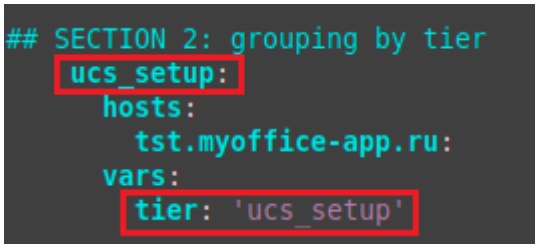


Рисунок 3 - настройка **ucs_setup**

2.2.2.3.3 Копирование папки групповых переменных

Для подготовки директория `~/group_vars` необходимо произвести следующие действия:

1. Создать в папке групповых переменных (`~/group_vars`) каталог для серверов с именем `<install_name>` группы инсталляции из файла `hosts.yml`. Имя данной папки обязательно должно совпадать с именем инсталляции из секции ## SECTION 2 (по умолчанию – **ucs_setup**, либо измененное имя).

```
cd group_vars
mkdir <install_name>
```

2. Для **кластерной** установки скопировать в папку групповых переменных (`~/group_vars`) каталог с переменными для заполнения:

```
cp -r contrib/mailion/cluster/group_vars/ucs_setup/*
group_vars/<install_name>
```

Для установки **standalone** необходимо скопировать конфигурационный файл из папки `contrib/mailion/standalone`.

```
cp -r contrib/mailion/standalone/group_vars/ucs_setup/*
group_vars/<install_name>
```

2.2.2.3.4 Конфигурирование файла main.yml

Открыть файл `main.yml` из каталога `group_vars/<install_name>` (см. предыдущий шаг) и отредактировать значение параметров, которые находятся в

комментариях. Набор параметров для минимальной настройки можно найти в разделе Параметры минимальной настройки main.yml.

При необходимости хранения паролей в зашифрованном виде следует зашифровать содержимое файла `main.yml` с помощью команды:

```
ansible-vault encrypt group_vars/ucs_setup/main.yml --ask-vault-pass
```

Затем ввести пароль для шифрования. Для удобства можно использовать файл с парольной фразой. Для этого необходимо создать текстовый файл с паролем. В таком случае команда будет следующей:

```
ansible-vault encrypt group_vars/ucs_setup/main.yml --vault-password-file=.filesecret
```

Чтобы отменить шифрование файла необходимо в команде опцию **encrypt** изменить на **decrypt**. Чтобы отредактировать зашифрованный файл, следует выполнить команду:

```
ansible-vault edit group_vars/ucs_setup/main.yml --vault-password-file=.filesecret* (или --ask-vault-pass)
```

2.2.2.3.5 Конфигурирование файла ministerium.yml

Открыть файл `ministerium.yml` из каталога размещения и отредактировать значение параметров, которые находятся в комментариях. Примеры заполнения параметров можно найти в разделе Настройка основных параметров установки. Подробная инструкция присутствует в главе 4 документа «Mailion. Руководство по администрированию».

2.2.3 Установка и обновление пакетов Python

Требуется наличие программного обеспечения, описанное в раделе Программные требования, для чего необходимо на машине оператора установить или обновить следующие пакеты:

– Установка или обновление каталога пакетов python:

```
pip3 -m install --upgrade pip==20.3.4
```

– Установка модуля ansible-core (версия может отличаться):

```
pip3 install --no-cache-dir hvac ansible-core==2.11.9
```

– Установка необходимых зависимостей:

```
pip3 install --no-cache-dir -r ~/install_mailion/contrib/mailion/requirements.txt
```

2.2.4 Размещение ssl-сертификатов для шифрования

Имена сертификатов могут быть произвольными, но они потребуются для дальнейшего заполнения параметров групповых переменных, поэтому важно их запомнить. В файле групповых переменных `extra_vars.yml`, создание которого было описано в разделе Копирование папки групповых переменных, заполнены имена сертификатов по умолчанию. Если назвать файлы сертификатов соответствующим образом, то менять имена в переменных не нужно.

Состав необходимых сертификатов:

1. Сертификат внешнего домена `server.crt`.
2. Ключ внешнего домена `server.nopass.key`.
3. Цепочка сертификатов промежуточных центров сертификации (CA) внешнего домена `ca.pem`.

Формат файла: в конце файла не должно быть пустой строки.

```
    cat certificates/server.crt

-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

Необходимо скопировать файлы сертификатов (`ca.pem`, `server.crt`, `server.nopass.key`) в папку:

```
    ~/install_mailion/certificates/
```

Имена ключей групповых переменных находятся в переменных **mailion_external_cert_filename**, **mailion_external_key_filename**, **mailion_external_ca_filename**:

```
    mailion_external_cert_filename: "server.crt"
    mailion_external_key_filename: "server.nopass.key"
    mailion_external_ca_filename: "ca.pem"
```

При установке ПО «Mailion» есть возможность использования сертификатов центра Let's Encrypt на усмотрение администратора установки.
Разработчик ПО «Mailion» не несет ответственности за получение, обновление и управление сертификатами Let's Encrypt

В случае использования самоподписанного сертификата в конфигурационный файл необходимо добавить флаг: **mailion_use_self_signed_external_certificate: true**

2.2.5 Настройка основных параметров установки

2.2.5.1 Минимальные параметры установки

Минимальные параметры, обязательные для заполнения:

- ansible_user;
- codec_secret_key;
- dispersed_object_store_management_token;
- grafana_admin_password;
- house_ldapauth_password_salt;
- hydra_get_service_list_token;
- jwt_key;
- keepalived_vrrp_instances;
- mailion_cluster, mailion_domain_module, mailion_external_domain, mailion_installation_admin_password, mailion_integrations, mailion_internal_web_auth, mailion_max_users, mailion_service_accounts, mailion_supported_domains, mailion_tenants;
- mongodb_root_password, mongodb_secured_key, mongodb_management_users;
- nats_authorization_password, nats_cluster_authorization_password;
- redis_cluster_replicas, redis_dafnis_password, redis_dowal_password, redis_ektor_password, redis_erakles_password, redis_euripides_password, redis_hog_password, redis_homeros_password, redis_leda_password, redis_minos_password, redis_rspamd_password, redis_sdd_password, redis_viper_password;
- rspamd_kse_endpoints, rspamd_dkim_hosts, rspamd_web_password;
- servus;
- sophokles_access_token;
- theseus_cipher_key;
- tls_certs_remote_token_key;
- unbound_forward_addresses.

Структура и способы заполнения указанных параметров приведены в разделах ниже.

2.2.5.1.1 Настройка параметров установки ansible_user

Настройка параметров приведена в таблице 19.

Таблица 19 – Настройка параметров ansible_user

Параметр	Тип данных	Описание
ansible_user:	str	Имя пользователя, под которым установщику будут доступны серверы инсталляции по **ssh**

Пример корректно настроенного параметра:

```
ansible_user: "root"
```

2.2.5.1.2 Настройка параметров codec_secret_key

Настройка параметров приведена в таблице 20.

Таблица 20 – Настройка параметров codec_secret_key

Параметр	Тип	Описание
codec_secret_key:		Словарь параметров секретов для формирования шифрованной ссылки
rcr:	str	Используется для формирования ссылки на проксирование данных внутри системы
secret_link:	str	Используется для формирования ссылки на проксируемые ресурсы
values_codec	str	Значение

Пример корректно настроенного параметра:

```
codec_secret_key:
  rcr: "O1Wk7ha80M1qfvq8UtuZg918AZyh+q65s68dKvXwVTQ="
  secret_link: "69rUgWgrLbV50CiAEK78AJIrLoWBGHGwYCX25phh3yg="
  values_codec: "ggxhfxrjshb034fosedfwd3d"
```

2.2.5.1.3 Настройка параметров dispersed_object_store

Настройка параметров приведена в таблице 21.

Таблица 21 – Настройка параметров dispersed_object_store

Параметр	Тип	Описание
dispersed_object_store_management_token: ""	str	Токен доступа для управления через API сервиса

Пример корректно настроенного параметра:

```
dispersed_object_store_management_token: "Aig2utoavi6iageiltas"
```

2.2.5.1.4 Настройка параметра Docker

Настройка параметров приведена в таблице 22.

Таблица 22 – Настройка параметров Docker

Параметр	Тип	Описание
docker_daemon_parameters:		Параметры демона **docker**
bip:	str	Подсеть и маска для **docker**
dns:	list	Список строк с адресами DNS-серверов
mtu:	int	Значение **MTU** для сетевого интерфейса **docker**

Пример корректно настроенного параметра:

```
docker_daemon_parameters:
  bip: "172.17.0.1/16"
  dns:
      - "8.8.8.8"
      - "1.1.1.1"
  mtu: 1412
```

2.2.5.1.5 Настройка параметров grafana

Настройка параметров приведена в таблице 23.

Таблица 23 – Настройка параметров grafana

Параметр	Тип	Описание
grafana_admin_password:	str	Пароль администратора grafana

Пример корректно настроенного параметра:

```
grafana_admin_password: "Ooj0Inahgh2Ixailoxie"
```

2.2.5.1.6 Настройка house

Настройка параметров приведена в таблице 24.

Таблица 24 – Настройка параметров house

Параметр	Тип	Описание
house_ldapauth_password_salt:	str	Соль для хеширования паролей при LDAP-авторизации

Пример корректно настроенного параметра:

```
house_ldapauth_password_salt: ")6_]*|,)(bJ;PN"
```

2.2.5.1.7 Настройка hydra

Настройка параметров приведена в таблице 25.

Таблица 25 – Настройка параметров hydra

Параметр	Тип	Описание
hydra_get_service_list_token:	str	Токен для обращения в API сервиса

Пример корректно настроенного параметра:

```
hydra_get_service_list_token: "maiquauzuwooQu9ooR7x"
```

2.2.5.1.8 Настройка параметров jwt_key

Настройка параметров приведена в таблице 26.

Таблица 26 – Настройка параметров jwt_key

Параметр	Тип	Описание
jwt_key:		Параметры **jwt_key**

Параметр	Тип	Описание
priv:	str	Закрытый ключ
pub:	str	Публичный ключ

Пример корректно настроенного параметра:

```
jwt_key:
  priv: |
    -----BEGIN RSA PRIVATE KEY-----
    MIIEowIBAAKCAQEA063xN82YOtJBq8sfd79bJ+4W9QEdOueQljPziN4JdYntS381
    AqxOA4Ud886S4LdwCN2KSpuh7QSHkzjzH9AlDrHCYShOfPAeHLMCBDszazr2IOc0
    Jaw3bHRfrM9Ilb+X4qdDE88Mfk+B/8Sa/xG2HJVy0Jjb4XoipwzEB900a+6zpnLT
    ............
    q/kNt7YtrTBmrgpSzFMr0VD+x0Ftb9zhiFVLyVscVKEl67+TNlWahgzh14YF8xP8
    gb89coH114YUNfxN8lKURdY9QFNuZLF+x8xfL4CWwydSbtL7dFFK0HVowMt4tnoJ
    okthJ5JZNw+XZAXHS3NyuvbYmP+iqRuL2YAr2wIDAQABAoIBAGyNHs5HGHHRsOuw
    Uq3/k9aD8NKVjJnJ7/kQEnLlBjcHcpazMHQJnvpfRaqfBre0G1ok9sPH/rvTgK1U
    clKH2eSXgRhKgLf3Dtf6m2bULj0HN0FIydngh0F1EqK10vnvqfkN
    -----END RSA PRIVATE KEY-----
  pub: |
    -----BEGIN PUBLIC KEY-----
    MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA063xN82YOtJBq8sfd79b
    J+4W9QEdOueQljPziN4JdYntS381AqxOA4Ud886S4LdwCN2KSpuh7QSHkzjzH9Al
    DrHCYShOfPAeHLMCBDszazr2IOc0Jaw3bHRfrM9Ilb+X4qdDE88Mfk+B/8Sa/xG2
    HJVy0Jjb4XoipwzEB900a+6zpnLTq/kNt7YtrTBmrgpSzFMr0VD+x0Ftb9zhiFVL
    yVscVKEl67+TNlWahgzh14YF8xP8gb89coH114YUNfxN8lKURdY9QFNuZLF+x8xf
    L4CWwydSbtL7dFFK0HVowMt4tnoJokthJ5JZNw+XZAXHS3NyuvbYmP+iqRuL2YAr
    2wIDAQAB
    -----END PUBLIC KEY-----
```

2.2.5.1.9 Настройка параметров keepalived

Настройка параметров приведена в таблице 27.

Таблица 27 – Настройка параметров keepalived

Параметр	Тип	Описание
keepalived_vrrp_instances		Параметры **keepalived**
ucs_frontend:		Параметры **ucs_frontend**
password:	str	Пароль
virtual_ip	str	Виртуальный IP для группы хостов **ucs_frontend**
ucs_mail:		Параметры **ucs_mail**
password:	str	Пароль
virtual_ip	str	Виртуальный IP для группы хостов **ucs_mail**

Пример корректно настроенного параметра:

```
keepalived_vrrp_instances:
  ucs_frontend:
    password: "UgohSh8i"
    virtual_ip: "192.168.10.10"
    ucs_mail:
      password: "keeB5ooH"
      virtual_ip: "192.168.10.10"
```

2.2.5.1.10 Настройка параметров mailion

Настройка параметров приведена в таблице 28.

Таблица 28 – Настройка параметров mailion

Параметр	Тип	Описание
mailion_cluster:	bool	Флаг кластерной или «Standalone» инсталляции
mailion_domain_module	special	Переменная для генерации эндпоинтов инсталляции (убедиться, что в значении используются разделители «-», а не «.»)
mailion_external_domain:	str	Внешний домен инсталляции
mailion_installation_admin_password	Str	Пароль для администратора всей инсталляции (!)
mailion_integrations	dict	Словарь, содержащий настройки интеграций
mailion_integrations.microsoft	bool	Включение и отключение интеграции с решениями Microsoft
mailion_integrations.freeipa	bool	Включение и отключение интеграции с FreeIpa
mailion_integrations.squadus	bool	Включение и отключение интеграции с ПО Squadus
mailion_integrations.co_auth	bool	Включение и отключение интеграции с ПО «МойОфис «Частное Облако»
mailion_integrations.psn	bool	Включение и отключение интеграции с PSN

Параметр	Тип	Описание
mailion_integrations.google_oauth	bool	Включение и отключение интеграции с Google OAuth
mailion_internal_web_auth	dict	Словарь, содержащий настройки внутренней веб-аутентификации
mailion_internal_web_auth.enabled	bool	Включение и отключение аутентификации для доступа к веб-интерфейсам инфраструктурных сервисов (мониторинг, grafana и т.д.)
mailion_internal_web_auth.password	str	Пароль для аутентификации для доступа к веб-интерфейсам инфраструктурных сервисов
mailion_max_users:	int	Максимальное количество пользователей в инсталляции
mailion_service_accounts	dict	Словарь, содержащий пароли сервисов (values) и имена сервисов (keys)
mailion_supported_domains	list	Список доменов, которые инсталляция будет поддерживать

Пример корректно настроенного параметра:

```
mailion_cluster: true
mailion_domain_module: "{service}.{domain}"
mailion_external_domain: "installation.example.net"
mailion_installation_admin_password: "oor3Iekichocaiphahr5"
mailion_integrations:
  aldpro: false
  co_auth: false
  freeipa: false
  google_oauth: false
  microsoft: false
  psn: false
  samba_dc: false
  squadus: false
mailion_internal_web_auth:
  enabled: true
  password: "rfkg7shtasjfha6vnd"
mailion_max_users: 100
mailion_service_accounts:
  ararat: "Jo8be1pheicahmieV2oa"
  ares: "72gyV456uh9ARiYs8jBx"
  ariadne: "Um6heiNie2doeshee2sa"
```

```
  atlas: "Gaezohg1Ad3naf5ahpef"
  clotho: "Hyrq5iedwemdLNrV47KT"
  cox: "Ii0eeceen5ti1Oe6xaeb"
  dflink_plugin: "Gaezohg1Ad312345hpef"
  elysion: "le0eelePhooghougoopo"
  erakles: "Ui6ohDahLeitozughugh"
  hog: "shee8einoh4AivigePei"
  homeros: "ooph8Efu1eesu2quah1u"
  house: "ahb9Hai3Quaid4aed7an"
  imap: "feo6aita3El6aiMaeboh"
  kongur: "aa6eizooguPhene9uifu"
  kronos: "iphuTh0eiY2ook4aeph5"
  leda: "72YjiCQrnwUwCR32sVrL"
  lmtp: "aicae3yo7Aukaejeel2e"
  marker: "eer1edaeceeJu6naiPom"
  minos: "eshegh3iaR0fie0G"
  othrys: "eeth8Avohv8OpheeHieg"
  paranoid: "Yoa4eNgahm0aeChu8uWe"
  perseus: "Oogh9ahroow2eicaeng7"
  razor: "Ohquietikenu2Aeloh6E"
  theseus: "eileixietai0cahQu3ma"
  viper: "Feir8uewie4Ieshu4thi"
  woof: "at6Ohdapohaitahtho2j"
  zeus: "fa4Ohxaithee0yaeleit"
mailion_supported_domains: []
```

2.2.5.1.11 Настройка параметров mongodb

Настройка параметров приведена в таблице 29.

Таблица 29 – Настройка параметров MongoDB

Параметр	Тип	Описание
mongodb_root_password:	str	Пароль пользователя root для СУБД
mongodb_secured_key:	str	Ключ для доступа к СУБД
mongodb_management_users:		Словарь. Каждый ключ словаря – пользователь
marker:		Ключ, имя пользователя
database:	str	База для аутентификации (опционально)
password:	str	Пароль для аутентификации
roles:		Список ролей (опционально)
- role:	str	Роль пользователя

Параметр	Тип	Описание
db	str	Имя базы данных, для которой пользователю присваивается роль

Пример корректно настроенного параметра:

```
## MongoDB secrets
## Generate the password with `pwgen 16 1`
mongodb_root_password: "ohre4Rohngahshah"
## Generate the password with `pwgen 16 1`
mongodb_secured_key: "uGhie5ieweixae9C"
mongodb_management_users:
  achill:
    password: "cohh0Av2mai2aJae"
  beef:
    password: "idohjie2Ikeice0I"
  clotho:
    password: "wahcoovei0bahRu4"
  daidal:
    password: "cheYichoongoh4gi"
  erakles:
    password: "Uxeu4iephluix1ah"
  hog:
    password: "rae0faeng1Seupee"
  homeros:
    password: "xoopunaihuopae4J"
  marker:
    password: "ohvufoosaeTeeCo3"
  mongodb_exporter:
    password: "woo2Yual2saeboh1"
  kongur:
    password: "ahmeayooH1yahlohreem"
  kronos:
    password: "peiNguxud8ooThaiCahL"
  odusseus:
    password: "oY9ja7ietheec6sahthe"
  perseus:
    password: "xuoboop5Geneemei"
  sophokles:
    password: "baexuli5oow8ohTh"
```

```
  talaos:
    password: "Ahroozait4pesupohpho"
  themis:
    password: "feef8euch8gaiwieRoig"
  theseus:
    password: "ua8mu0uoj6uvieDu2gei
  "thoth:
    password: "BooRah6oal9Naehai2ph"
```

2.2.5.1.12 Настройка параметров nats

Настройка параметров приведена в таблице 30.

Таблица 30 – Настройка параметров NATS

Параметр	Тип	Описание
nats_authorization_password:	str	Пароль для авторизации в **NATS**
nats_cluster_authorization_password:	str	Пароль для **NATS cluster auth**

Пример корректно настроенных параметров:

```
nats_authorization_password: "Fiohoogh7Raobi4yeiSi"
nats_cluster_authorization_password: "aolIey7luRohlahf9eVe"
```

2.2.5.1.13 Настройка дополнительных параметров postfix

Настройка дополнительных параметров приведена в таблице 31.

Таблица 31 – Настройка дополнительных параметров postfix

Параметр	Тип	Описание
postfix_additional_mynetworks:	list	Список дополнительных сетей, из которых разрешена отправка через MTA инсталляции

Пример корректно настроенного параметра:

```
## POSTFIX configuration
### (optional) list of networks allowed to use this SMTP relay
# postfix_additional_mynetworks:
#  - "192.168.113.0/24"
```

2.2.5.1.14 Настройка параметров redis

Настройка параметров приведена в таблице 32.

Таблица 32 – Настройка параметров redis

Параметр	Тип	Описание
redis_cluster_replicas	int	redis_cluster_replicas аналогичен параметру - replicas redis-cli. см. официальную документацию https://redis.io/docs/manual/replication/. Для HA redis с slave, требуется минимум 6 машин с redis_cluster_replicas 1, и 9 машин с redis_cluster_replicas 2.
redis_dafnis_password	str	Пароль для **redis_dafnis**
redis_dowal_password	str	Пароль для **redis_dowal**
redis_ektor_password	str	Пароль для **redis_ektor**
redis_erakles_password	str	Пароль для **redis_erakles**
redis_euripides_password	str	Пароль для **redis_euripides**
redis_hog_password	str	Пароль для **redis_hog**
redis_homeros_password	str	Пароль для **redis_homeros**
redis_leda_password	str	Пароль для **redis_leda**
redis_minos_password	str	Пароль для **redis_minos**
redis_rspamd_password	str	Пароль для **redis_rspamd**
redis_sdd_password	str	Пароль для **redis_sdd**
redis_viper_password	str	Пароль для **redis_viper**

Пример корректно настроенных параметров:

```
redis_dafnis_password: "eexaiSheQuoivu1oo4ak"
redis_dowal_password: "oasu7nieNg0aeshaiphi"
redis_ektor_password: "eisach9eet8thaug9Ieg"
redis_erakles_password: "zae9iaL3ooth3ahphugh"
redis_euripides_password: "xi6Ohy8io5ku7veQuau7"
redis_hog_password: "dighaeX0hoov6aeJee3u"
redis_homeros_password: "chae7quah7Li2zohbe8o"
redis_leda_password: "Aiy6iiyeiZo2caaleofe"
redis_minos_password: "quie2jiG2CeucooShahG"
redis_rspamd_password: "Iughoo2iuS2Xew1die4p"
redis_sdd_password: "fohphow6eat1aekod5Oh"
redis_viper_password: "Tee9han6ienaYoSievoo"
```

2.2.5.1.15 Настройка параметров resolv

Настройка параметров приведена в таблице 33.

Таблица 33 – Настройка параметров resolv

Параметр	Тип	Описание
resolv_nameservers:	list	Список строк с адресами DNS-серверов для настройки файла **resolv.conf**

Пример корректно настроенного параметра:

```
resolv_nameservers:
  - "192.168.1.1"
  - "192.168.1.2"
  - "192.168.1.3"
```

2.2.5.1.16 Настройка параметров rspamd

Настройка параметров приведена в таблице 34.

Таблица 34 – Настройка параметров rspamd

Параметр	Тип	Описание
rspamd_dkim_hosts:		Параметры антиспама
		Параметры **dkim_hosts**
<your_external_domain>		Имя внешнего домена, который необходимо подписывать DKIM-ключом
dkim_key:	str	DKIM-ключ
rspamd_web_password:	str	Пароль от веб-интерфейса

Пример корректно настроенного параметра:

```
rspamd_dkim_hosts:
    installation.example.net:
      dkim_key: |
        -----BEGIN PRIVATE KEY-----
        MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQC3euVQm/Djy1z1
        JhbTC5Cs99HmrgN6DldM5xivTyhopgkGlHXIoWaKfvt3wKm/Pzah2/BkcTXtDa3w
        E70bmjVXFX2xkXG5DAuY9ChnX6+xWYCeBUeRsMSnWdyoNBwFK9rjE2vZ+u3OzLhz
        wP6PuIyigV7A3D9Mtok0XA3iH/7G+99ARjxhj8hCkYEqEsR688uU1JNeztTfkte+
        mz6n7w8AO2jdpdG8wRqjvj4B4H0MaaP7R4y/UopZ+UP0RAbm7KryOjgC15uLou9Y
        Yg9ym0VkcaIOvc0xQT7Zk13yf8vIuVS/6yhO3FcKYB4mx0Szz1RpU2ueyvD2COSj
        C+2uZsPFAgMBAAECggEBAK6+xEH2kwFRAPKWWSydGigySl4KI1OO7wRWIMNuf4zT
        fUsf/+GaHoAPGk7eVozHlq+nOhdfXz2rRpqdIgF06BJNbI2+ePIFj9IXz5dMoZcm
        KAHYA2a1VUYRpr8oCfu+3dRg/dn4S58miRHtoESfPonS7rx9x2e3fYs5lRtk35EA
        Wp5Vy+2U36cKIJLVtAOvzRbGl9SLjPAvuc/WKGda2lA7HBlhep/Yrm0RUoH//5Px
        fJwLVSy34B31Fx1wZk80aVquXCv644GbR89RIQttziHg9q4g/wyZ5/+ZG/967kim
        tKDS8PWhAK5pjUHS9cED/hjs+ITlNCI4qKf2zj2XSqECgYEA3X9zmzAw9JLnelZN
        3oVM/boqtwfPgnO6Y98inDMsecAICWLCAsEsWYY90IB3FQCXJXVrGTxKnHa3S0fR
        MTX5xx3Rta5SWf88jUQCmZEuxHBeIEN9JKebKC97rKIlIJmYJ8PVZ8c6LAvMgmYc
        sd+GyjJAmV+N7j5Eo8tXmZCCuK0CgYEA1A9t7P6GjXQQFrIk81+x+0JHmIN+DPKs
        eyR6avDfd32HIq2dPCMmjCAl7EFbfOPVNx9rZvLrEWtTkgU8DYBPlZ955EJORi9l
        eqYeOKwhWLUMgwHyWlEJZPeY3o31TF1NwNG16Qy98h4zr2SUaTuCdccoNWAc0GuI
```

