



# MAILION

## Руководство по установке

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2014–2022

**ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»**

**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**

**«Mailion»**

**РУКОВОДСТВО ПО УСТАНОВКЕ**

**1.1**

На 56 листах

**Москва**

**2022**

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам. Товарные знаки «МойОфис», «MyOffice» и «Mailion» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

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

## Содержание

<b>Перечень сокращений, терминов и определений .....</b>	<b>6</b>
<b>1 Общие сведения.....</b>	<b>7</b>
1.2 Требования к квалификации персонала .....	7
1.3 Системные требования.....	8
1.3.1 Аппаратные требования.....	8
1.3.2 Программные требования.....	13
1.4 Требования по работе с DNS .....	14
1.4.1 Организация работы сервисов разрешения имен.....	14
1.4.2. Формирование внешних доменных имен инсталляций.....	15
1.4.3. Необходимые DNS-записи .....	15
1.4.3.1. Внешние DNS-записи .....	15
1.4.3.2. Внутренние DNS-записи.....	17
1.5 Ограничения.....	17
1.5.1 Ограничения при выполнении кластерной установки.....	17
1.5.2 Ограничение по работе с файлом inventory .....	18
1.5.3 Ограничение по работе с подсистемой управления конфигурациями.....	18
1.5.4 Ограничение по работе с системами виртуализации.....	18
1.5.5 Ограничение по работе с хостами MX .....	18
1.5.6 Ограничение при заполнении файлов переменных .....	18
1.6 Рекомендации.....	18
1.6.1 Рекомендации по использованию файловых систем .....	18
1.6.2 Рекомендации по разбивке дисков .....	19
<b>2 Описание системы «Mailion» .....</b>	<b>20</b>
2.1 Общая логическая схема .....	20
2.2 Детальная логическая схема .....	21
<b>3 Типовые схемы установки «Mailion» .....</b>	<b>22</b>
3.1 Конфигурация без отказоустойчивости .....	22
3.2 Кластерная отказоустойчивая конфигурация .....	22
3.3 Типовая схема масштабирования.....	22
<b>4 Первичная установка.....</b>	<b>25</b>
4.1 Состав дистрибутива .....	25
4.2 Подготовка к установке .....	25
4.2.1 Описание общих ролей подсистемы управления конфигурациями для преднастройки серверов перед установкой.....	25
4.2.2 Подготовка инфраструктуры установки .....	28
4.2.3 Настройка основных параметров установки .....	34
4.2.4 Настройка дополнительных параметров установки .....	48
4.2.5 Настройка межсетевого экранирования.....	48
4.2.6 Разграничение доступа .....	50
4.2.7 Настройка удаленного доступа .....	50
4.3 Установка «Mailion».....	50
4.3.1 Конфигурация без отказоустойчивости .....	50
4.3.2 Кластерная отказоустойчивая конфигурация.....	51
4.4 Установка в составе других продуктов «МойОфис» .....	52
4.5 Установка надстройки для Microsoft Outlook .....	52
<b>5 Обновление с предыдущих версий .....</b>	<b>53</b>
5.1 Состав дистрибутива .....	53

5.2 Подготовка к обновлению .....	53
5.2.1 Описание ролей .....	53
5.2.2 Проверка и настройка инфраструктуры установки .....	53
5.2.3 Проверка и настройка основных параметров установки.....	53
5.2.4 Проверка и настройка дополнительных параметров установки.....	53
5.2.5 Проверка и настройка межсетевого экранирования .....	53
5.2.6 Проверка и настройка разграничения доступа .....	53
5.2.7 Проверка и настройка удаленного доступа .....	53
5.2.8 Создание резервных копий.....	53
5.3 Обновление «Mailion» .....	53
5.3.1 Конфигурация без отказоустойчивости .....	53
5.3.2 Кластерная отказоустойчивая конфигурация.....	54
<b>6 Дополнительные возможности и рекомендации по установке.....</b>	<b>55</b>
6.1 Настройка мониторинга состояния.....	55
6.2 Настройка взаимодействия со службой каталогов.....	55
6.3 Настройка антивирусного программного обеспечения .....	55
<b>7 Техническая поддержка.....</b>	<b>56</b>

## Перечень сокращений, терминов и определений

Перечень терминов и определений приведен в Таблице 1.

Таблица 1 – Перечень сокращений, терминов и определений

<b>Сокращение, термин</b>	<b>Расшифровка и определение</b>
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 автоматическую 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» – расширение, которое обеспечивает работу с почтой, календарем и контактами «Mailion» в интерфейсе приложения Microsoft Outlook.

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

### 1.2 Требования к квалификации персонала

Администратор «Mailion» должен соответствовать следующим требованиям:

- 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);
- опыт работы с подсистемами виртуализации на уровне эксперта:
  - работа с подсистемой контейнерной виртуализации (**Docker**);
  - работа с одной из подсистем серверной виртуализации на базе гипервизоров

Hyper-V, VMWare vSphere ESXi, KVM;

- опыт работы с командной строкой ОС Linux: знания в объеме курсов Red Hat RH124, RH134, RH254;
- 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;
- 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);
- практический опыт администрирования на уровне эксперта:
  - **Redis;**
  - **nats;**
  - **Prometheus;**
  - **monogdb;**
  - **Arangodb;**
  - **Postfix.**
- опыт работы с подсистемой централизованного управления Ansible;
- опыт работы со стандартными офисными приложениями.

## 1.3 Системные требования

Перечень системных требований к программному и аппаратному обеспечению приведен в п. 1.3.1 и п. 1.3.2.

### 1.3.1 Аппаратные требования

Ниже представлены минимальные и рекомендованные требования.



## 1.3.1.1 Минимальные требования

Минимальные требования для установки «Mailion» на оборудовании без отказоустойчивости и отказоустойчивом оборудовании приведены в таблицах 2, 3.



Режим и последующая настройка параметров на оборудовании без поддержки отказоустойчивости предоставляется в целях демонстрации функциональности «Mailion». **Данный режим не поддерживается, не рекомендуется его использовать.**

Таблица 2 – Минимальные требования (установка без отказоустойчивости)

Имя роли сервера	VCPU	RAM, Gb	HDD, Gb (без учёта ОС)	SSD, Gb	Количество серверов	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ucs_frontend	2	2	30	2	1	12	16	–	50
ucs_mail	1	3	20	10					
ucs_apps	2	4		4					
ucs_catalog	2	2		2					
ucs_calendar	1	1		2					
ucs_balancers	1	1		0					
ucs_search	1	2		10					
ucs_converter	1	2		4					
ucs_etcd	1	1		1					
ucs_arangodb_agency	1	1		1					

ucs_mongodb	1	3		30					
ucs_arangodb	1	2		2					
dispersed_object_store	1	4		40					
ucs_mq	1	1		1					
ucs_redis_data	2	2	70						
ucs_redis_cache	2	2	50						
ucs_infrastructure	4	8		40					
				<b>ИТОГО:</b>	<b>1</b>	<b>12</b>	<b>16</b>	<b>0</b>	<b>50</b>

Таблица 3 – Минимальные требования (отказоустойчивая установка)

Имя роли сервера	VCPU	RAM Gb	HDD, Gb (без учёта ОС)	SSD, Gb	Количество серверов	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ucs_frontend	2	8	30		2	4	16	60	
ucs_mail	1	3	20	10	2	2	6	40	20
ucs_apps	3	4	4		2	16	24	120	
ucs_catalog	3	4	2						
ucs_calendar	1	3	2						
ucs_balancers	1	1	0						
ucs_search	2	13	35		2	8	34	140	
ucs_converter	2	4	5						
ucs_etcd	1	1		1	3	15	30	48	69
ucs_arangodb_agency	1	1		1					

ucs_mongodb	1	3		21					
ucs_arangodb	1	2	20		3	24	48	1773	63
dispersed_object_store	3	6	500	21					
ucs_mq	1	1	1						
ucs_redis_data	2	2	10		6				
ucs_redis_cache	2	2							
ucs_infrastructure	4	8	200		1	4	8	200	
				<b>ИТОГО:</b>	<b>21</b>	<b>73</b>	<b>166</b>	<b>2333</b>	<b>152</b>

### 1.3.1.2 Рекомендованные требования

Рекомендованные требования для установки «Mailion» на оборудовании без отказоустойчивости и отказоустойчивом оборудовании приведены в таблице 4.