```
        rAlGjn7AonkCgYEAuMpgFJS8Aw+cdwARrxffB7+Na23kvZz3X+ME6PP4owqGqe3u
        loW7DmVkpNLIhokbkHDJjSAzzx1sBi5AZKH3ZRuHnd91bQf36JNY5+2r6s8keB5W
        BYKfe4NB1uDfwLbjrik/nXklGyIs2I2AWxV1SrNqGYsSyjTA5zX6O2/I33ECgYBS
        eO23jgWmXc0kBoR4Ym9F2LEfj4QmZPrPqZAypxtBzYAQ7JSKHuGO/bHCAGkkWTdD
        COUsVK03SRZnY8HHPm+1MSCmtWLbyPMekByQzeDqLv9+s/MdTQbqTaEWbP9Jg8AJ
        jYXB7UKyNyzCucs+YfaK97mbiJWsOSYeQ8t8/67LgQKBgQCk4q/D5Cq5Fqalbk/0
        jyEQAmHgrhWEJO2bECGjGIJ13/Hj3bbQ3znfPUDf9MLDtrveGu4YdspL3S4yahLO
        EXxXPgwHCDLqamx5vj4QKFPFQEHXv68RK6RKhw7m2IeyI/7nsHPvjZhNZI4ulSTN
        CLCjuiw8tvIafY26wKDylpvnRQ==
        -----END PRIVATE KEY-----

  rspamd_web_password: "iePixieTaf4IriequieX"
```

2.2.5.1.17 Настройка параметров servus

Настройка параметров приведена в таблице 35.

Таблица 35 – Настройка параметров servus

Параметр	Тип	Описание
servus:	str	Параметры **servus**

Пример корректно настроенного параметра:

```
servus: "Iefae4yoh4rohceepoli"
```

2.2.5.1.18 Настройка параметров sophokles

Настройка параметров приведена в таблице 36.

Таблица 36 – Настройка параметров sophokles

Параметр	Тип	Описание
sophokles_access_token:	str	Токен для сервиса авторизации **minos** и **sophokles**

Пример корректно настроенного параметра:

```
sophokles_access_token: "IeWoh9eateihuvoxekah":
```

2.2.5.1.19 Настройка параметров theseus

Настройка параметров приведена в таблице 37.

Таблица 37 – Настройка параметров theseus

Параметр	Тип	Описание
theseus_cipher_key:	str	Ключ шифрования **theseus**

Пример корректно настроенного параметра:

```
theseus_cipher_key: "RWVmb21pZXhvbmFpYzZvaHlhaTR6aURhd2VpZzhlZW4="
```

2.2.5.1.20 Настройка параметров unbound

Настройка параметров приведена в таблице 38.

Таблица 38 – Настройка параметров unbound

Параметр	Тип	Описание
unbound_access_control:	dict	Параметры доступа к управлению **unbound**
network1	str	Подсеть, из которой разрешен доступ к кэширующему **DNS**
unbound_enable_autowildcard:	bool	Флаг использования автоматического формирования DNS-записей внутренних адресов на базе серверов в файле **inventory** и их значений переменной **ansible_default_ipv4**
unbound_forward_addresses:	list	Список строк внешних DNS-сервисов, на которые будут перенаправляться запросы **unbound** серверов

Пример корректно настроенного параметра:

```
unbound_enable_autowildcard: false
unbound_access_control:
  network1: "192.168.1.0/24"
unbound_forward_addresses:
  - "8.8.8.8"
  - "1.1.1.1"
```

2.2.5.1.21 Настройка параметров CA

Настройка параметров приведена в таблице 39.

Таблица 39 – Настройка параметров CA

Параметр	Тип	Описание
tls_certs_remote_token_key:	str	Ключ для доступа к API внутреннего **Certificate Authority**

Пример корректно настроенного параметра:

```
tls_certs_remote_token_key: "afba15d0def55ca6e57efb481f8232a5"
```

2.2.5.1.22 Настройка параметров viper

Настройка параметров приведена в таблице 40.

Таблица 40 – Настройка параметров viper

Параметр	Тип	Описание
viper_calendar_settings_sender_white_list:	list	Список отправителей, которые могут присылать календарные письма за участника события (например, сервисные ящики noreply).

Параметр	Тип	Описание
regexp:	str	Выбор отправителей по регулярному выражению
sender_in_reply_to	bool	Добавить отправителя в **reply_to**
Переменные для ограничения индексации писем		
viper_rate_limit_mail_indexer_enable	bool	Если **true**, то механизм ограничения индексации включен
viper_rate_limit_mail_indexer_events_per_sec	int	Ограничение на количество запросов в секунду (RPS)
viper_rate_limit_mail_indexer_burst	int	Размер разрешенного единовременного всплеска событий. Данная переменная нужна для обработки пиковой нагрузки. Значение может быть больше ограничения на количество запросов в секунду (RPS). Практическое применение этого параметра заключается в ограничении количества одновременно обрабатываемых событий
viper_rate_limit_mail_indexer_max_delay_sec	int	Максимальное время, на которое может блокироваться обработка события при реиндексации. Если это время превышено, попытка индексации будет происходить позже, когда нагрузка станет меньше. Для отключения проверки максимальной задержки следует установить значение 0
Переменные для ограничения индексации вложений писем		
viper_rate_limit_attachment_indexer_enable	bool	Если **true**, то механизм ограничения индексации включен
viper_rate_limit_attachment_indexer_events_per_sec	int	Ограничение на количество запросов в секунду (RPS)
viper_rate_limit_attachment_indexer_burst	int	Размер разрешенного единовременного всплеска событий. Данная переменная нужна для обработки пиковой нагрузки. Значение может быть больше ограничения на количество запросов в секунду (RPS). Практическое применение этого параметра заключается в ограничении количества одновременно обрабатываемых событий
viper_rate_limit_attachment_indexer_max_delay_sec	int	Максимальное время, на которое может блокироваться обработка события при реиндексации. Если это время превышено, попытка индексации будет происходить позже, когда нагрузка станет меньше. Для отключения проверки максимальной задержки следует установить значение 0

Пример корректно настроенного параметра:

```
viper_calendar_settings_sender_white_list:
- regexp: "[^@]+@calendar.example.ru$"
```

```
  sender_in_reply_to: true
- regexp: "^calendar@calendar.example.ru$"
  sender_in_reply_to: false

viper_rate_limit_mail_indexer_enable: false
viper_rate_limit_mail_indexer_events_per_sec: 100
viper_rate_limit_mail_indexer_burst: 50
viper_rate_limit_mail_indexer_max_delay_sec: 300
viper_rate_limit_attachment_indexer_enable: false
viper_rate_limit_attachment_indexer_events_per_sec: 100
viper_rate_limit_attachment_indexer_burst: 50
viper_rate_limit_attachment_indexer_max_delay_sec: 300
```

2.2.5.1.23 Настройка параметров ntp

Настройка параметров приведена в таблице 41.

Таблица 41 – Настройка параметров ntp

Параметр	Тип	Описание
ntp_servers:	list	Список **ntp** серверов
ntp_listen_on_default_v4	bool	Определяет какие сетевые адреса открывает **ntpd**
ntp_listen_on_default_v6	bool	Определяет какие сетевые адреса открывает **ntpd**
ntp_clients_inventory_access	bool	Ограничивает все хосты из inventory по флагу **nomodify notrap**
ntp_clients:	list	Список хостов/адресов для ограничения
name:	str	Имя хоста или адреса
access:	str	Флаг доступа
ntp_driftfile_directory	str	Путь к файлу данных **ntp**
ntp_custom_config	dict	Выборочная конфигурация **ntp**

2.2.5.1.24 Настройка параметров chrony

Настройка параметров приведена в таблице 42.

Таблица 42 – Настройка параметров chrony

Параметр	Тип	Описание
ntp_servers:	list	Список **ntp** серверов

2.2.6 Настройка межсетевого экранирования

⚠ Во время установки на все серверы **автоматически** будет установлена служба управления межсетевым экраном **iptables** и настроены правила, ограничивающие

входящий доступ по всем портам, кроме тех, которые занимают запущенные контейнеры на соответствующих серверах, и разрешены заданными правилами экрана

Установленные правила межсетевого экрана приведены в таблице 43.

Таблица 43 – Установленные правила межсетевого экрана

Серверы	Таблица	Состояние	Порт	Протокол	Интерфейс	Разрешение
Серверы группы ucs	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
	INPUT				docker0 или cni-podman0*	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
Серверы группы ucs_etcd	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
	INPUT				docker0 или cni-podman0*	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT	NEW	53	UDP		ACCEPT
Серверы группы ucs_infrastructure	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
					docker0 или cni-podman0*	ACCEPT

Серверы	Таблица	Состояние	Порт	Протокол	Интерфейс	Разрешение
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT		53	TCP		ACCEPT
	INPUT		53	UDP		ACCEPT
Серверы группы ucs_frontend	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
					docker0 или cni-podman0*	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT			VRRP		ACCEPT
Серверы группы ucs_mail	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
					docker0 или cni-podman0*	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT			VRRP		ACCEPT

***** если используется контейнерная виртуализация **podman**.

2.2.6.1 Настройки правил внешнего межсетевого экрана

Во время установки происходит настройка межсетевого экрана внутри контура инсталляции. Тем не менее, очень важно обеспечить дополнительную защиту системы с внешней стороны по отношению к контуру инсталляции.

Во внешний контур должны быть доступны только следующие порты:

– порты на виртуальные IP серверов с ролью **ucs_frontend**:

- 80/tcp;

- 143/tcp;
- 443/tcp;
- 993/tcp;
- 3142/tcp;
- 6787/tcp;
- 389/tcp;
- 389/udp;
- 636/tcp;
- 636/udp;

– порты на виртуальные IP серверов с ролью **ucs_mail**:

- 465/tcp;
- 587/tcp;

– порты на реальные IP серверов **ucs_mail**:

- 25/tcp.

2.3 Запуск установки

Для установки на контейнеры **docker** необходимо запустить следующую команду:

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

Для установки на контейнеры **podman** необходимо запустить следующую команду:

```
ansible-playbook playbooks/main.yml --skip-tags=cadvisor --extra-vars
'{"container_management_tool": "podman"}'  --extra-vars
'{"podman_container_no_hosts": "true"}' -e '{"confd_max_memory": "100M"}' -e
'{"pregen_max_memory": "100M"}' -e '{"cvm_max_memory": "2000M"}' --diff
```

Если использовалось шифрование паролей, описанное в разделе Установка Mailion с машины оператора, то к команде установки необходимо добавить ключи **--vault-password-file=.filesecret** или **--ask-vault-pass**.

После этого запускаются роли, описанные в разделе Описание ролей Ansible.

2.4 Проверка корректности установки

Для проверки корректности установки необходимо запустить установленный ПО «Mailion»:

1. Открыть в поддерживаемом веб-браузере страницу по адресу, который указывался в **mailion_external_domain**.

2. Использовать для входа учетные данные созданных пользователей.
3. Если вход был выполнен под пользователем, то необходимо отправить письмо самому себе внутри ПО «Mailion». Если вход выполнен под администратором, то сначала нужно создать пользователя (при условии, что он не был создан плейбуком **ministerium**).
4. Если письмо успешно отправилось и пришло — установка настроена корректно.

2.4.1 Добавление дополнительных доменов для обслуживания инсталляцией

В ПО «Mailion» реализована поддержка дополнительных доменов. Чтобы добавить дополнительный домен необходимо включить его в список **mailion_supported_domain**:

```
mailion_supported_domains:
  - "example.com"
```

Затем необходимо добавить dkim-ключ к домену в словарь **rspamd_dkim_hosts**:

```
rspamd_dkim_hosts:
  domain2.example.net:
    dkim_key: |
......
```

После этого с машины оператора из папки с инсталлятором необходимо выполнить команду:

```
ansible-playbook playbooks/ucs/main.yml --tags postfix,rspamd --limit ucs_mail
--diff
```

Эта команда запустит роль **postfix** с функцией **mx** и добавит указанные домены для **MTA**, а также добавит dkim-ключи для доменов в **rspamd**.

2.5 Установка в составе других продуктов ПО «МойОфис»

Установка в составе других продуктов ПО «МойОфис» не выполняется.

2.6 Установка Надстройки для Microsoft Outlook

Подробное описание установки Надстройки для Microsoft Outlook приведено в документе «Mailion. Руководство по установке (Надстройка для Microsoft Outlook)».

3 ОБНОВЛЕНИЕ С ПРЕДЫДУЩИХ ВЕРСИЙ

Обновления возможны с версий 1.7 и 1.8 . Список компонентов приведен в разделе Состав дистрибутива.

Перед обновлением необходимо в файлах `group_vars/ucs_setup/*` проверять наличие новых переменных (где `ucs_setup` - название инсталяции). Новые переменные находятся в файлах `contrib/mailion/cluster/group_vars/ucs_setup/*` (для «Standalone» инсталляции в `contrib/mailion/standalone/group_vars/ucs_setup/*`).

Например, при обновлении с версии 1.7 необходимо добавить следующие новые переменные:

```
mailion_service_accounts:
  broteas: "quaSh0thae9iegh9chai"
  pasifae: "eeLaiB5iegheibaeb3Qu"
mongodb_management_users:
  dorofej:
  password: "quaiheguqu7Nee2u
  dafnis:
  password: "exah4laekiefu7pa"
```

Обновление ПО «Mailion» осуществляется аналогично установке новой версии (см. раздел Первичная установка) за исключением того, что обновление с версии 1.7 должно производиться с параметром **permission_migration=true**, который используется для смены пользователей и прав доступа на файлы сервисов при переходе на `rootful` режим. При обновлении Mailion его нужно применить только один раз. При последующих установках отдельных сервисов данный параметр использовать не нужно.

Запуск обновления с версии 1.7 с миграцией данных:

```
ansible-playbook playbooks/main.yml -e "permission_migration=true" -diff
```

Обновление без миграции данных (см. раздел Запуск установки):

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

⚠ Перед обновлением необходимо в файле **contrib/mailion/cluster/group_vars/ucs_Имя_Инсталяции/version.yml** изменить значение переменной **mailion_release_name** на значение, аналогичное номеру актуального релиза релиза

4 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ И РЕКОМЕНДАЦИИ ПО УСТАНОВКЕ

4.1 Настройка Redis TLS

Последовательность действий:

1. Изначально необходимо установить Mailion без поддержки TLS, установив параметр `redis_sentinel_single_installation_enabled` в значение `true`. Это необходимо для того, чтобы для каждого сервиса, использующего `redis`, создавался отдельный экземпляр `redis sentinel`, при этом впоследствии все экземпляры `redis sentinel` переключаются в режим TSL за исключением `redis sentinel` для сервиса `rspadm` (см. исключение, пункт 6).
2. Сгенерировать TSL сертификаты для всех серверов `redis` (см. исключение, пункт 6), включая все `sentinel`. Сертификаты должны быть подписаны корневым сертификатом, который будет доступен в клиентах (сервисах, подключающихся к редисам по TLS) - для верификации `redis`, также сертификаты должны включать IP адреса сервисов `redis`, на которых будут серверы `redis` (IP SANs - https://serverfault.com/a/611121).
3. Настроить все `redis` сервера, включая `redis sentinel` на работу с TLS
4. Настройка сервисов с поддержкой TLS для Redis
5. Перезапустить сервисы
6. Обратить внимание на исключение для rspamd: `redis_sentinel_rspamd / redis_rspamd` - оставить как есть без TLS.

4.1.1 Генерация сертификатов и запуск контейнеров с сертификатами

Для генерации сертификатов в нужном формате необходимо добавить следующие изменения в коллекцию `nct.redis` для ролей `redis` и `sentinel`:

1. Добавить переменные для TLS в файлы `redis/defaults/main.yml` и `sentinel/defaults/main.yml`.

```
redis_tls_certs_authority_name: "Intermediate main"
redis_tls_certs_generate_cert_auth_key_name: "services"
```

2. Добавить изменения в следующие файлы:

   В файл `redis/tasks/main.yml` добавить ("Reset vars", "Create TLS certs", "Set TLS directories for mount volumes", "Set container volumes", заменить "Start redis container").

```
- name: "Install python dependencies"
  ansible.builtin.include_role:
```

```
    name: "init"
  when: >
    (redis_packages is not defined) or
    ((redis_packages.changed is defined) and (not redis_packages.changed))

- name: "Reset vars"
  ansible.builtin.set_fact:
    redis_tls_volumes: []
    redis_volumes: []

 - name: "Create TLS certs"
  ansible.builtin.include_role:
    name: "nct.certs.tls_certs"
  vars:
    tls_certs_authority_name: "{{ redis_tls_certs_authority_name }}"
    tls_certs_copy_ca: true
    tls_certs_create_certs: true
    tls_certs_generate_cert_auth_key_name:
"{{ redis_tls_certs_generate_cert_auth_key_name if ca_multiroot else '' }}"
    tls_certs_generate_cert_domain_name: "redis.{{ inventory_hostname }}"
    tls_certs_generate_cert_domain_aliases: ["{{ ansible_nic_ipv4_address }}"]
    tls_certs_generate_cert_key_algorithm: "rsa"
    tls_certs_generate_cert_key_size: 2048
    tls_certs_generate_cert_profile: "both"

- name: "Set TLS directories for mount volumes"
  ansible.builtin.set_fact:
    redis_tls_volumes:
      - "{{ tls_ca }}:/etc/pki/tls/certs/{{ tls_ca_name }}:ro"
      - "{{ tls_cert_client }}:/etc/pki/tls/certs/{{ tls_cert_client_name }}:ro"
      - "{{ tls_cert_server }}:/etc/pki/tls/certs/{{ tls_cert_server_name }}:ro"
      - "{{ tls_key }}:/etc/pki/tls/private/{{ tls_key_name }}:ro"

...

- name: "Set container volumes"
  ansible.builtin.set_fact:
    redis_volumes:
      - "{{ vars['redis_' + redis_id + '_conf_dir'] }}:/etc/redis"
      - "{{ vars['redis_' + redis_id + '_data_dir'] }}:/data"
      - "{{ vars['redis_' + redis_id + '_cluster_conf_dir'] }}:/etc/redis-
cluster"

- name: "Start redis container"
  ansible.builtin.include_role:
    name: "nct.tools.container_launcher"
  vars:
    service_container_management_tool: "{{ redis_container_management_tool }}"
    service_name: "redis_{{ redis_id }}"
    service_image_name: "redis"
    service_image_registry: "{{ redis_image_registry }}"
    service_image_tag: "{{ redis_image_tag }}"
    service_container_state: "started"
    service_container_log_driver: "{{ redis_container_log_driver | default(omit)
}}"
    service_container_log_options: "{{ redis_container_log_options |
default(omit) }}"
    service_container_cpus: "{{ redis_container_cpu_limit | default(omit) }}"
```

```
    service_container_memory: "{{ redis_container_memory_limit |
default(omit) }}"
    service_published_ports:
      - "{{ redis_port }}:{{ redis_port }}"
      - "{{ redis_replication_port }}:{{ redis_replication_port }}"
    service_env:
      TZ: "{{ system_timezone }}"
      REDIS_PASSWORD: "{{ redis_password }}"
    service_volumes: "{{ redis_tls_volumes + redis_volumes }}"
    service_container_command: "{{ redis_command }}"
    when: >
        (redis_static_conf.changed) or (molecule_test_mode is not defined) or
        (not molecule_test_mode) or (redis_sensitive_conf1.changed) or
        (redis_sensitive_conf2.changed) or (redis_sensitive_conf3.changed) or
        (redis_sensitive_conf4.changed)
    service_container_restart: >-
      {{-
        (redis_static_conf.changed) or
        (redis_sensitive_conf1.changed) or
        (redis_sensitive_conf2.changed) or
        (redis_sensitive_conf3.changed) or
        (redis_sensitive_conf4.changed) or
        (tls_certs_generate_cert_force_update | default(omit))
      -}}
    service_published_ports:
      - "{{ redis_sentinel_port }}:{{ redis_sentinel_port }}"
    service_volumes: "{{ redis_sentinel_tls_volumes + redis_sentinel_volumes }}"
    service_container_command: "redis-sentinel /etc/redis/sentinel.conf"
```

В файл `sentinel/tasks/main.yml` добавить ("Reset vars", "Create TLS certs", "Set TLS directories for mount volumes", заменить "Start redis container").

```
- name: "Reset vars"
  ansible.builtin.set_fact:
    redis_sentinel_tls_volumes: []

  - name: "Create TLS certs"
  ansible.builtin.include_role:
    name: "nct.certs.tls_certs"
  vars:
    tls_certs_authority_name: "{{ redis_tls_certs_authority_name }}"
    tls_certs_copy_ca: true
    tls_certs_create_certs: true
    tls_certs_generate_cert_auth_key_name:
"{{ redis_tls_certs_generate_cert_auth_key_name if ca_multiroot else '' }}"
    tls_certs_generate_cert_domain_name: "redis.{{ inventory_hostname }}"
    tls_certs_generate_cert_domain_aliases: ["{{ ansible_nic_ipv4_address }}"]
    tls_certs_generate_cert_key_algorithm: "rsa"
    tls_certs_generate_cert_key_size: 2048
    tls_certs_generate_cert_profile: "both"

- name: "Set TLS directories for mount volumes"
  ansible.builtin.set_fact:
    redis_tls_volumes:
      - "{{ tls_ca }}:/etc/pki/tls/certs/{{ tls_ca_name }}:ro"
      - "{{ tls_cert_client }}:/etc/pki/tls/certs/{{ tls_cert_client_name }}:ro"
      - "{{ tls_cert_server }}:/etc/pki/tls/certs/{{ tls_cert_server_name }}:ro"
      - "{{ tls_key }}:/etc/pki/tls/private/{{ tls_key_name }}:ro"
```

```
...

- name: "Start container"
  ansible.builtin.include_role:
    name: "nct.tools.container_launcher"
  vars:
    service_container_management_tool:
"{{ redis_sentinel_container_management_tool }}"
    service_name: "redis_sentinel_{{ redis_sentinel_name }}"
    service_image_name: "redis"
    service_image_registry: "{{ redis_image_registry }}"
    service_image_tag: "{{ redis_image_tag }}"
    service_container_state: "started"
    service_container_log_driver: "{{ redis_sentinel_container_log_driver |
default(omit) }}"
    service_container_log_options: "{{ redis_sentinel_container_log_options |
default(omit) }}"
    service_container_restart: >-
      {{-
        (sentinel_auth_pass.changed) or
        (sentinel_default_conf.changed) or
        (sentinel_requirepass.changed) or
        (sentinel_static_conf.changed) or
        (tls_certs_generate_cert_force_update | default(omit))
      -}}
    service_published_ports:
      - "{{ redis_sentinel_port }}:{{ redis_sentinel_port }}"
    service_volumes: "{{ redis_sentinel_tls_volumes + redis_sentinel_volumes }}"
    service_container_command: "redis-sentinel /etc/redis/sentinel.conf"
```

В файл `sentinel/tasks/configure_sentinel.yml` добавить ("Reset vars", "Set container volumes").

```
- name: "Reset vars"
  ansible.builtin.set_fact:
    redis_sentinel_volumes: []

- name: "Configure sentinel : create directories required by containers and get
variables"
....

- name: "Set container volumes"
  ansible.builtin.set_fact:
    redis_sentinel_volumes:
      - "{{ vars['redis_sentinel_' + redis_sentinel_name +
'_conf_dir'] }}:/etc/redis"
```

В файл `sentinel/tasks/sanitize_sentinel.yml` добавить ("Reset vars", "Create TLS certs", "Set TLS directories for mount volumes", "Set container volumes", заменить "Start redis container").

```
- name: "Reset vars"
  ansible.builtin.set_fact:
    redis_sentinel_tls_volumes: []
```

```
- name: "Sanitize sentinel : create directories required by containers and get
variables"
...

- name: "Create TLS certs"
  ansible.builtin.include_role:
    name: "nct.certs.tls_certs"
  vars:
    tls_certs_authority_name: "{{ redis_tls_certs_authority_name }}"
    tls_certs_copy_ca: true
    tls_certs_create_certs: true
    tls_certs_generate_cert_auth_key_name:
"{{ redis_tls_certs_generate_cert_auth_key_name if ca_multiroot else '' }}"
    tls_certs_generate_cert_domain_name: "redis.{{ inventory_hostname }}"
    tls_certs_generate_cert_domain_aliases: ["{{ ansible_nic_ipv4_address }}"]
    tls_certs_generate_cert_key_algorithm: "rsa"
    tls_certs_generate_cert_key_size: 2048
    tls_certs_generate_cert_profile: "both"

- name: "Set TLS directories for mount volumes"
  ansible.builtin.set_fact:
    redis_tls_volumes:
      - "{{ tls_ca }}:/etc/pki/tls/certs/{{ tls_ca_name }}:ro"
      - "{{ tls_cert_client }}:/etc/pki/tls/certs/{{ tls_cert_client_name }}:ro"
      - "{{ tls_cert_server }}:/etc/pki/tls/certs/{{ tls_cert_server_name }}:ro"
      - "{{ tls_key }}:/etc/pki/tls/private/{{ tls_key_name }}:ro"

- name: "Set container volumes"
  ansible.builtin.set_fact:
    redis_sentinel_volumes:
      - "{{ vars['redis_sentinel_' + redis_sentinel_name +
'_conf_dir'] }}:/etc/redis"

...

- name: "Start container"
  ansible.builtin.include_role:
    name: "nct.tools.container_launcher"
  vars:
    service_container_management_tool:
"{{ redis_sentinel_container_management_tool }}"
    service_name: "redis_sentinel_{{ redis_sentinel_name }}"
    service_image_name: "redis"
    service_image_registry: "{{ redis_image_registry }}"
    service_image_tag: "{{ redis_image_tag }}"
    service_container_state: "started"
    service_container_log_driver: "{{ redis_sentinel_container_log_driver |
default(omit) }}"
    service_container_log_options: "{{ redis_sentinel_container_log_options |
default(omit) }}"
    service_container_cpus: "{{ redis_sentinel_container_cpu_limit |
default(omit) }}"
    service_container_memory: "{{ redis_sentinel_container_memory_limit |
default(omit) }}"
    service_container_restart: true # we always restart after sanitizing
    service_published_ports:
      - "{{ redis_sentinel_port }}:{{ redis_sentinel_port }}"
    service_volumes: "{{ redis_sentinel_tls_volumes + redis_sentinel_volumes }}"
```

```
    service_container_command: "{{ redis_command }}
{{ redis_sentinel_sanitized_params }}"
```

3. Запустить плейбук обновления ролей `redis` и `redis_sentinel` с перегенирацией сертификатов.