Таблица 4 – Рекомендованные требования (отказоустойчивая установка)

Имя роли серверов	VCPU	RAM, Gb	HDD, Gb (без учёта ОС)	SSD, Gb	Количество серверов	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ucs_frontend	2	8	40		4	8	32	160	
ucs_mail	4	4	40	10	6	24	24	240	60
ucs_apps	8	16	20		6	96	144	480	
ucs_catalog	8	8	20						
ucs_calendar	8	16	20						

<b>ucs_balancers</b>	2	2							
<b>ucs_search</b>	8	9	18		4	48	52	232	
<b>ucs_converter</b>	4	4	40		4				
<b>ucs_etcd</b>	1	1		1	5	33	61	140	113
<b>ucs_arangodb_agency</b>	1	1		10					
<b>ucs_mongodb</b>	4	8		10					
<b>ucs_arangodb</b>	2	4	20	20	7				
<b>dispersed_object_store</b>	16	64	200	21					
<b>ucs_mq</b>	2	2	1		9				
<b>ucs_redis_data</b>	2	2	70						
<b>ucs_redis_cache</b>	2	2	50						
<b>ucs_infrastructure</b>	4	8	200		1	4	8	200	
				<b>ИТОГО:</b>	<b>59</b>	<b>325</b>	<b>769</b>	<b>2852</b>	<b>320</b>

## 1.3.2 Программные требования

Требования к программному обеспечению для места оператора, на котором производится установка, приведены в таблицах 5, 6.

Таблица 5 – Требования к программному обеспечению для места оператора

Требование	Описания	
Поддерживаемые браузеры	Chrome	не ниже версии 61
	Microsoft Edge	не ниже версии 38
	Mozilla Firefox	не ниже версии 56
	Apple Safari	не ниже версии 11
	Яндекс-браузер	не ниже версии 17.9.1.768
Python	v. 3.6+	
Модули Python	jmespath	
	jinja2	не ниже версии v.2.10 (обновление для CentOS можно выполнить с любого репозитория OpenStack: <a href="http://mirror.centos.org/centos/7/cloud/x86_64/openstack-train/">http://mirror.centos.org/centos/7/cloud/x86_64/openstack-train/</a> или <a href="https://mirror.yandex.ru/centos/7/cloud/x86_64/openstack-train/">https://mirror.yandex.ru/centos/7/cloud/x86_64/openstack-train/</a> )
	ansible	2.11 или новее, но до 2.12
	python-netaddr	python3-netaddr
	dnspython	

Таблица 6 – Требования к программному обеспечению для серверов, на которые производится установка<sup>1</sup>

Требование	Описание
ОС	<ul style="list-style-type: none"> <li>• CentOS 7.7+;</li> <li>• Ubuntu 20.04;</li> <li>• Альт Линукс 10;</li> <li>• Astra Linux Special Editor 1.7 Орёл (Уровень защищенности – Базовый);</li> <li>• Astra Linux Special Editor 1.7 Воронеж (Уровень защищенности – Усиленный);</li> <li>• Astra Linux Special Editor 1.7 Смоленск (Уровень защищенности – Максимальный);</li> <li>• Astra Linux Common Editor 2.12.43;</li> <li>• РЕД ОС 7.3 Муром (версия ФСТЭК)</li> </ul>
Стандартные репозитории ОС	Подключение всех стандартных репозиторий 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 репозиторий <b>elrepo</b> ( <a href="http://elrepo.org">http://elrepo.org</a> ) и <b>docker-ce</b> ( <a href="https://download.docker.com/linux/centos/docker-ce.repo">https://download.docker.com/linux/centos/docker-ce.repo</a> ) для установки соответствующих пакетов ядра Linux и ПО <b>docker</b> , не входящих в состав поставки для установок в закрытом контуре
Доступ	Для каждого сервера, на котором выполняется установка, должен быть обеспечен SSH-доступ: <ul style="list-style-type: none"> <li>• с sudo привилегиями (ALL=(ALL) NOPASSWD: ALL);</li> <li>• без пароля (доступ по ключу)</li> </ul>

## 1.4 Требования по работе с DNS

### 1.4.1 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 сервера будут перенастроены на работу через **unbound** и не будут принимать параметры серверов разрешения имен по **DNCP**. Поэтому важно направить **unbound** на внутренние DNS-сервера

<sup>1</sup> В таблице описана минимальная настройка.

компании, если такая необходимость есть. По умолчанию **unbound** настроен на проброс запросов на адреса 8.8.8.8 и 1.1.1.1.

## 1.4.2. 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 7.

Таблица 7 – Примеры работы шаблона

<b>mailion_domain_module</b>	<b>Имя ссылки</b>	<b>mailion_external_domain</b>	<b>Результат</b>
{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-xy-1.test.example.com

Таким образом, можно гибко настраивать принцип формирования доменных имен инсталляции. Это может пригодиться, например, если имеется wild-card сертификат SSL 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 wild-card сертификат SSL.

## 1.4.3. Необходимые DNS-записи

### 1.4.3.1. Внешние DNS-записи

В таблицах 8, 9 приведены все необходимые внешние DNS-записи, требуемые для инсталляции. Данная таблица сформирована для **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 8 – Сведения про необходимые для инсталляции внешние DNS-записи

<b>Имя записи</b>	<b>Тип записи</b>	<b>Значение</b>	<b>Комментарии</b>

Имя записи	Тип записи	Значение	Комментарии
api	CNAME	@	
auth	CNAME	@	
autoconfig	CNAME	@	
avatars	CNAME	@	
caldav	CNAME	@	
carddav	CNAME	@	
@	A	<ucs_frontend_vip>	Значение должно быть равно VIP-адресу между серверами с ролью <b>ucs_frontend</b> 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 <b>mailion_external_domain</b>
@	MX	10 <mx1>	MX-запись указывает на A-запись в которой содержится адрес первого сервера из группы <b>ucs_mail</b>
@	MX	10 <mx2>	MX-запись указывает на A-запись в которой содержится адрес второго сервера из группы <b>ucs_mail</b> (и т.д.)
grpc	CNAME	@	
imap	CNAME	@	
mail	CNAME	@	
mail._domainkey	TXT	"v=DKIM1; k=rsa; p=<DKIM_KEY>"	Значение <b>DKIM_KEY</b> определяется на этапе установки в параграфе 4.2.2.3, п.9
mx1	A	<ucs_mail_mx[0]>	Внешний IP-адрес, по которому доступен первый сервер из группы <b>ucs_mail</b>
mx2	A	<ucs_mail_mx[1]>	Внешний IP-адрес, по которому доступен второй сервер из группы <b>ucs_mail</b> (и т.д.)
preview	CNAME	@	
relay	A	<ucs_mail_relay_vip>	Значение должно быть равно VIP-адресу между серверами с ролью <b>ucs_mail</b> или адресу самого сервера этой группы, если производится установка без отказоустойчивости
secured	CNAME	@	
smtp	CNAME	@	
_adsp._domainkey	TXT	"dkim=all"	

Таблица 9 – Сведения про необходимые для инсталляции внешние DNS-записи

Имя записи	Тип	Приоритет	Вес	Порт	Адрес
_autodiscover._tcp	SRV	0	0	443	<mailion_external_domain>.



Имя записи	Тип	Приоритет	Вес	Порт	Адрес
_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	imaps.<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>.

### 1.4.3.2. 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 “А”-записи для каждого сервера, вписанного в файл **inventory**, а так же CNAME адреса на все поддомены (“\*”) к каждому серверу, вписанному в **inventory**.

Пример заполнения таких записей приведен в Таблице 10.

Таблица 10 – 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” **unbound** будет установлен, но не будет принимать участия в работе «Mailion».

## 1.5 Ограничения

### 1.5.1 Ограничения при выполнении кластерной установки

Не рекомендуется совмещать серверные роли при установке. При совмещении серверных ролей необходимо учитывать следующие рекомендации:

- не совмещать роль **ucs\_infra**, роль **dispersed\_object\_store**, роль **ucs\_search** с какой-либо другой ролью;
- не совмещать роли **ucs\_arangodb**, **ucs\_mongodb**, **ucs\_etcd**, **ucs\_redis\_cache**, **ucs\_redis\_data** с ролями **ucs\_apps**, **ucs\_mail**, **ucs\_converter**, **ucs\_catalog**.

## 1.5.2 Ограничение по работе с файлом inventory

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

## 1.5.3 Ограничение по работе с подсистемой управления конфигурациями

В подсистеме управления конфигурациями не должно быть 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](https://docs.ansible.com/ansible/latest/reference_appendices/config.html#the-configuration-file).

Важно самостоятельно установить необходимые модули python из пункта 1.3.2, так как они не являются частью поставки системы.

## 1.5.4 Ограничение по работе с системами виртуализации

Следующие системы виртуализации поддерживаются для обеспечения работы «Mailion»:

- VMWare;
- KVM.

## 1.5.5 Ограничение по работе с хостами MX

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

## 1.5.6 Ограничение при заполнении файлов переменных

При заполнении инвентарного файла имя **tier** (Section 2) должно всегда начинаться с "ucs\_".

## 1.6 Рекомендации

### 1.6.1 Рекомендации по использованию файловых систем

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

## 1.6.2 Рекомендации по разбивке дисков

Требуется учитывать следующее:

- все рекомендуемые аппаратные требования указаны в разделе 1.3.1, 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. Так же в этот раздел могут быть направлены копии журналов работы компонентов, при соответствующей настройке лог-коллектора, что потребует дополнительного дискового пространства;
- для сервера роли **ucs\_dos** рекомендуется выделять независимые диски HDD для серверной части и диски SSD под метаданные. К примеру:
  - /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;
- избыточность данных (**data segments + parity segments**):
  - не менее 2 + 1;
  - сумма **data segments + parity segments** не должна превышать количества независимых дисков в серверной части хранилища;
  - для кластера из трех машин минимально допустимые значения – 2 + 1. Независимых дисков в случае кластера должно быть не меньше, чем определенное количество.

## 2 Описание системы «Mailion»

### 2.1 Общая логическая схема

Общая логическая схема «Mailion» приведена на Рисунке 1.



Рисунок 1 – Общая логическая схема «Mailion»

## 2.2 Детальная логическая схема

Детальная логическая схема приведена на Рисунке 2.

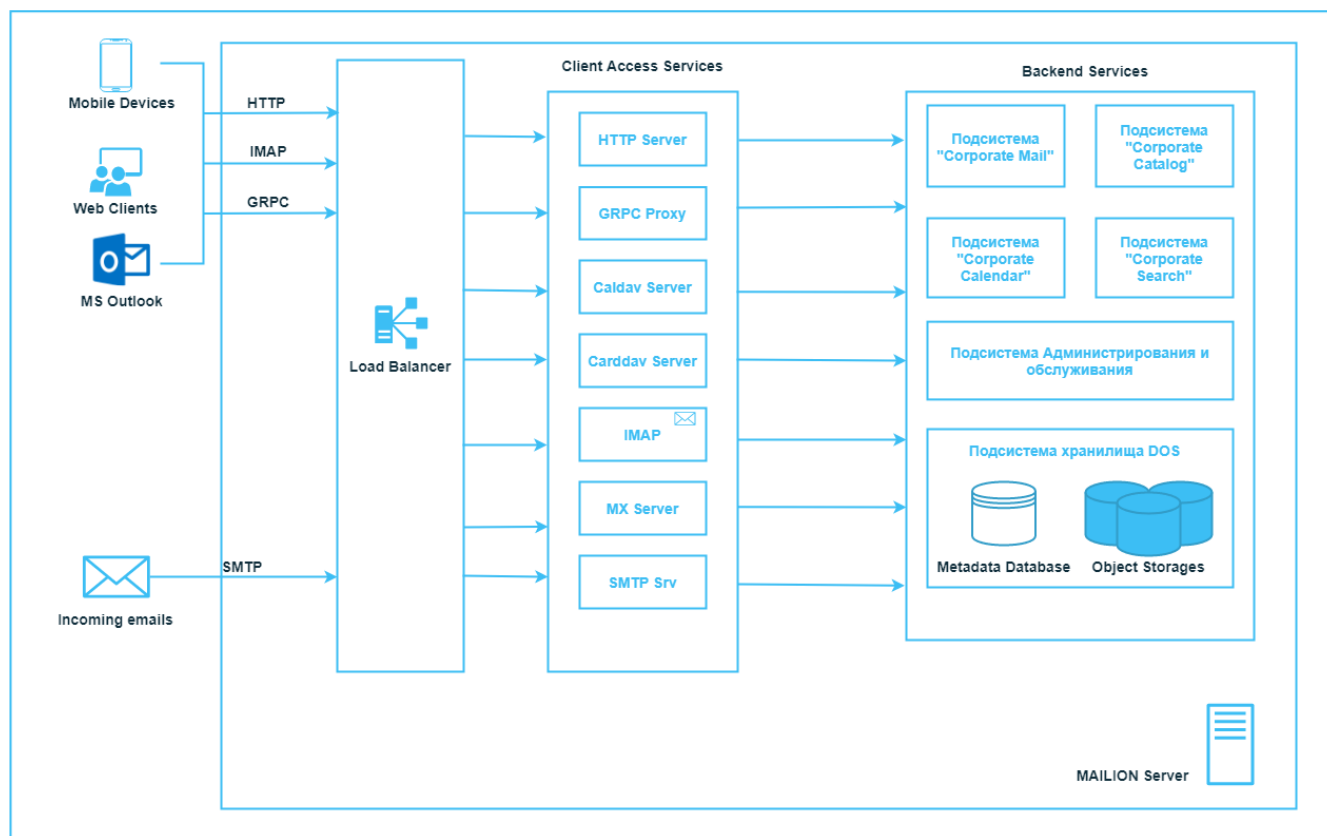


Рисунок 2 – Детальная логическая схема «Mailion»

## 3 Типовые схемы установки «Mailion»

### 3.1 Конфигурация без отказоустойчивости

См. раздел 1.3.

### 3.2 Кластерная отказоустойчивая конфигурация

См. раздел 1.3.

### 3.3 Типовая схема масштабирования

Стандартные варианты масштабирования приведены в п. 1.3.1.

Рекомендованные требования для отказоустойчивого оборудования из расчёта на 1000 и 200 000 пользователей приведены в таблицах 11, 12.

Таблица 11 – Рекомендованные требования (1000 пользователей)

Имя роли серверов	VCPU	RAM, Gb	HDD, Gb (без учёта ОС)	SSD, Gb	Количество серверов	на каждую роль			
						VCPU	RAM, Gb	HDD, Gb	SSD, Gb
<b>ucs_frontend</b>	2	8	30		2	4	16	60	
<b>ucs_mail</b>	1	3	20	10	2	2	6	40	20
<b>ucs_apps</b>	3	4	10		2	16	24	120	
<b>ucs_catalog</b>	3	4	10						
<b>ucs_calendar</b>	1	3	10						
<b>ucs_balancers</b>	1	1	30						
<b>ucs_search</b>	2	31	105 <sup>2</sup>		2	8	70	280	
<b>ucs_converter</b>	2	4	35						

<sup>2</sup> Данные требуют резервирования на уровне RAID-массива на каждой ноде.

Имя роли серверов	VCPU	RAM, Gb	HDD, Gb (без учёта ОС)	SSD, Gb	Количество серверов				
						на каждую роль	итого на группу		
ucs_etcd	1	1		1	3	15	30	0	189
ucs_arangodb_agency	1	1		1					
ucs_mongodb	3	8		61 <sup>3</sup>					
ucs_arangodb	2	4	20		3	24	48	4773	186
dispersed_object_store	3	6	1500 <sup>4</sup>	62 <sup>5</sup>					
ucs_mq	1	2	1						
ucs_redis_data	2	4	70		6				
ucs_redis_cache	2	2	50						
ucs_infrastructure	4	8	200		1	4	8	200	
				<b>ИТОГО:</b>	<b>21</b>	<b>73</b>	<b>202</b>	<b>5473</b>	<b>395</b>

Таблица 12 – Рекомендованные требования (200 000 пользователей)

Имя роли серверов	VCPU	RAM, Gb	HDD, Gb (без учёта ОС)	SSD, Gb	Количество серверов				
						на каждую роль	итого на группу		
ucs_frontend	2	8	40		4	8	32	160	
ucs_mail	4	4	40	10	6	24	24	240	60
ucs_apps	8	16	40		6	96	144	480	
ucs_calendar	8	16	40						

<sup>3</sup> Фактор репликации 3

<sup>4</sup> Фактор репликации 3, d+p =3. Основные данные на HDD не требуют резервирования на уровне RAID-массива на каждой ноде.

<sup>5</sup> Метаданные на SSD требуют резервирования на уровне RAID-массива на каждой ноде.

Имя роли серверов	VCPU	RAM, Gb	HDD, Gb (без учёта ОС)	SSD, Gb	Количество серверов	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ucs_balancers	2	2							
ucs_catalog	8	8	40		6				
ucs_search	8	56	205 <sup>6</sup>		12	112	688	2620	
ucs_converter	4	4	40		4				
ucs_etcd	1	1		10	5	33	61	140	2185
ucs_mq5	1	2							
ucs_mongodb	4	8	20	305	7				
ucs_arangodb	2	4	50	20					
ucs_arangodb_agency	1	1		10					
ucs_redis_cache	4	2			9				
ucs_redis_persist	2	2							
dispersed_object_store	16	64	7000	720 <sup>7</sup>	7	112	448	49000	5040
ucs_infrastructure	4	8	200		1	4	8	200	
				<b>ИТОГО:</b>	68	391	1407	52860	7285

Характеристики дисков приведены в таблице 13.