```
ansible-playbook -i inventory/<your_inventory>.yml playbooks/mailion/infra.yml \
    --extra-vars "ansible_user=<your_ansible_user>" \
    --extra-vars "tls_certs_generate_cert_force_update=true" \
    --tags redis_cache,redis_data \
    --diff --limit ucs_redis_cache,ucs_redis_data
```

4. После обновления ролей `redis` и `redis_sentinel` с перегенерацией сертификатов на хостах группы `ucs_redis_cache,ucs_redis_data`, сертификаты будут находиться в каталогах `/srv/tls/certs` и `/srv/tls/private`:

- `redis.<domain>-main-client.pem`
- `redis.<domain>-main-server.pem`
- `redis.<domain>-main-key.pem`
- `...<domain>-main-ca.pem`

4.1.2 Настройка Redis и Sentinel для работы по TLS

Для добавления параметров TLS для Redis и Sentinel следует выполнить команды:

1. Отредактировать файл `/srv/docker/<redis_<имя_сервиса>/conf/redis.conf` для сервисов Redis.
2. Отредактировать файл `/srv/docker/<redis_sentinel_<имя_сервиса>/conf/sentinel.conf` для сервисов Redis Sentinel.
3. Добавить параметры TLS в конфигурационный файл и сохранить.
4. В файлах `redis.conf` и `sentinel.conf` необходимо указать следующие параметры:

```
port 0
tls-auth-clients no
tls-ca-cert-file "/etc/pki/tls/certs/<имя файла tls-ca-cert-file>"
tls-cert-file "/etc/pki/tls/certs/<имя файла tls-cert-file>"
tls-cluster yes
tls-key-file "/etc/pki/tls/private/<имя файла tls-key-file>"
```

```
tls-port <redis_port> или <redis_sentinel_port>
tls-replication yes
```

Пример конфигурации с TLS для Redis и Sentinel:

```
port 0
tls-auth-clients no
tls-ca-cert-file "/etc/pki/tls/certs/intermediate_main.pem"
tls-cert-file "/etc/pki/tls/certs/redis.redis-sentinel-docker-astra-
1.molecule.stageoffice.ru-intermediate_main-server.pem"
tls-cluster yes
tls-key-file "/etc/pki/tls/private/redis.redis-sentinel-docker-astra-
1.molecule.stageoffice.ru-intermediate_main-key.pem"
tls-port <redis_port> или <redis_sentinel_port>
tls-replication yes
# Generated by CONFIG REWRITE
...
```

5. Запустить команду внутри каждого контейнера с Redis и Sentinel

– для контейнеров Redis без аутентификации:

```
docker exec -ti redis_<service_name> redis-cli -p <redis_port> CONFIG REWRITE
```

– для контейнеров Redis с аутентификацей:

```
docker exec -ti redis_<service_name> redis-cli -p <redis_port> --no-auth-warning
-a <redis_password> CONFIG REWRITE
```

– для контейнеров Redis Sentinel без аутентификации:

```
docker exec -ti redis_sentinel_<service_name> redis-cli -p <redis_port> CONFIG
REWRITE
```

– для контейнеров Redis Sentinel, с аутентификацей:

```
docker exec -ti redis_sentinel_<service_name> redis-cli -p <redis_port> --no-
auth-warning -a <redis_password> CONFIG REWRITE
```

После выполнения данных команд, нужно учитывать, что в конфигурационные файлы Redis, Redis Sentinel будет заново добавлена чувствительная информация, которая убирается запуском плейбука:

```
ansible-playbook -i inventory/<your_inventory>.yml playbooks/mailion/infra.yml \
    --extra-vars "ansible_user=<your_ansible_user>" \
    --extra-vars "redis_sentinel_sanitized_enabled=1" \
```

```
    --tags redis_sanitize \
    --diff --limit ucs_redis_cache,ucs_redis_data
```

4.1.3 Настройка сервисов с поддержкой TLS для Redis

Для того, чтобы сервисы обращались к Redis и Sentinel по TLS, необходимо изменить конфигурацию сервисов для секции `redis`:

– Зайти на хосты, где расположен сервис.

– Открыть конфигурационный файл сервиса для редактирования:

```
vim /srv/docker/<имя_сервиса>/conf/config.json
```

– Добавить параметр `"use_tls": true` в секцию `redis`.

– Сохранить изменения.

В таблице 44 для каждого сервиса указана группа хостов. Проверить имена хостов можно по группе в файле `inventory/<your_inventory>.yml`.

Таблица 44 – Группа хостов для сервисов

Сервис	Группа хостов
ares	ucs_caledar
homeros	ucs_catalog
leda	ucs_frontend
erakles	ucs_catalog
viper	ucs_apps
ektor	ucs_catalog
mars	ucs_calendar
hog	ucs_apps
minos	ucs_catalog
euripides	ucs_catalog
rspamd	-
dafnis	ucs_catalog, ucs_calendar
dowal	ucs_apps

Пример файла `config.json`:

```
"redis": {
    "addresses": [
    "redis.mailion-obst-1.redis.stageoffice.ru:26379",
    "redis.mailion-obst-2.redis.stageoffice.ru:26379",
    "redis.mailion-obst-3.redis.stageoffice.ru:26379"
```

```
  ],
  "dial_timeout": "3s",
  "master_name": "minos",
  "max_retries": 0,
  "password": "",
  "pool_size": 25,
  "read_timeout": "10s",
  "redis_mode": "sentinel",
  "use_tls": true,
  "write_timeout": "10s"
},
```

4.1.4 Перезапуск сервисов

Для перезапуска всех контейнеров с Redis и Redis Sentinel нужно зайти на хосты группы `ucs_redis_cache` и `ucs_redis_data` и выполнить:

```
docker restart $(docker ps -qf "name=^redis_")
```

Далее перезапустить сервисы на каждом хосте (см. раздел Настройка сервисов с поддержкой TLS для Redis):