Таблица 13 – 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

<sup>6</sup> Данные требуют резервирования на уровне RAID массива на каждой ноде.

<sup>7</sup> Фактор репликации 3, d+p =7. Основные данные на HDD не требуют резервирования на уровне RAID-массива на каждой ноде. Метаданные на SSD требуют резервирования на уровне RAID-массива на каждой ноде.



## 4 Первичная установка

### 4.1 Состав дистрибутива

В состав дистрибутива входит ПО «Mailion»:

1. Установщик места оператора (**ansible\_bin**).
2. Установщик окружения для проведения установки, включающий все необходимые образы и пакеты (**infra\_bin**).
3. Файлы tpl (Third-party license).

### 4.2 Подготовка к установке

#### 4.2.1 Описание общих ролей подсистемы управления конфигурациями для преднастройки серверов перед установкой

Данные роли описаны в таблице 14.

Таблица 14 – Описание общих ролей **ansible** для преднастройки серверов перед установкой

Наименование роли	Описание
<b>authorized_keys</b>	Добавляет указанные ssh-ключи для выбранных пользователей на сервера группы <b>play_hosts</b>
<b>hostname</b>	Устанавливает <b>hostname</b> для выбранных серверов
<b>SELinux</b>	Проверяет режим работы <b>SELinux</b> и переключает его в режим "enforcing" <sup>8</sup>
<b>packagemanager</b>	Настраивает пакетный менеджер
<b>locale</b>	Устанавливает параметры <b>locale</b> на серверах
<b>timezone</b>	Устанавливает часовой пояс на серверах
<b>sshd</b>	Производит настройку службы удаленного доступа <b>sshd</b>
<b>chrony</b>	Устанавливает и настраивает службу синхронизации времени <b>chronyd</b> <sup>9</sup>
<b>timesyncd</b>	Устанавливает и настраивает службу синхронизации времени <b>timesyncd</b> <sup>10</sup>
<b>sysctl</b>	Устанавливает требуемые параметры ядра на серверах
<b>limits</b>	Настраивает параметры ограничений на серверах
<b>kernel_ml</b>	Устанавливает пакет <b>kernel_ml</b> последнего доступного ядра <sup>11</sup>
<b>kernel_ml_deb</b>	Устанавливает пакет <b>kernel_ml</b> последнего доступного ядра для ubuntu
<b>rsyslog</b>	Устанавливает и настраивает сервис сбора журналов
<b>docker</b>	Устанавливает и настраивает <b>Docker</b> , подключает к <b>docker registry</b>
<b>unbound</b>	Устанавливает и настраивает кэширующий DNS-сервер

<sup>8</sup> Только для дистрибутивов с пакетным менеджером **yum**.

<sup>9</sup> Только для RH-based ОС.

<sup>10</sup> Только для ОС Astra Linux.

Наименование роли	Описание
<b>iptables</b>	Устанавливает и настраивает службы межсетевого экрана с параметрами, требуемыми для конкретной роли
<b>resolv</b>	Производит настройку файла <b>resolv.conf</b>
<b>package_tools</b>	Добавляет требуемые пакеты для работы «Mailion» в целевую ОС

Роли, используемые для подготовки «Mailion» описаны далее в таблице 15.

Таблица 15 – Описание ролей, используемых при подготовке «Mailion»

Наименование роли	Описание
<b>keepalived</b>	Устанавливает и запускает службу, реализующую протокол VRRP
<b>cAdvisor</b>	Устанавливает сервис <b>cAdvisor</b> , осуществляющий сбор метрик работы контейнеров
<b>node_exporter</b>	Устанавливает сервис <b>node_exporter</b> , осуществляющий сбор метрик работы сервера
<b>node_cert_exporter</b>	Мониторинг срока действия сертификатов
<b>node_filestat_exporter</b>	Мониторинг появления дампов памяти
<b>blackbox_exporter</b>	Мониторинг доступности веб-интерфейса
<b>syslog_ng</b>	Устанавливает сервис централизованного сбора журналов работы системы
<b>logrotate</b>	Настраивает ротацию хранимых журналов работы системы
<b>ca</b>	Устанавливает и настраивает сервис внутреннего центра сертификации
<b>alertmanager</b>	Устанавливает и настраивает сервис оповещений о событиях мониторинга
<b>devkalion</b>	Устанавливает и настраивает сервис автообнаружения сервисов инсталляции для мониторинга
<b>gesiona</b>	Устанавливает и настраивает сервис, экспортирующий список сервисов инсталляции для сервиса мониторинга
<b>prometheus</b>	Устанавливает и настраивает сервис мониторинга
<b>grafana</b>	Устанавливает и настраивает сервис отображения данных мониторинга инсталляции
<b>kunkka</b>	Устанавливает и настраивает сервис отображения данных о запущенных контейнерах на каждом сервере и их конфигурационных файлов
<b>plugin_certificate</b>	Роль, выписывающая сертификат для сборки клиентских приложений <b>outlook plugin</b>
<b>etcd</b>	Устанавливает базу данных <b>etcd</b>
<b>hydra</b>	Устанавливает и настраивает сервис обнаружения и балансировки нагрузки gRPC
<b>nats</b>	Устанавливает и настраивает <b>nats</b>
<b>nats_exporter</b>	Сбор метрик мониторинга с <b>nats</b>
<b>mongodb</b>	Устанавливает и настраивает документоориентированную СУБД
<b>mongodb.mailion_migration</b>	Устанавливает миграции данных сервисов в базах <b>mongodb</b>
<b>mongodb_exporter</b>	Сбор метрик мониторинга с <b>mongodb</b>
<b>dorofej</b>	Роль работы с модулем <b>ansible</b> , реализующим первичную миграцию СУБД

Наименование роли	Описание
<b>arangodb</b>	Устанавливает и настраивает гибридную, документо+графориентированную базу данных
<b>arangodb.migration</b>	Устанавливает миграции данных сервисов в базах <b>arangodb</b>
<b>redis</b>	Устанавливает и настраивает кластер хранилищ <b>Redis</b>
<b>theseus</b>	Устанавливает и настраивает сервис работы с учетными данными
<b>perseus</b>	Устанавливает и настраивает сервис хранения контактов
<b>erakles</b>	Устанавливает и настраивает сервис работы со сущностями
<b>odusseus</b>	Устанавливает и настраивает сервис работы с регионами
<b>talaos</b>	Устанавливает и настраивает сервис работы с тенантами
<b>daidal</b>	Устанавливает и настраивает сервис работы с доменами
<b>minos</b>	Устанавливает и настраивает сервис работы с сессиями
<b>ektor</b>	Устанавливает и настраивает сервис работы со связями, сущностями
<b>pasifae</b>	Устанавливает и настраивает сервис подсказок при поиске
<b>dispersed_object_store</b>	Устанавливает и настраивает объектное хранилище, предоставляющее gRPC-интерфейс для хранения бинарных данных и метаданных
<b>achill</b>	Устанавливает и настраивает сервис работы с аватарками
<b>jod</b>	Устанавливает и настраивает сервис для конвертации документов
<b>pregen</b>	Устанавливает и настраивает сервис для конвертации документов
<b>cvm</b>	Устанавливает и настраивает сервис для конвертации документов
<b>cu</b>	Устанавливает и настраивает сервис для конвертации документов
<b>sdd</b>	Устанавливает и настраивает сервис для конвертации документов
<b>meepo</b>	Устанавливает и настраивает сервис генерации превью
<b>mailbek</b>	Устанавливает и настраивает сервис проксирования запросов к шардированным данным на экземплярах поисковой системы
<b>dirbek</b>	Сервис поиска по каталогу
<b>helpbek</b>	Устанавливает и настраивает поисковый сервис по имеющейся веб-документации инсталляции
<b>clamav</b>	Устанавливает и настраивает антивирус для проверки писем
<b>rspamd</b>	Устанавливает и настраивает сервис антиспама
<b>zeus</b>	Устанавливает и настраивает сервис, отвечающий за шаблонизацию и настройку работы с письмами
<b>paranoid</b>	Устанавливает и настраивает сервис, реализующий протоколы <b>Postfix Policy Delegation</b> и <b>Nging HTTP Auth</b>
<b>woof</b>	Устанавливает и настраивает сервис, реализующий метод <b>search</b> протокола LDAP для резолвинга групповых адресов, алиасов, получения списка доменов со стороны <b>postfix</b>
<b>ariadne</b>	Сервис аутентификации для МТА
<b>lmtpt</b>	Устанавливает и настраивает сервис, реализующий протокол <b>lmtpt</b>
<b>postfix</b>	Устанавливает роль для развертывания почтового сервера (МТА)
<b>nginx</b>	Устанавливает и настраивает сервер <b>nginx</b> в режиме <b>smtp</b>
<b>kongur</b>	Устанавливает и настраивает сервис, отвечающий за работу календарных событий
<b>kex</b>	Устанавливает и настраивает сервис проксирования запросов к внешним

Наименование роли	Описание
	календарям
<b>thoth</b>	Устанавливает и настраивает сервис сохранения полей
<b>othrys</b>	Устанавливает и настраивает взаимодействия с внешними календарными серверами
<b>elysion</b>	Устанавливает и настраивает сервис выполнения асинхронных работ в календаре
<b>mosquito</b>	Устанавливает и настраивает сервис, предоставляющий абстракцию pub/sub над <b>AMQP</b>
<b>viper</b>	Устанавливает и настраивает сервис для сохранения писем в системе
<b>razor</b>	Устанавливает и настраивает сервис для отправки писем по шаблону с локализацией
<b>weaver</b>	Устанавливает и настраивает сервис для построения всего сообщения (его web-представления) или его части (для <b>IMAP</b> )
<b>marker</b>	Устанавливает и настраивает сервис, для управления тегами пользователя
<b>hog</b>	Устанавливает и настраивает сервис для получения и сохранения настроек пользователей
<b>beef</b>	Устанавливает и настраивает сервис для сохранения и получения метаданных писем.
<b>mixer</b>	Устанавливает и настраивает сервис для получения объектов веб-интерфейсом
<b>atlas</b>	Устанавливает и настраивает сервис для отправки почтовых сообщений
<b>kronos</b>	Устанавливает и настраивает сервис, предназначенный для регистрации задач на отложенное исполнение операций
<b>clotho</b>	Устанавливает и настраивает сервис для хранения истории изменений объектов и тегов
<b>orpheus</b>	Устанавливает и настраивает сервис проксирования аутентификации и поиска сущностей
<b>iason</b>	Устанавливает и настраивает сервис контроля за регистрацией внешних пользователей
<b>cleanup</b>	Производит полное удаление выбранных компонентов (при необходимости)
<b>imap</b>	Устанавливает и настраивает сервис, реализующий протокол <b>IMAP</b>
<b>cox</b>	Устанавливает и настраивает <b>proxy gRPC</b> сервис
<b>house</b>	Устанавливает и настраивает веб-сервер
<b>ararat</b>	Устанавливает и настраивает сервис для работы десктопных и мобильных клиентов с календарем по протоколу CalDAV/CardDAV
<b>leda</b>	Устанавливает и настраивает ldap-прокси сервер
<b>sophokles</b>	Устанавливает и настраивает сервис авторизации
<b>dafnis</b>	Устанавливает и настраивает сервис квот
<b>iolaos</b>	Устанавливает и настраивает сервис создания динамических групп
<b>homeros</b>	Устанавливает и настраивает сервис аудита действий пользователя.
<b>adonis</b>	Устанавливает и настраивает сервис для административных функций ministerium
<b>arangodb.backup</b>	Настройка автоматического бекапа <b>arangodb</b> .

Наименование роли	Описание
<b>etcd.etcd_backup</b>	Настройка автоматических бекапов для <b>etcd</b>
<b>mongodb.mongodb_backup</b>	Настройка автоматических бекапов для <b>mongodb</b>
<b>sreindexer</b>	Настройка инструмента для переиндексации поиска
<b>nats.nats_backup</b>	Настройка автоматического бекапа <b>nats</b>

## 4.2.2 Подготовка инфраструктуры установки

Для подготовки инфраструктуры установки должны быть проведены следующие действия:

1. Установка хранилища образов **Docker (docker\_registry)**.
2. Установка подсистемы управления конфигурациями (**Ansible**).

Подробная информация о выполнении данных действий приведена в пп. 4.2.2.1 и пп. 4.2.2.2.

### 4.2.2.1 Установка хранилища образов Docker (docker\_registry)

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

Этапы установки:

1. Скопировать файл `ucs_infra_[RELEASE]11.run` на сервер.
2. Запустить скрипт установки: `bash ucs_infra_[RELEASE]13.run`.
3. Согласиться на продолжение установки, нажать на клавишу "Y".

Администратору отобразится:

```

Welcome to Mailion Infrastructure Installer
This script is meant to be used on Infrastructure Server (see manual for default)

Do you want to continue? [y/N] y
Make sure that the operating system is compatible [ OK ]
Ensure that yum-utils is installed [CHANGE]
Ensure that docker-ce repository is available [CHANGE]
Ensure that docker is installed [CHANGE]
Ensure that jq package is installed [ OK ]
Install nct-ministerium [ OK ]
Install ucs-colorize [CHANGE]
Ensure that docker dir exists [CHANGE]
Ensure that docker daemon config exists [ OK ]
Check if docker daemon needs to be restarted [CHANGE]
    
```

<sup>11</sup> [RELEASE] – Имя релиза.

Ensure that docker is started	[ OK ]
Ensure that docker is enabled	[CHANGE]
Check if docker is available	[ OK ]
Ensure that registry image is available	[CHANGE]
Check if container with registry is available	[CHANGE]
Ensure that registry configuration directory exists	[ OK ]
Ensure that docker-registry anv file exists	[CHANGE]
Check if old registry data directory exists	[ OK ]
Ensure that registry data directory exists	[ OK ]
Ensure that container with registry is available	[ OK ]
Wait for docker-registry to start	[ OK ]
Ensure that docker-registry is running	[ OK ]
Extracting registry archive...	
Check if the script is run with superuser privileges	
Remove dangling and outdated images	

После этого установка хранилища образов **Docker (docker\_registry)** будет завершена.

#### 4.2.2.2 Установка подсистемы управления конфигурациями (Ansible)

Установка производится на рабочем месте оператора. Перед началом установки проверить, что:

- вход выполнен под пользователем **root** или под пользователем **sudo** с привилегиями **yum (dnf<sup>12</sup>)**;
- машина, на которой выполняется установка, соответствует требованиям, указанным в п. 1.3;
- с выбранного сервера есть возможность доступа по SSH до других серверов, на которых выполняется установка;
- подсистема управления конфигурациями **Ansible** установлена, другие конфигурационные файлы **Ansible** не присутствуют в системе;
- необходимые модули установлены в системе, их версии соответствуют требованиям.

Этапы установки:

1. Скопировать файл `ucs_ansible_bin_[RELEASE].run` (где RELEASE – имя релиза) в домашнюю директорию пользователя.
2. Запустить скрипт установки: `bash ucs_ansible_bin_[RELEASE].run`, где RELEASE – имя релиза.

---

<sup>12</sup> При использовании других ОС, не CentOS.

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

Администратору отобразится:

```
Welcome to Mailion Ansible Installer version 2022.01
This script is meant to be used on operator workstation

Do you want to continue? [y/N] y
Ensure that python-netaddr is installed [CHANGE]
Ensure that python2-jmespath is installed [CHANGE]
Install nct-dorofej [ OK ]
Install nct-ministerium [ OK ]
Ensure that version directory is present [CHANGE]
Ensure that version 2022.01 is present [ OK ]
Set 2022.01 as latest [ OK ]
Create roles symlink [ OK ]
Create contrib symlink [ OK ]
Create playbooks symlink [ OK ]
Create group_vars directory [ OK ]
Create group_vars/all symlink [ OK ]
Create host_vars directory [ OK ]
Create certificates directory [ OK ]
Install ucs-storm
Create certificates symlink
```

После этого установка подсистемы управления конфигурациями будет завершена.

#### 4.2.2.3 Установка «Mailion» с машины оператора

В инсталляторе представлены предзаполненные файлы конфигураций, которые призваны помочь в настройке необходимого функционала будущей системы. В ДУ в папке **contrib** находятся различные варианты возможной установки: кластерная конфигурация, Standalone и распределенная конфигурация Standalone.

Так как целевое назначение системы – крупная отказоустойчивая инсталляция, в данном документе будет описан только кластерный вариант.