```
docker restart <service_name>
```

После рестарта контейнеров применятся новые настройки с TLS для Redis и Redis Sentinel.

4.2 Доступ к веб-интерфейсам вспомогательных систем для управления ПО «Mailion»

4.2.1 Rspamd

Rspamd – система управления антиспамом (конфигурация правил рейтингов, история обработки). Веб-интерфейс Rspamd доступен по адресу `http://rspamd.<mail_inventory_hostname>:11334/`.

Где `<mail_inventory_hostname>` - FQDN хоста из группы **ucs_mail** (см. Рисунок 4).

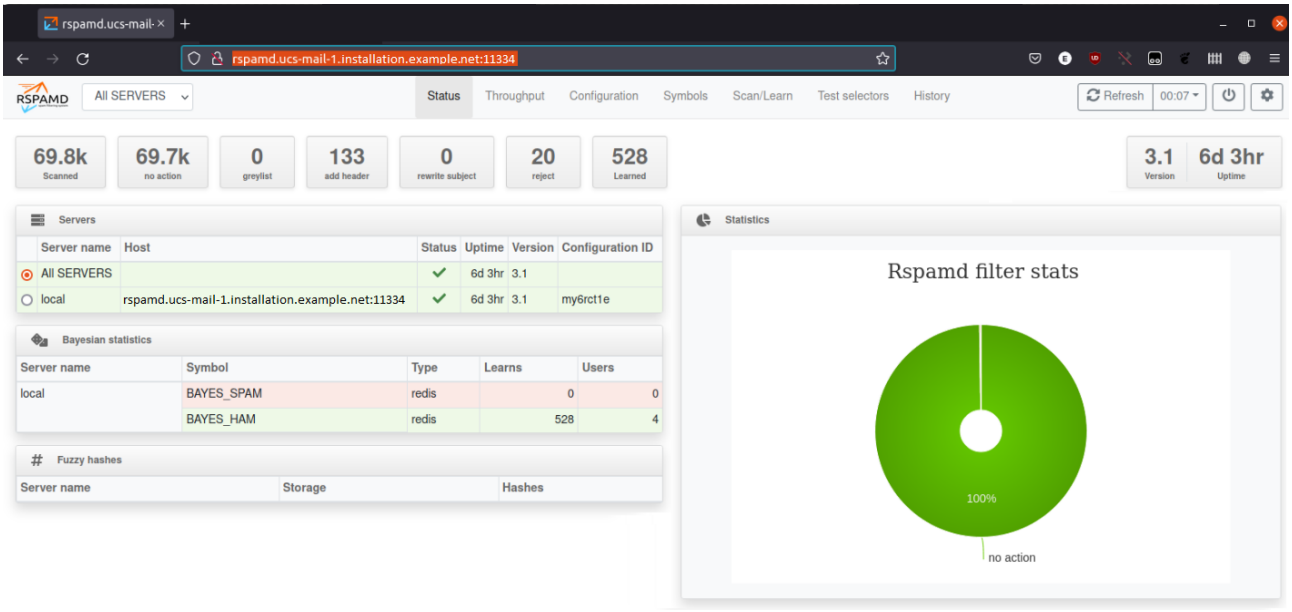


Рисунок 4 – Веб-интерфейс Rspamd

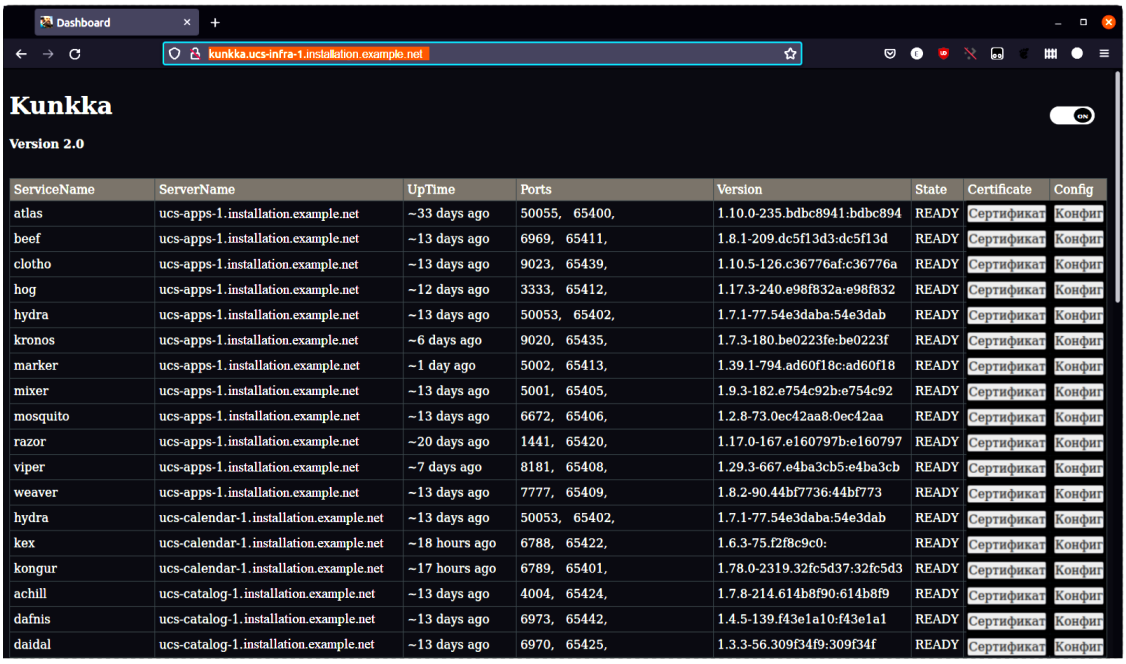
Доступ в Rspamd необходимо осуществлять по протоколу HTTP из внутренней сети инсталляции.

Для доступа к веб-интерфейсу потребуется пароль, который указан в переменной **rspamd_web_password**.

4.2.2 Kunkka

Kunkka – веб-страница с отображением подсистем на серверах. Веб-интерфейс Kunkka доступен по адресу `http://kunkka.<infrastructure_inventory_hostname>/`.

Где `<infrastructure_inventory_hostname>` - FQDN хоста группы **ucs_infrastructure** (см. Рисунок 5).



ServiceName	ServerName	UpTime	Ports	Version	State	Certificate	Config
atlas	ucs-apps-1.installation.example.net	~33 days ago	50055, 65400,	1.10.0-235.bdbc8941:bdbc894	READY	Сертификат	Конфиг
beef	ucs-apps-1.installation.example.net	~13 days ago	6969, 65411,	1.8.1-209.dc5f13d3:dc5f13d	READY	Сертификат	Конфиг
clotho	ucs-apps-1.installation.example.net	~13 days ago	9023, 65439,	1.10.5-126.c36776af:c36776a	READY	Сертификат	Конфиг
hog	ucs-apps-1.installation.example.net	~12 days ago	3333, 65412,	1.17.3-240.e98f832a:e98f832	READY	Сертификат	Конфиг
hydra	ucs-apps-1.installation.example.net	~13 days ago	50053, 65402,	1.7.1-77.54e3daba:54e3dab	READY	Сертификат	Конфиг
kronos	ucs-apps-1.installation.example.net	~6 days ago	9020, 65435,	1.7.3-180.be0223fe:be0223f	READY	Сертификат	Конфиг
marker	ucs-apps-1.installation.example.net	~1 day ago	5002, 65413,	1.39.1-794.ad60f18c:ad60f18	READY	Сертификат	Конфиг
mixer	ucs-apps-1.installation.example.net	~13 days ago	5001, 65405,	1.9.3-182.e754c92b:e754c92	READY	Сертификат	Конфиг
mosquito	ucs-apps-1.installation.example.net	~13 days ago	6672, 65406,	1.2.8-73.0ec42aa8:0ec42aa	READY	Сертификат	Конфиг
razor	ucs-apps-1.installation.example.net	~20 days ago	1441, 65420,	1.17.0-167.e160797b:e160797	READY	Сертификат	Конфиг
viper	ucs-apps-1.installation.example.net	~7 days ago	8181, 65408,	1.29.3-667.e4ba3cb5:e4ba3cb	READY	Сертификат	Конфиг
weaver	ucs-apps-1.installation.example.net	~13 days ago	7777, 65409,	1.8.2-90.44bf7736:44bf773	READY	Сертификат	Конфиг
hydra	ucs-calendar-1.installation.example.net	~13 days ago	50053, 65402,	1.7.1-77.54e3daba:54e3dab	READY	Сертификат	Конфиг
kex	ucs-calendar-1.installation.example.net	~18 hours ago	6788, 65422,	1.6.3-75.f2f8c9c0:	READY	Сертификат	Конфиг
kongur	ucs-calendar-1.installation.example.net	~17 hours ago	6789, 65401,	1.78.0-2319.32fc5d37:32fc5d3	READY	Сертификат	Конфиг
achill	ucs-catalog-1.installation.example.net	~13 days ago	4004, 65424,	1.7.8-214.614b8f90:614b8f9	READY	Сертификат	Конфиг
dafnis	ucs-catalog-1.installation.example.net	~13 days ago	6973, 65442,	1.4.5-139.f43e1a10:f43e1a1	READY	Сертификат	Конфиг
daidal	ucs-catalog-1.installation.example.net	~13 days ago	6970, 65425,	1.3.3-56.309f34f9:309f34f	READY	Сертификат	Конфиг

Рисунок 5 – Веб-интерфейс Kunkka

Для доступа может потребоваться логин «admin» и пароль, хранящийся в переменной **mailion_internal_web_auth.password.**

4.2.3 Prometheus

Prometheus – система мониторинга. Веб-интерфейс Prometheus доступен по адресу `http://prometheus.<infrastructure_inventory_hostname>/`.

Где `<infrastructure_inventory_hostname>` - FQDN хоста группы **ucs_infrastructure** (см. Рисунок 6).

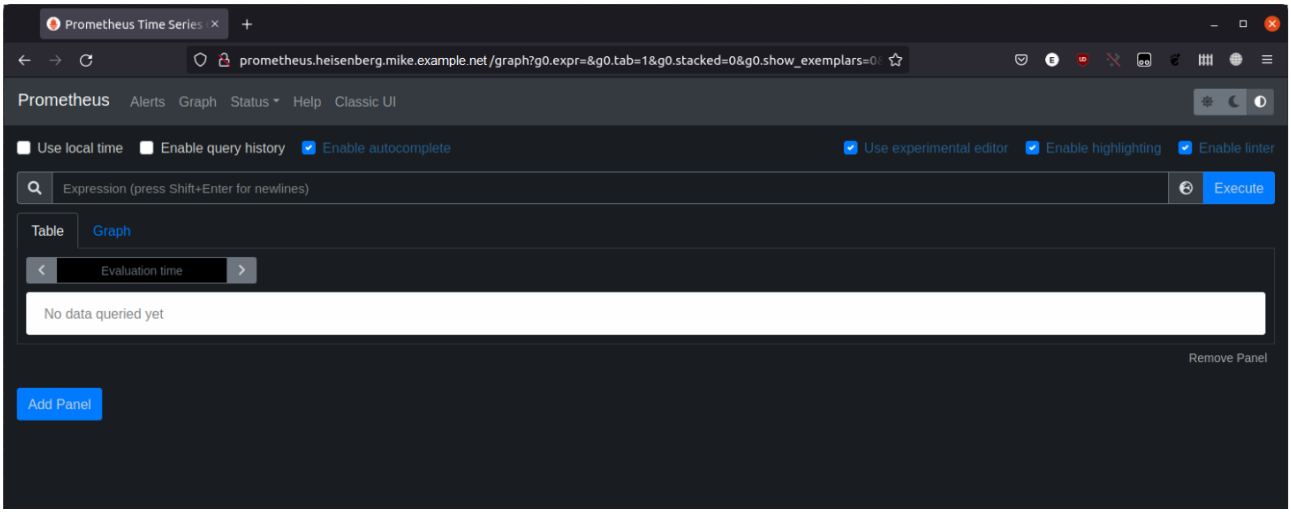


Рисунок 6 – Веб-интерфейс Prometheus

Для доступа может потребоваться логин «admin» и пароль, хранящийся в переменной **mailion_internal_web_auth.password**.

4.2.4 Alertmanager

Alertmanager – система алертинга. Веб-интерфейс Alertmanager доступен по адресу `http://alertmanager.<infrastructure_inventory_hostname>/`.

Где `<infrastructure_inventory_hostname>` - FQDN хоста группы **ucs_infrastructure** (см. Рисунок 7).

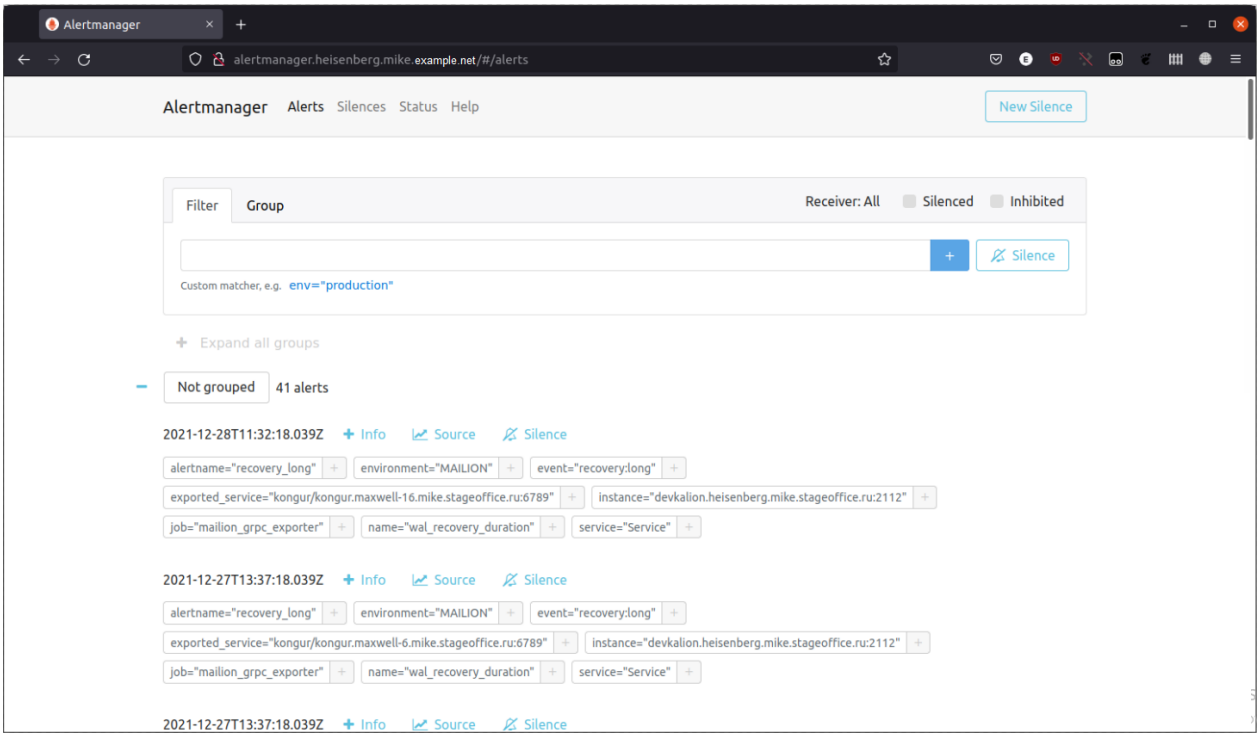


Рисунок 7 – Веб-интерфейс Alertmanager

Для доступа может потребоваться логин «admin» и пароль, хранящийся в переменной **mailion_internal_web_auth.password.**

4.2.5 Grafana

Grafana – система отображения метрик. Веб-интерфейс Grafana доступен по адресу `http://grafana.<infrastructure_inventory_hostname>`.

Где `<infrastructure_inventory_hostname>` - FQDN хоста группы **ucs_infrastructure** (см. Рисунок 8).

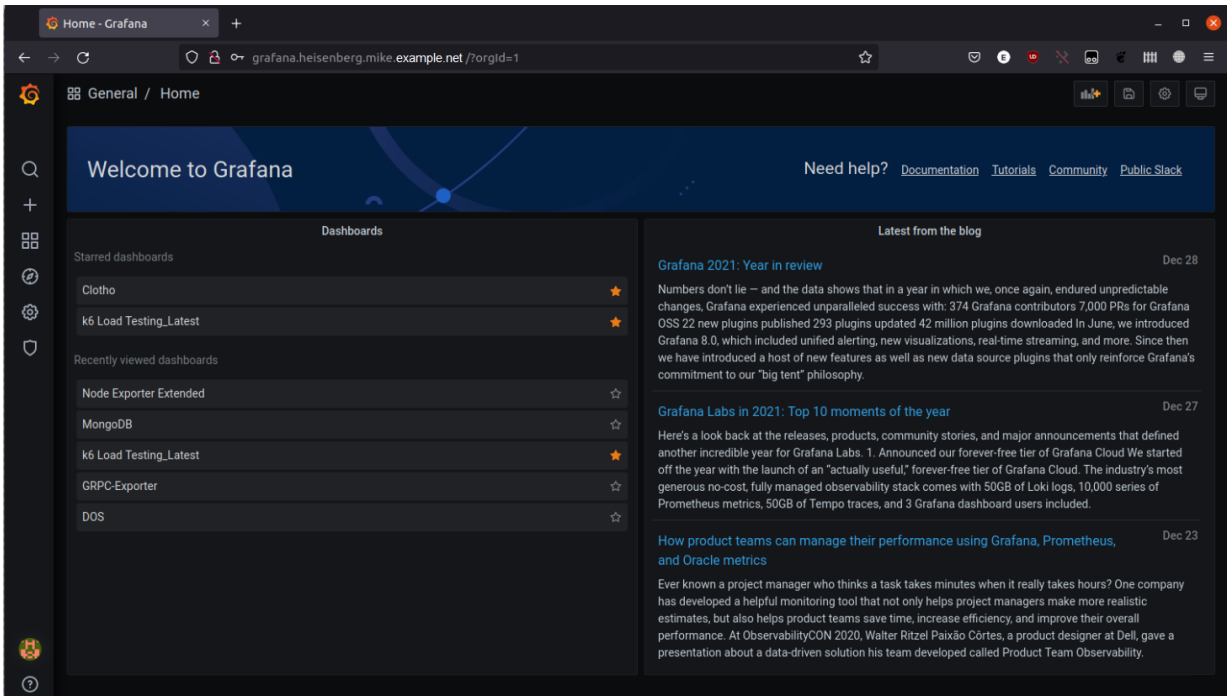


Рисунок 8 – Веб-интерфейс Grafana

Для доступа может потребоваться логин «admin» и пароль, хранящийся в переменной **grafana_admin_password**.

4.3 Настройка взаимодействия со службой каталогов

Для настройки интеграции с одним из каталогов (Microsoft Active Directory, FreeIPA, ALD Pro, РЕД АДМ и Samba DC) до инсталляции необходимо в соответствующем словаре указать уникальный ключ, в котором будут храниться параметры интеграции. Ключ можно сгенерировать с помощью команды «**pwgen 25 1**».

Настройки интеграции необходимо прописать в файле **group_vars/ucs_setup/main.yml/**. Пользователь, который прописывается в секции **bind_user** в данном конфигурационном файле, должен иметь права доступа на чтение к дереву Microsoft Active Directory, FreeIPA, ALD Pro и Samba DC.

Корректно заполненные параметры приведены ниже.

```
integrations:
 microsoft:
   "IS7YluhZ318G7Sm89SkkfZbO":
     ads:
       base_dn: "dc=example,dc=net"
       bind_user: "example\\aduser"
```

```
      bind_password: "adUserPassword"
      name: "AD"
      servers:
        - endpoint: "dc.example.net:636"
          tls:
            ca_filename: "ca_example.net.pem"
            cert_file: ""
            key_file: ""
          use_tls: true
      use_dc: false
    exchanges:
      exchange_version: "Exchange2013_SP1"
      ca_filename: ""
freeipa:
  "zuif6jeifiQueey5ahWatoo0o":
    dcs:
      base_dn: "dc=ipa-example,dc=net"
      bind_user: "uid=admin,cn=users,cn=accounts,dc=ipa-example,dc=net"
      bind_password: "adminPassword"
      name: "FreeIPA"
      servers:
        - endpoint: "freeipa.ipa-example.net:389"
          tls:
            ca_filename: ""
            cert_file: ""
            key_file: ""
          use_tls: false
      use_dc: false
samba_dc:
  "PeZh0WisXah5thooWhoo9bgG":
    smb:
      base_dn: "DC=samba-dc-test,DC=example,DC=com"
      bind_user: "Administrator"
      bind_password: "ahTh6uu7sah4so1C"
      name: "SAMBA_DC"
      servers:
        - endpoint: "samba-dc-test.example.com:389"
          tls:
            ca_filename: ""
```

```
            cert_file: ""
            key_file: ""
          use_tls: false
      use_dc: false
 aldpro:
   "ALDh9ZisXah5thooWhoo9bgZ":
     ald:
       base_dn: "DC=domain,DC=test"
       bind_user: "admin"
       bind_password: "ahTh6uu7sah4so1C"
       name: "ALDPRO"
       servers:
         - endpoint: "aldpro-test.example.com:389"
           tls:
             ca_filename: ""
             cert_file: ""
             key_file: ""
           use_tls: false
       use_dc: false
```

Для включения интеграции с Microsoft Active Directory необходимо указать в групповых переменных:

```
mailion_integrations:
 microsoft: true
```

Для включения интеграции с FreeIPA необходимо указать в групповых переменных:

```
mailion_integrations:
 freeipa: true
```

Для включения интеграции с ALD Pro необходимо указать в групповых переменных:

```
mailion_integrations:
 aldpro: true
```

Для включения интеграции с Samba DC необходимо указать в групповых переменных:

```
mailion_integrations:
 samba_dc: true
```

Поддержка каталога РЕД АДМ осуществляется без заполнения параметров в конфигурационном файле.

В настройках для Microsoft Active Directory добавлена возможность конфигурировать используемую версию Exchange. Для этого используется переменная **exchange_version**. Она будет влиять на поддерживаемую версию Exchange, с которой идут запросы в EWS API. Данная переменная находится в разделе **exchanges**.