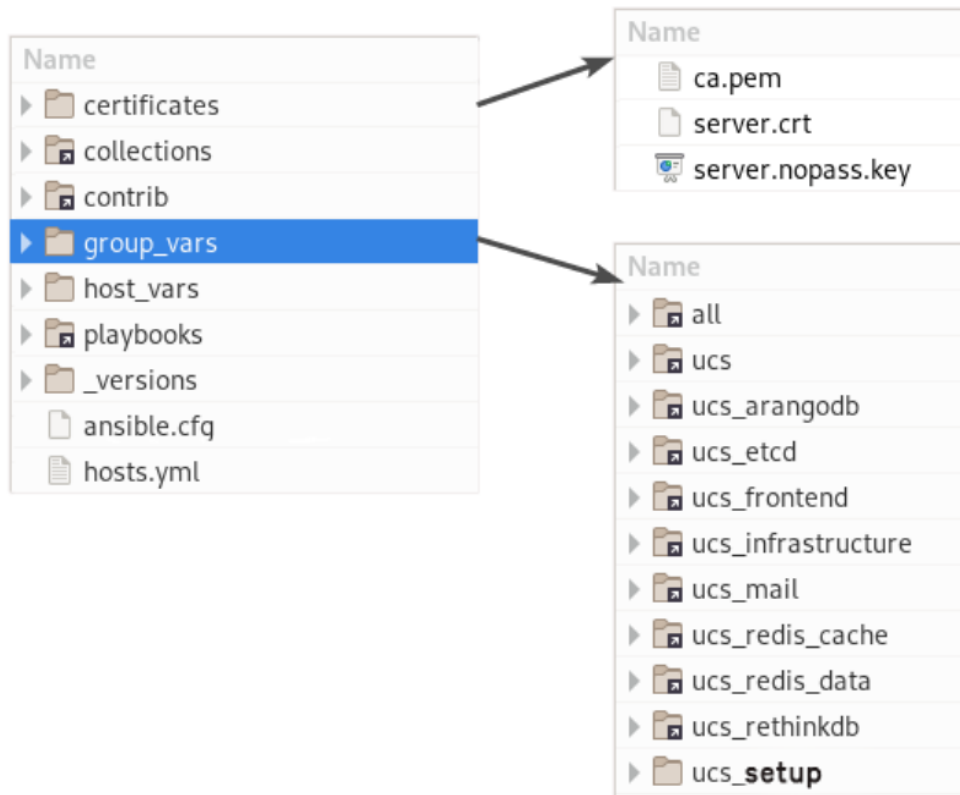


Рисунок 3 – Структура папок

Этапы установки:

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

```
[root@ucs-installer ~]# cd ~/install_mailion
```

2. Скопировать файл **contrib/mailion/ansible.cfg** в корневой раздел <ДУ> с помощью команды:

```
[root@ucs-installer ~]# cp contrib/mailion/ansible.cfg .  
[root@ucs-installer ~]#
```

3. Подготовить файл **inventory**. Примеры заполненных файлов можно найти в каталоге `~/contrib/ucs/`. Скопировать необходимый файл следующей командой:

```
[root@ucs-installer ~]# cp contrib/mailion/cluster/hosts.yml hosts.yml
```

4. Заполнить файл **inventory**.
5. Заменить имя группы **ucs\_setup** на имя текущей инсталляции.



6. Скопировать ssl-ключи для внешнего домена в каталог **certificates**. Подробнее про размещение ключей можно прочитать в пп. 4.2.2.3.1.
7. Создать в папке групповых переменных (**group\_vars**) каталог для серверов с именем группы инсталляции из секции 3 файла **inventory** (по умолчанию – **ucs\_setup**).
8. Скопировать в папку групповых переменных (**group\_vars**) каталог с переменными для заполнения:

```
[root@ucs-installer ~]# cp -r contrib/mailion/cluster/group_vars/ucs_setup/* group_vars/ucs_setup
```

9. Открыть файл **main.yml** из каталога размещения.
10. Отредактировать значение параметров по комментариям. Примеры параметров для минимальной настройки можно найти в пп. 4.2.3.1.
11. Открыть файл **ministerium.yml** из каталога размещения.
12. Отредактировать значение параметров по комментариям. Примеры заполнения параметров можно найти в пп. 4.2.3.

#### 4.2.2.3.1 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**, который был скопирован на шаге 7 в п. 4.2.2.3, заполнены имена сертификатов по умолчанию. Если назвать файлы сертификатов соответственно, то менять имена в переменных не нужно. В документации далее используются примеры именно таких имен.

Порядок размещения сертификатов<sup>13</sup>:

1. Разместить сертификат внешнего домена:

```
[root@ucs-installer ~]# vim certificates/server.crt
```

2. Разместить ключ внешнего домена:

```
[root@ucs-installer ~]# vim certificates/server.nopass.key
```

---

<sup>13</sup> В примере показан порядок размещения сертификатов с использованием редактора vim, разместить сертификаты можно без его использования.

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

```
[root@ucs-installer ~]# vim certificates/ca.pem
```

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

```
[root@ucs-installer ~]# cat certificates/server.crt
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
[root@ucs-installer ~]#
```

Имена ключей в 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"
```

## 4.2.3 Настройка основных параметров установки

### 4.2.3.1 Минимальные параметры установки

Минимальные параметры, обязательные для заполнения:

- **ansible\_user;**
- **arangodb\_bearer\_token;**
- **arangodb\_users;**
- **codec\_secret\_key;**
- **dispersed\_object\_store\_management\_token;**
- **grafana\_admin\_password;**
- **hydra\_get\_service\_list\_token;**
- **jwt\_key;**
- **keepalived;**
- **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\_tenants**
- **mongodb\_root\_password;**
- **mongodb\_secured\_key;**
- **mongodb\_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\_minos\_password;**
- **redis\_rspamd\_password;**
- **redis\_sdd\_password;**
- **redis\_viper\_password;**
- **rspamd\_clamav\_enabled;**
- **clamav\_database\_mirror;**
- **rspamd\_kse\_endpoints;**
- **rspamd\_dkim\_hosts;**
- **rspamd\_web\_password;**
- **servus;**
- **setup;**
- **sophokles\_access\_token;**
- **theseus\_cipher\_key;**

- **unbound\_forward\_address.**

Структура, а также способы заполнения указанных параметров, приведены в таблицах ниже.

#### 4.2.3.1.1 Настройка параметров установки **ansible\_user**

Настройка параметров приведена в Таблице 16.

Таблица 16 – Настройка параметров **ansible\_user**

Параметр	Тип данных	Описание
<b>ansible_user:</b>	Str	Имя пользователя, под которым установщику будут доступны сервера инсталляции по <b>ssh</b>

Пример корректно настроенного параметра:

```
ansible_user: "root"
```

#### 4.2.3.1.2 Настройка параметров установки **arangodb**

Настройка параметров приведена в Таблице 17.

Таблица 17 – Настройка параметров **arangodb**

Параметр	Тип	Описание
arangodb_bearer_token:	Str	Токен авторизации по http для сбора метрик сервисом мониторинга
arangodb_users:		Словарь пользователей СУБД
ektor:		Имя пользователя одноименного сервиса <sup>14</sup>
password:	Str	Пароль пользователя одноименного сервиса
root:		Имя суперпользователя СУБД <sup>12</sup>
password:	Str	Пароль суперпользователя СУБД

Пример корректно настроенного параметра:

```
arangodb_bearer_token:
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJhcmFuZ29kYiIsInNlcnZlcCI6ImZvbyJ9.Vra2xX
Wl2-XS9leYTYgosSLXiswSfPa8SCLN8C1VVR8"
arangodb_users:
ektor:
# Generate the password with: pwgen 20 1
```

<sup>14</sup> Не изменяется.

```
password: "oikahy2dah4aHah3quia"
sophokles:
# Generate the password with: pwgen 20 1
password: "quuuphoh6Yoomae2Ieso"
euripides:
# Generate the password with: pwgen 20 1
password: "we0quee4vaesiex8liJa"
root:
# Generate the password with: pwgen 20 1
password: "jeibash6jaes0Inoo7ka"
```

#### 4.2.3.1.4 Настройка параметров `codec_secret_key`

Настройка параметров приведена в таблице 18.

Таблица 18 – Настройка параметров `codec_secret_key`

Параметр	Тип	Описание
<code>codec_secret_key:</code>		Словарь параметров секретов для формирования зашифрованной ссылки
<code>rcr:</code>	Str	Используется для формирования ссылки на проксирование данных внутри системы
<code>secret_link:</code>	Str	Используется для формирования ссылки на проксируемые ресурсы
<code>values_codec</code>	Str	Значение

Пример корректно настроенного параметра:

```
codec_secret_key:
rcr: "O1Wk7ha80M1qfvq8UtuZg918AZyh+q65s68dKvXwVTQ="
secret_link: "69rUgWgrLbV50CiAEK78AJrLoWBGHGwYCX25phh3yg="
values_codec: "ggxhfxrjshb034fosedfwd3d"
```

#### 4.2.3.1.5 Настройка параметров `dispersed_object_store`

Настройка параметров приведена в Таблице 19.

Таблица 19 – Настройка параметров `dispersed_object_store`

Параметр	Тип	Описание
<code>dispersed_object_store_management_token:</code> ""	Str	Токен доступа для управления через API сервиса

Пример корректно настроенного параметра:

```
dispersed_object_store_management_token: "Aig2utoavi6iagieltas"
```

#### 4.2.3.1.6 Настройка параметра `Docker`

Настройка параметров приведена в Таблице 20.

Таблица 20 – Настройка параметров **Docker**

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

Пример корректно настроенного параметра:

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

#### 4.2.3.1.7 Настройка параметров grafana

Настройка параметров приведена в Таблице 21.

Таблица 21 – Настройка параметров **grafana**

Параметр	Тип	Описание
grafana_admin_password:	Str	Пароль администратора grafana

Пример корректно настроенного параметра:

```
grafana_admin_password: "Ooj0Inahgh2Ixailoxie"
```

#### 4.2.3.1.8 Настройка hydra

Настройка параметров приведена в Таблице 22.

Таблица 22 – 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"
```

#### 4.2.3.1.9 Настройка параметров jwt\_key

Настройка параметров приведена в Таблице 23.

Таблица 23 – Настройка параметров **jwt\_key**

Параметр	Тип	Описание
jwt_key:		Параметры <b>jwt_key</b>
priv:	Str	Закрытый ключ
pub:	Str	Публичный ключ

Пример корректно настроенного параметра:

```

jwt_key:
priv: |
----BEGIN RSA PRIVATE KEY-----
MIIIEowIBAAKCAQEA063xN82Y0tJBq8sfD79bJ+4W9QEdOueQljPziN4JdYntS381
AqxOA4Ud886S4LdwCN2KSpuh7QSHkzjzH9AIDrHCYShOfPAeHLMCBDSzazr2IOc0
Jaw3bHRfrM9Iib+X4qdDE88Mfk+B/8Sa/xG2HJVy0Jb4XoipwzEB900a+6zpnLT
q/kNt7YtrTBmrpSzFMr0VD+x0Ftb9zhiFVlyVscVKEl67+TNIWahgzH14YF8xP8
gb89coH114YUNfxN8IKURdY9QFNuZLF+x8xfL4CWwydSbtL7dFFK0HVowMt4tnoJ
okthJ5JZNw+XZAXHS3NyuvbYmP+iqRuL2YAr2wIDAQABAoIBAGyNHs5HGHRsOuw
VorKDq0DY7Jwx9SVO4hLS/A8LQ2hlZbJvR2JztfvQ9TrclbauxFQysJH3Vn2oK/W
3JbL3rUSY2P/j4Bygn6lLbuNwGiU6/MjnZJUJnfvlcDA67AfeHw62iMmYnnDvB61
a+ax5nnyCdb/DIMsZujTmxONVHykFSF8xQhIRCJQCIXx3f1dJyaG4Qpy9WqIDVRX
5SUYegDVtNQKQO4UgrgTnOFBkPCbN9SmWEqNTnZVzPAMA3sbJkYsNEVbtuHg8G0M
nWzN7hBV6pu1P096IDrSJC7qpVmb75UG5f9Oo2F0x1hHyE7bCiXN+iCdhPful7g
u6vptYECgYEA+PWFT4+kYRA3cb5Ki6oHLM4uhIrJzxJxWalb2Iky1Ta3YZ4alsXL
9uac3vqZJBTxPjJLwmUaktUmf+xf3CBq5e3O3BcKDDn3svs7ibawjoWK6lG5D+tf
XwzkRMT2IK6hDn16IK/DchFYTw5zy/AbyjjEAjN2y/JaLwhTywGXLdkCgYEA2aqD
zNT+Oxt9LTnvr8RUAMIgN/g07WQNYWwmlc6HSq+IhxvypN5+PaFjMLCioP7X7t
YG9arh8PwDfc4kpZwnB6QWcqTucZOzbIcsVWWsMoWftVjpbCCkxZ9Sg0waKju7Bz
Dzrjzsn+AoC7O/RydhbUALUoEN5Toz8Sv5bZMtMCgYEA1mnGHaaNoNbxmXGVDEIs
mccdQyOw+TleDCWTJ6PJ9t2ABH/BUJcbuhIViujzGaM7viBdJRgkUc9nsAbo7FGz
H0G3xc/F5I/MKAa92TZRSv3yjSpDI1XITrkIo72qzJS1uyAQHbSitEwB7Vx6GGs7
0+cd0PN33eBIEVqvqAg/pskCgYB00NJTR6v5RNN1RwBymlBMRJR3ta8Pb82qCv47
dbd2l83auLA2Y9d+Ca+sjkBJnX905WAy9RARipIFcvWUbjqng33ZQ+is19HuuYPy
NH4Xz80EHaLZF4ejxz4wGBfYI9UDkbruxYiNHik4PSY/Eu+20KGOj6qlAuyYG+2P
7QE8CQKBgBxUBFeFTRZxvUV+FfcVgrQxoD6C9PA46/wV9qkVfCo8i7UnDc7ovKuQ
Uq3/k9aD8NKVjJn7/kQENLIBjCHcpazMHQJnvpfRaQfBre0G1ok9sPH/rvTgK1U
clKH2eSXgRhKglf3Dtf6m2bULj0HN0FIydngh0F1EqK10vnnvqfkN
----END RSA PRIVATE KEY-----

pub: |
----BEGIN PUBLIC KEY-----
MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA063xN82Y0tJBq8sfD79b
J+4W9QEdOueQljPziN4JdYntS381AqxOA4Ud886S4LdwCN2KSpuh7QSHkzjzH9A
IDrHCYShOfPAeHLMCBDSzazr2IOc0Jaw3bHRfrM9Iib+X4qdDE88Mfk+B/8Sa/xG2

```

```
HJVy0Jjb4XoipwzEB900a+6zpnLTq/kNt7YtrTBmrgpSzFMr0VD+x0Ftb9zhiFVL
yVscVKEl67+TNIWahgzh14YF8xP8gb89coH114YUNfxN8IKURdY9QFNuZLF+x8xf
L4CWwydSbtL7dFFK0HVowMt4tnoJokthJ5JZNw+XZAXHS3NyuvbYmP+iqRuL2YAr
2wIDAQAB
-----END PUBLIC KEY-----
```

#### 4.2.3.1.10 Настройка параметров **keepalived**

Настройка параметров приведена в Таблице 24.

Таблица 24 – Настройка параметров **keepalived**

Параметр	Тип	Описание
keepalived_vrrp_instances		Параметры <b>keepalived</b>
ucs_frontend:		Параметры <b>ucs_frontend</b>
password:	Str	Пароль
virtual_ip:	Str	Виртуальный IP для серверов с ролью <b>ucs_frontend</b>
ucs_mail:		Параметры <b>ucs_mail_relay</b>
password:	Str	Пароль
virtual_ip:	Str	Виртуальный IP для серверов с ролью <b>ucs_mail_relay</b>

Пример корректно настроенного параметра:

```
keepalived_vrrp_instances:
ucs_frontend:

password: "UgohSh8i"
virtual_ip: "192.168.119.35"
ucs_mail_relay:

password: "keeB5ooH"
virtual_ip: "192.168.119.12"
```

#### 4.2.3.1.11 Настройка параметров **mongodb**

Настройка параметров приведена в Таблице 25.