```
microsoft:
   ..................
   ads:
   ..................
   exchanges:
     ..................
     exchange_version: "Exchange2013_SP1"
```

Доступны следующие варинаты:

– "Exchange2010";

– "Exchange2010_SP1";

– "Exchange2010_SP2";

– "Exchange2013";

– "Exchange2013_SP1".

Если переменная не задана, то по умолчанию будет использовано значение "Exchange2013_SP1".

В настройках exchange присутствует поле **tls_min_version**. Оно содержит минимальную приемлемую версию TLS для работы с сервисами.

Данная настройка является обязательной для установки (значение по умолчанию не задано), без нее сервисы работать не будут.

Расположение переменной в файле конфигурации:

```
integrations:
  ..................
  microsoft:
    ..................
    exchanges:
      ..................
      servers:
          tls_min_version: "..."
```

В настройках exchange обязательным является поле **ca_filename**. Оно содержит имя файла сертификата, который необходимо скопировать в папку `~/install_mailion/certificates/` перед инсталляцией .

Расположение переменной **ca_filename** в файле конфигурации:

```
microsoft:
    ...................
    ads:
    ...................
    exchanges:
      ...................
      ca_filename: ""
```

4.4 Настройка антивирусного программного обеспечения

В ПО «Mailion» **Rspamd** поддерживает несколько сторонних антивирусных модулей, в том числе KSE (Kaspersky). Настройка данного модуля осуществляется через переменные роли **Rspamd**. Подробное описание этих ролей приведено в таблицах 45 и 46.

Таблица 45 – Настройка Rspamd role vars

Параметр	Пример заполнения	Описание
rspamd:		
kse_use_https:	false	Использование **https** для подключения к серверам Касперского
kse_endpoints:	[]	Адреса серверов Касперского для обновления сигнатур (Обязательно наличие инсталляции KSE внутри компании)
kse_timeout:	"5.0"	Максимальный период времени для сканирования объекта
kse_scan_mime_parts:	true	Включение сканирования вложений
kse_use_files:	false	Отключение file mode в пользу TCP Stream. Не рекомендуется менять значение на true, режим file mode используется только для случаев наличия быстрой **tmpfs**
kse_max_size:	2048000	Максимальный размер файла для сканирования

Включение модуля антивирусной защиты Kaspersky осуществляется через групповые переменные инсталлятора ПО «Mailion», при наличии установленного в компании Сервера управления «Касперский антивирус».

Таблица 46 – Настройка Rspamd role vars

Параметр	Пример заполнения	Описание
rspamd:		
kse_enabled	true	Включение модуля Касперский для **rsmapd**
kse_endpoints:	"kaspersky.example.net:8085"	Список серверов управления антивирусной защитой Касперский

Продукт Kaspersky Scan Engine не является частью поставки ПО «Mailion».

4.5 Настройка сервиса Vault

Сервис хранения ключей Vault поддерживает многосерверный режим для обеспечения высокой доступности. Этот режим защищает от сбоев в работе за счет запуска нескольких серверов хранилища. Режим высокой доступности включается автоматически при использовании хранилища данных, которое его поддерживает.

Vault работает в такой схеме, когда все инстансы кластера развернуты и работоспособны, при этом только один инстанс активен. Он принимает запросы на чтение/запись, остальные инстансы остаются в режиме ожидания и перенаправляют все запросы на активный инстанс. Если активный инстанс выходит из строя, кластер сам выбирает новый активный хост, и система продолжает работать.

Все данные (секреты) автоматически синхронизируются и хранятся на всех трех инстансах. Количество инстансов Vault в кластере должно быть нечетным.

4.5.1 Установка сервиса Vault

Необходимо установить Vault на хосты vault1, vault2, vault3, при этом сам Vault не запускать и не распечатывать.

Для этого необходимо установить и запустить первый инстанс Vault.

Установка Vault сервера **осуществляется до установки остальных компонент** ПО «Mailion» один раз, в дальнейшем не нужно выполнять установку Vault, если она уже была выполнена или если нет рекомендаций по переустановке.

4.5.1.1 Этапы установки

1. Подготовить DNS-запись, по которой будет происходить обращение к сервису Vault.
2. Убедиться в доступности портов 8200, 8201, или других, если планируется их использовать на машине, которая будет предназначена для развертывания Vault.
3. Необходимо подготовить 3 файла для корректной работы сервиса Vault. Все файлы должны быть выпущены на доменное имя, подготовленное в предыдущем пункте, либо должны поддерживать Wildcard SSL сертификат, в который входит доменное имя из предыдущего пункта.

   Пример: если доменное имя **vault.example.ru**, то сертификаты должны быть выпущены либо на домен **vault.example.ru**, либо на ***.example.ru**. В последнем случае допустимо использовать сертификаты, уже подготовленные для инсталляции Mailion (см. раздел Размещение ssl-сертификатов):

- CA сертификат, подписанный доверенным удостоверяющим центром (необходимо использовать для корректной работы);
- сертификат сервера, подписанный подготовленным в предыдущем пункте приватным ключом CA;
- приватный ключ для сертификата из предыдущего пункта.

4. Подготовленные ранее сертификаты необходимо расположить в директории коллекции **nct.certs/roles/tls_certs/files/**. Данная директория будет создана после распаковки установщика.
5. Необходимо обновить файл **inventory** и указать в нем созданные файлы. Пример секции в конфигурационном файле:

```
vault_tls:
  enabled: true
  certs:
    ca_filename: "<Имя CA файла>"
    cert_filename: "<Имя файла сертификата сервера>"
    key_filename: "<Имя файла ключа сервера>"
```

6. Выполнить команду установки:

```
install-mailion playbooks/mailion/vault.yml --tags=mln_vault -i <Путь к файлу inventory>
```

7. Необходимо распаковать сервис Vault. Для этого перейти в веб-браузере по адресу Vault сервиса с указанием порта и схемы (пример: https://vault.example.ru:8200). На странице будет предложено задать несколько параметров:
   - Key shares – количество ключей, которое будет сгенерировано;
   - Key threshold - количество ключей из сгенерированных, которое понадобиться для распаковки Vault. Не может быть больше, чем Key shares.
8. Задать значения и инициализировать сервис. Будет предложено сохранить сгенерированные значения ключей для распаковки и токен для root-доступа на сервер в файл.

Необходимо обязательно сохранить файл! В случае рестарта сервиса Vault без ключей для распаковки его будет невозможно восстановить, так как все данные будут зашифрованы. Также для настройки понадобится root token, его можно будет перевыпустить, используя ключи для распаковки.

9. Ввести сохраненные ключи для распаковки, пока сервер не будет распакован полностью.

4.5.1.2 Настройка Vault AppRole и доступа к кластеру для приложений

Для настройки Vault AppRole и доступа к кластеру необходимо запустить команду:

```
install-mailion playbooks/mailion/vault.yml --tags=mln_vault_init -i <Путь к файлу inventory> -e vault_init_address=<Полный адрес до Vault сервера вместе с портом и схемой> -e vault_init_token=<Root токен, сохраненный на этапе инициализации Vault сервера>
```

Данная команда создает AppRole и необходимые политики доступа на Vault сервере, также она инициализирует пустой секрет по нужному пути.

В выводе данной команды будет указан токен **APP_ROLE_TOKEN** для доступа на Vault сервер для приложений ПО «Mailion», который нужно сохранить. Срок действия данного токена - 1 год. Для перевыпуска токена можно запустить команду еще раз.

4.5.1.3 Инициализация секретов

Чтобы создать список секретов необходимо выполнить следующие действия:

1. Проанализировать файл inventory и сохранить результат в файл с помощью команды:

```
grep -rni 'vault:.*' <Путь к директории с inventory файлами> | grep -o 'vault:.*' | sed 's/vault://g' | tr -d '\"' |  sort -h | uniq > first.txt
```

2. Проанализировать файл inventory на предмет других секретов с помощью команды:

```
grep -rnio 'vault_secrets\[.*\]' <Путь к директории с inventory файлами>  | grep -o '\[.*\]' | tr -d "[,']" | sort -h | uniq > second.txt
```

3. Сформировать финальный список секретов, которые необходимо внести в Vault. Для этого выполнить команду:

```
cat first.txt second.txt | sort -h | uniq > final_secret_list.txt
```

Сформированный файл будет содержать список секретов, которые необходимо внести в Vault. Значения для секретов заполняются самостоятельно.

4. Также необходимо проанализировать inventory файл на наличие открытых паролей, указанных в открытом виде. В случае наличия таковых, значения для них можно поменять на маскированные значения, и добавлять свои секреты в Vault.

Подробная информация приведена в приложении Настройки inventory файла для работы с Vault).

5. В веб-браузере зайти на сервис Vault, используя полный адрес с портом.
6. Авторизоваться, используя root токен, полученный на этапе инициализации сервиса Vault.
7. Перейти во вкладку Secrets, в списке секретов перейти на **mailion** и далее на **installation**. Путь для секретов **mailion/installation**.
8. Нажать кнопку **Create new version** и заполнить в соответствии с полученными ранее секретами.
9. Создать секрет **vault_token** в качестве значения, указать токен для доступа приложений, полученный ранее на этапе настройки Vault AppRole (см. Настройка Vault AppRole и доступа к кластеру для приложений).
10. Для удобства можно заполнить в виде файла в формате JSON. Для этого есть специальная кнопка JSON, нужно ее включить.

4.5.1.4 Настройка .ansible.cfg для доступа к развернутому Vault серверу

Для настройки необходимо отредактировать файл **~/.ansible.cfg** на той машине, с которой планируется запускать установку ПО «Mailion», добавив следующую секцию:

```
[hashi_vault_collection]
token_path = /Users/user/projects/secrets/
token_file = vault.token # Внутри файла необходимо указать токен для приложений, полученный ранее на этапе настройки Vault AppRole
url = https://vault.server.company:8200 # URL, где будет доступен hosted vault – в случае с HA vault – достаточно одного из инстансов
```

4.5.1.5 Подготовка inventory файла

Для дальнейшей установки ПО «Mailion» необходимо подготовить inventory файл. При использовании Vault необходимо использовать `main.yml.hosted_vault`. Данный файл конфигурациии достаточно хорошо документирован, описание использования каждой секции подробно описано в комментариях.

Пример:

```
## ANSIBLE configuration
## remote SSH user with correct permissions
```

```
ansible_user: "root"
################################################################################
####################
# данный файл содержит актуальный пример настроек переменных
# в случае установки Mailion вместе с hosted vault
################################################################################
############

################################################################################
############
# данная секция обеспечивает
# интеграцию ansible с hosted vaut сервером
# для интеграции
# необходимо включить переменные:
# use_hashi_vault_secrets,
# use_hashi_vault_ad_secrets
.............................
```

4.5.2 Установка на другие хосты

Установка на другие хосты (vault2, vault3) осуществляется стандартным способом скачивания Vault дистрибутива с docker-контейнера, на котором запущен первый vault инстанс:

```
ssh infra # зайти на машину, на которой запущен докер контейнер с первым vault
инстансом
sudo docker cp vault:/usr/local/bin/vault /tmp/vault
sudo chmod a+r /tmp/vault
exit
ssh vault2
scp infra:/tmp/vault vault
sudo mv /tmp/vault /usr/local/bin/
./vault --version
```

4.5.3 Создание доменных имен

Опционально: для каждого из хостов, на DNS-серверах разворачиваемой инфраструктуры создать доменные имена:

– vault1.stageoffice.ru;

– vault2.stageoffice.ru;

– vault3.stageoffice.ru.

Для этого перед установкой ПО «Mailion» необходимо добавить в файл (пример: ./папка_инсталяции/group_vars/ucs_Имя_Стенда/main.yml) следующие опции:

```
- type: "transparent"
    zone: "vault1.stageoffice.ru"
    local_data:
      - domain: "vault1.stageoffice.ru"
        type: "A"
        ip: "192.168.0.1"
  - type: "transparent"
    zone: "vault2.stageoffice.ru"
    local_data:
      - domain: "vault2.stageoffice.ru"
        type: "A"
        ip: "192.168.0.2"
  - type: "transparent"
    zone: "vault3.stageoffice.ru"
    local_data:
      - domain: "vault3.stageoffice.ru"
        type: "A"
        ip: "192.168.0.3"
```

На серверах с Vault рекомендуется добавить в файле **/etc/hosts** следующие записи:

```
192.168.0.1 vault1.stageoffice.ru
192.168.0.2 vault2.stageoffice.ru
192.168.0.3 vault3.stageoffice.ru
```

Секции IP-адресов необходимо установить на соответствующие устанавливаемой конфигурации.

4.5.4 Генерация CA сертификата

Необходимо выпустить Wildcard SSL сертификат под домен для инсталляции ПО «Mailion» в аккредитованном центре сертификации. Либо использовать уже имеющийся Wildcard SSL сертификат аккредитованного CA и формировать доменные имена третьего уровня исходя из имени домена, на который он был выдан.

В результате должны получиться три файла:

– server.crt;

– server.key;

– ca.pem.

4.5.5 Создание сертификатов для каждого инстанса

Для работы Vault необходимы сертификаты в формате PEM. Ключи могут уже быть в формате PEM, но им просто будет присвоено имя .crt или .key.

Если они начинаются с -----BEGIN и есть возможность прочитать их в текстовом редакторе (они используют base64, который читается в ASCII, а не в двоичном формате), то они находятся в формате PEM.

Если файлы в двоичном формате:

```
#для server.crt необходимо использовать:
openssl x509 -inform DER -outform PEM -in server.crt -out server_crt.pem

#для server.key необходимо использовать:
openssl rsa -inform DER -outform PEM -in server.key -out server_key.pem
```

Чтобы настроить параметр **tls_cert_file** в секции **listener** на использование сертификата CA, объедините основной сертификат (server.crt) и сертификат CA (ca.pem) в одном файле server.pem:

```
cat server.crt ca.pem > server.pem
```

В результате файл server.pem должен содержать сертификат и цепочку корневого сертификата:

```
cat server.pem
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

После этого необходимо скопировать сертификаты, созданные на предыдущем шаге в пути установки Vault и изменить владельцев и права доступа:

```
cp ./server_key.pem ./server.pem ./ca.pem /opt/vault/tls
chown root:root /opt/vault/tls/ca.pem
chown root:root /opt/vault/tls/server.pem
chown root:vault /opt/vault/tls/server_key.pem
chmod 0644 /opt/vault/tls/ca.pem
```

```
chmod 0644 /opt/vault/tls/server.pem
chmod 0644 /opt/vault/tls/server_key.pem
```

Для управления верификацией используется переменная

othrys_insecure_skip_verify: true

Значение **false** включает верификацию недоверенных сертификатов, значение **true** игнорирует ее

4.5.6 Настройка конфигурационного файла Vault для каждого инстанса

Для каждого из хостов, где установлен Vault необходимо создать один и тоже конфигурационный файл с разницей только в том, что необходимо указать доменное имя хоста и IP адрес, по которому Vault будет доступен.

Во всех секциях, где необходимо указать TLS сертификаты, нужно указать сертификат/ключ, а также CA сертификат, созданные на предыдущем шаге.

Для первого инстанса Vault, запущенного, как docker контейнер, предварительно рекомендуется сделать резервную копию директории **/srv/docker/vault**.

Далее необходимо отредактировать конфигурационный файл по пути **/srd/docker/vault/conf/config.hcl** способом, аналогичным другим инстансам. После того, как он будет отредактирован, необходимо перезапустить контейнер с помощью команды **sudo docker restart vault**.

```
ssh infra # машина в кластере mailion, на которой запущен первый vault инстанс
cat << HERE > /srv/docker/vault/config/vault.hcl
cluster_addr = "https://192.168.0.1:8201
api_addr = "https://192.168.0.1:8200
disable_mlock = true
ui = true

 listener "tcp" {
  address = "0.0.0.0:8200"
  tls_client_ca_file = "/opt/vault/tls/ca.pem"
  tls_cert_file = "/opt/vault/tls/server.pem"
  tls_key_file = "/opt/vault/tls/server_key.pem"
 }

# секция raft содержит в себе ссылки на _все_ инстансы vault
# доступные в кластере (включая инстанс, который установлен на данном хосте)
 storage "raft" {
```

```
  path = "/opt/vault/data"
  node_id = "vault1.stageoffice.ru"

 retry_join {
  leader_tls_servername = "vault1.stageoffice.ru"
  leader_api_addr = "https://192.168.0.1:8200
  leader_ca_cert_file = "/opt/vault/tls/ca.pem"
  leader_client_cert_file = "/opt/vault/tls/server.pem"
  leader_client_key_file = "/opt/vault/tls/server_key.pem"
 }
 retry_join {
  leader_tls_servername = "vault2.stageoffice.ru"
  leader_api_addr = "https://192.168.0.2:8200
  leader_ca_cert_file = "/opt/vault/tls/ca.pem"
  leader_client_cert_file = "/opt/vault/tls/server.pem"
  leader_client_key_file = "/opt/vault/tls/server_key.pem"
 }
 retry_join {
  leader_tls_servername = "vault3.stageoffice.ru"
  leader_api_addr = "https://192.168.0.3:8200
  leader_ca_cert_file = "/opt/vault/tls/ca.pem"
  leader_client_cert_file = "/opt/vault/tls/server.pem"
  leader_client_key_file = "/opt/vault/tls/server_key.pem"
 }
}
HERE
ssh vault2
[root@vault1] cat << HERE > /etc/vault.d/vault.hcl
cluster_addr  = "https://192.168.0.1:8201
api_addr      = "https://192.168.0.1:8200
disable_mlock = true

ui = true

listener "tcp" {
  address             = "0.0.0.0:8200"
  tls_client_ca_file  = "/opt/vault/tls/ca.pem"
  tls_cert_file       = "/opt/vault/tls/server.pem"
```

```
  tls_key_file        = "/opt/vault/tls/server_key.pem"
}

# секция raft содержит в себе ссылки на _все_ инстансы vault
# доступные в кластере (включая инстанс, который установлен на данном хосте)
storage "raft" {
  path    = "/opt/vault/data"
  node_id = "vault2.stageoffice.ru"

  retry_join {
    leader_tls_servername   = "vault1.stageoffice.ru"
    leader_api_addr         = "https://192.168.0.1:8200
    leader_ca_cert_file     = "/opt/vault/tls/ca.pem"
    leader_client_cert_file = "/opt/vault/tls/server.pem"
    leader_client_key_file  = "/opt/vault/tls/server_key.pem"
  }
  retry_join {
    leader_tls_servername   = "vault2.stageoffice.ru"
    leader_api_addr         = "https://192.168.0.2:8200
    leader_ca_cert_file     = "/opt/vault/tls/ca.pem"
    leader_client_cert_file = "/opt/vault/tls/server.pem"
    leader_client_key_file  = "/opt/vault/tls/server_key.pem"
  }
  retry_join {
    leader_tls_servername   = "vault3.stageoffice.ru"
    leader_api_addr         = "https://192.168.0.3:8200
    leader_ca_cert_file     = "/opt/vault/tls/ca.pem"
    leader_client_cert_file = "/opt/vault/tls/server.pem"
    leader_client_key_file  = "/opt/vault/tls/server_key.pem"
  }
}
HERE
```

4.5.7 Рестарт, распечатка первого инстанса Vault

Когда конфигурационные файлы готовы, необходимо на первый узел (vault1) и запустить сервис Vault с помощью команды:

```
ssh infra
docker restart vault
#  зайти в web интерфейс и распечатать
```

4.5.8 Запуск и распечатка остальных инстансов Vault

Для всех остальных нод кластера необходимо запустить и распечатать сервис Vault.

Инициализация для данных инстансов не требуется.

```
ssh vault2
sudo apt-get install screen
screen # мы будем использовать screen для запуска vault в режиме сервиса
# вы также можете создать systemd unit для этого и запускать vault сервис через
systemd
# следуйте руководству вашего Linux дистрибутива о том, как создавать новые
systemd сервисы

sudo vault server
^D # выход из screen сессии
vault operator unseal
```

Для распечатки необходимо следовать процедуре, описанной в разделе Рестарт, распечатка первого инстанса Vault. Использовать те же ключи распечатки, которые использовали для распечатки первого инстанса. Пример **systemd** конфигурации для сервиса Vautl. Выполняется с помощью команды **nano /etc/systemd/system/vault.service**.

```
[Unit]
Description=a tool for managing secrets
Documentation=https://vaultproject.io/docs/
After=network.target
ConditionFileNotEmpty=/etc/vault.d/vault.hcl

[Service]
User=vault
Group=vault
ExecStart=/usr/local/bin/vault server -config=/etc/vault.d/vault.hcl
ExecReload=/usr/local/bin/kill --signal HUP $MAINPID
CapabilityBoundingSet=CAP_SYSLOG CAP_IPC_LOCK
Capabilities=CAP_IPC_LOCK+ep
```

```
SecureBits=keep-caps
NoNewPrivileges=yes
KillSignal=SIGINT

[Install]
WantedBy=multi-user.target
```

Запуск через system:

```
systemctl daemon-reload
systemctl enable --now vault.service
systemctl start  vault.service
systemctl status vault.service
```

4.5.9 Верификации работы кластера

На данном этапе сформирован кластер из трех нод. Для верификации необходимо вернуться на вторую ноду и проверить состояние кластера.

Необходимо авторизоваться с токеном, который был получен ранее:

```
ssh vault2
vault login
Token (will be hidden):
Success! You are now authenticated. The token information displayed below
is already stored in the token helper. You do NOT need to run "vault login"
again. Future Vault requests will automatically use this token.
```

Затем проверить статус хранилища:

```
[root@vault1]# vault operator raft list-peers
Node                    Address             State       Voter
----                    -------             -----       -----
vault1.stageoffice.ru    192.168.0.1:8201    leader      true
vault2.stageoffice.ru    192.168.0.2:8201    follower    true
vault3.stageoffice.ru    192.168.0.3:8201    follower    true
```

По статусу видно 3 сервера, один из которых в статусе лидера, а два других – ведомые.

4.6 Дополнительные настройки микросервиса imap

Для корректной работы микросервиса imap в файл конфигурации /srv/docker/imap/conf/config.json необходимо добавить следующие параметры:

```
{
...
"beef_client_cache": {"disable": true},
"tag_object_cache": {"disable": true},
...
"disable_audit": true,
...
}
```

5 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Контактная информация службы технической поддержки ООО «Новые облачные технологии» в случае возникновения вопросов, неописанных в данном руководстве:

- Адрес электронной почты: support@service.myoffice.ru
- Телефон: 8-800-222-1-888.

6 ПРИЛОЖЕНИЕ А - ПРИМЕР НАПИСАНИЯ ВНЕШНИХ DNS-ЗАПИСЕЙ

Имя записи	Пример написания записи
api	api-test.example.com IN A <ucs_frontend_vip>
auth	auth-test.example.com IN A <ucs_frontend_vip>
autoconfig	autoconfig-test.example.com IN A <ucs_frontend_vip>
avatars	avatars-test.example.com IN A <ucs_frontend_vip>
caldav	caldav-test.example.com. 900 IN CNAME <ucs_frontend_vip>
carddav	carddav-test.example.com. 878 IN CNAME <ucs_frontend_vip>
db	db-test.example.com IN A <ucs_frontend_vip>
grpc	grpc-test.example.com IN A <ucs_frontend_vip>
imap	imap-test.example.com IN A <ucs_frontend_vip>
mail	mail-test.example.com IN A <ucs_frontend_vip>
mail._domainkey	mail._domainkey.test.example.com. 899 IN TXT "v=DKIM1;" "g=*;" "k=rsa;" "p=<DKIM_KEY>"
mx1	mx-test.example.com. 900 IN A ucs-mail-1.test.example.com
mx2	mx-test.example.com. 900 IN A ucs-mail-2.test.example.com
preview	preview-test.example.com. 900 IN CNAME <ucs_frontend_vip>
relay	relay-test.example.com. 900 IN A <ucs_mail_vip>
resources	resources-test.example.com. 900 IN A <ucs_frontend_vip>
secured	secured-test.example.com. 900 IN A <ucs_frontend_vip>
smtp	smtp-test.example.com IN A <ucs_mail_vip>
_adsp._domainkey	_adsp._domainkey.test.example.com. 900 IN TXT "dkim=all"
_autodiscover._tcp	_autodiscover._tcp.test.example.com. 900 IN SRV 0 0 443 <mailion_external_domain>
_caldavs._tcp	_caldavs._tcp.test.example.com. 900 IN SRV 0 1 6787 caldav-test.example.com.
_carddavs._tcp	_carddavs._tcp.test.example.com. 900 IN SRV 0 1 6787 carddav-test.example.com.
_grpcsec._tcp	_grpcsec._tcp.test.example.com. 900 IN SRV 0 0 3142 grpc-test.example.com.
_imap._tcp	_imap._tcp.test.example.com. 900 IN SRV 10 0 143 imap-test.example.com.
_imaps._tcp	_imaps._tcp.test.example.com. 900 IN SRV 0 0 993 imap-test.example.com.
_smtps._tcp	_smtps._tcp.test.example.com. 900 IN SRV 0 0 465 smtp-test.example.com.
_submission._tcp	_submission._tcp.test.example.com. 900 IN SRV 0 0 587 smtp-test.example.com.
_submissions._tcp	_submissions._tcp.test.example.com. 900 IN SRV 0 0 465 smtp-test.example.com.