Таблица 25 – Настройка параметров **mongodb**

Параметр	Тип	Описание
mongodb_root_password:	Str	Пароль пользователя root для СУБД



Параметр	Тип	Описание
mongodb_secured_key:	Str	Ключ для доступа к СУБД
mongodb_users:		Словарь. Каждый ключ словаря – пользователь
marker:		Ключ, имя пользователя
database:	Str	База для аутентификации
password:	Str	Пароль для аутентификации
roles:		Список ролей
- role:	Str	Роль пользователя
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_users:
  achill:
    password: "cohh0Av2mai2aJae"
  beef:
    password: "idohjie2Ikeice0I"
  clotho:
    password: "wahcoovei0bahRu4"
  daidal:
    password: "cheYichoongoh4gi"
  erakles:
    password: "Uxeu4ieph1uix1ah"
  hog:
    password: "rae0faeng1Seupee"
  homeros:
    password: "хоопunaihuopaе4J"
  marker:
    password: "ohvufoosaeTeeCo3"
```

```
mongodb_exporter:  
  password: "woo2Yual2saeboh1"  
kongur:  
  password: "ahmeayooH1yahlohreem"  
kronos:  
  password: "peiNguxud8ooThaiCahL"  
odusseus:  
  password: "oY9ja7ietheec6sahthe"  
perseus:  
  password: "xuoboop5Geneemei"  
talaos:  
  password: "Ahroozait4pesupohpho"  
theseus:  
  password: "ua8mu0uoj6uvieDu2gei"  
thoth:  
  password: "BooRah6oal9Naehai2ph"
```

#### 4.2.3.1.12 Настройка дополнительных параметров postfix

Настройка дополнительных параметров приведена в Таблице 26.

Таблица 26 – Настройка дополнительных параметров postfix

Параметр	Тип	Описание
postfix_additional_mynetworks:	list	Список дополнительных сетей, из которых разрешена отправка через МТА 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"
```

#### 4.2.3.1.13 Настройка параметров nats

Настройка параметров приведена в Таблице 27.

Таблица 27 – Настройка параметров nats

Параметр	Тип	Описание
nats_authorization_password:	Str	Пароль для авторизации в <b>nats</b>
nats_cluster_authorization_password:	Str	Пароль для <b>nats cluster auth</b>

Пример корректно настроенных параметров:

```
nats_authorization_password: "Fiohoogh7Raobi4yeiSi"
nats_cluster_authorization_password: "ao1Iey7luRoh1ahf9eVe"
```

#### 4.2.3.1.14 Настройка параметров redis

Настройка параметров приведена в Таблице 28.

Таблица 28 – Настройка параметров **redis**

Параметр	Тип	Описание
redis_dafnis_password	Str	Пароль для <b>redis_dafnis</b>
redis_dowal_password	Str	Пароль для <b>redis_dowal</b>
redis_ektor_password	Str	Пароль для <b>redis_ektor</b>
redis_erakles_password	Str	Пароль для <b>redis_erakles</b>
redis_euripides_password	Str	Пароль для <b>redis_euripides</b>
redis_hog_password	Str	Пароль для <b>redis_hog</b>
redis_homeros_password	Str	Пароль для <b>redis_homeros</b>
redis_minos_password	Str	Пароль для <b>redis_minos</b>
redis_rspamd_password	Str	Пароль для <b>redis_rspamd</b>
redis_sdd_password	Str	Пароль для <b>redis_sdd</b>
redis_viper_password	Str	Пароль для <b>redis_viper</b>

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_minos_password: "quie2jiG2CeucosShahG"
redis_rspamd_password: "Iughoo2iuS2Xew1die4p"
redis_sdd_password: "fohphow6eat1aekod5Oh"
redis_viper_password: "Tee9han6ienaYoSievo"
```

#### 4.2.3.1.16 Настройка параметров rspamd

Настройка параметров приведена в Таблице 29.

Таблица 29 – Настройка параметров **rspamd**

Параметр	Тип	Описание
rspamd_dkim_hosts:		Параметры антиспама
		Параметры <b>dkim_hosts</b>
<your_external_domain>		Имя внешнего домена, который необходимо подписывать ДКИМ-ключом
dkim_key:	Str	ДКИМ-ключ
rspamd_web_password:	Str	Пароль от веб-интерфейса

Пример корректно настроенного параметра:

```
rspamd:
dkim_hosts:
example.domain.org:
dkim_key: |
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBBKkwggSIAgEAAoIBAQC3euVQm/Djy1z1
JhbTC5Cs99HmrgN6DldM5xivTyhopgkG1HXIoWaKfvt3wKm/Pzah2/BkcThtDa3w
E70bmjVXFX2xkXG5DAuY9ChnX6+xWYCeBUeRsMSnWdyoNBwFK9rjE2vZ+u3OzLhz
wP6PuIyigV7A3D9Mtok0XA3iH/7G+99ARjxhj8hCkYEeqEsR688uU1JNeztTfkte+
mz6n7w8A02jdpdG8wRqjvj4B4H0MaaP7R4y/UopZ+UP0RAbm7KryOjgC15uLou9Y
Yg9ym0VkcAIovc0xQT7Zk13yf8vIuVS/6yhO3FcKYB4mx0Szz1RpU2ueyvD2COSj
C+2uZsPFAgMBAAECggEBAK6+xEH2kwFRAPKWWSydGigyS14K11OO7wRWIMNuf4zT
fUsf/+GaHoAPGk7eVozHlq+nOhdfXz2rRpqdIgF06BJNbI2+ePIFj9IXz5dMoZcm
KAHYA2a1VUYRpr8oCfu+3dRg/dn4S58miRHtoESfPonS7rx9x2e3fyS5lRtk35EA
Wp5Vy+2U36cKIJLVtAOvzRbG19SLjPAvuc/WKGda2lA7HBlhep/Yrm0RUoH//5Px
fJwLVSy34B31FxlwZk80aVquXCv644GbR89RIQtziHg9q4g/wyZ5/+ZG/967kim
tKDS8PWhAK5pjUHS9cED/hjs+ITINCI4qKf2zj2XSqECgYEA3X9zmaAw9JLnelZN
3oVM/boqtwfPgnO6Y98inDMsecAICWLCAsEsWYY90IB3FQCXJXVrGTxKnHa3S0fR
MTX5xx3Rta5SWf88jUQCmZEuxHBeIEN9JKebKC97rKIIJmYJ8PVZ8c6LAvMgmYc
sd+GyjJAmV+N7j5Eo8tXmZCCuK0CgYEA1A9t7P6GjXQQFrIk81+x+0JHmIN+DPKs
eyR6avDfd32HIq2dPCMmjCA17EFbfOPVnx9rZvLrEWtTkgU8DYBPIZ955EJORi9l
eqYeOKwhWLUMgwHyWIEJZPeY3o31TF1NwNG16Qy98h4zr2SUaTuCdccoNWAc0GuI
rA1Gjn7AonkCgYEAuMpgFJS8Aw+cdwARrxfB7+Na23kvZz3X+ME6PP4owqGqe3u
loW7DmVkpNLihokbkHDJjSAzxx1sBi5AZKH3ZRuHnd91bQf36JNY5+2r6s8keB5W
BYKfe4NB1uDfwLbjrik/nXklGyIs2l2AWxV1SrNqGysSyjTA5zX6O2/I33ECgYBS
eO23jgWmXc0kBoR4Ym9F2LEfj4QmZPrPqZAypxtBzYAQ7JSKHuGO/bHCAGkkWTdD
COUsVK03SRZnY8HHPm+1MSCmtWLbyPMekByQzeDqLv9+s/MdTQbqTaEWbP9Jg8AJ
jYXB7UKyNyzCucs+YfaK97mbiJWsOSYeQ8t8/67LgQKBgQCk4q/D5Cq5Fqalbk/0
jyEQAmHgrhWEJO2bECGjGIJ13/Hj3bbQ3znfPUDf9MLDtrveGu4YdspL3S4yahLO
```

```
EXxXPgwHCDLqamx5vj4QKFPPQEHXv68RK6RKhw7m2IeyI/7nsHPvjZhNZI4ulSTN
CLCjuiw8tvIafY26wKDylpvnRQ==
-----END PRIVATE KEY-----
```

```
web_password: "iePixieTaf4IriequieX"
```

#### 4.2.3.1.17 Настройка параметров servus

Настройка параметров приведена в Таблице 30.

Таблица 30 – Настройка параметров **servus**

Параметр	Тип	Описание
servus:	Str	Параметры <b>servus</b>

Пример корректно настроенного параметра:

```
servus: "Iefae4yoh4rohceepoli"
```

#### 4.2.3.1.18 Настройка параметров mailion\_\*

Настройка параметров приведена в Таблице 31.

Таблица 31 – Настройка параметров **setup**

Параметр	Тип	Описание
mailion_cluster:	bool	Флаг кластерной\SA инсталляции
mailion_domain_module	special	Переменная для генерации эндпоинтов инсталляции
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 интеграция с решениями MS
mailion_integrations.psn	bool	Включение и отключение интеграция с PSN
mailion_internal_web_auth	dict	Словарь содержащий настройки внутренней веб-аутентификации
mailion_internal_web_auth.enabled	bool	Включение и отключение аутентификация для доступа к веб-интерфейсам инфраструктурных сервисов (мониторинг, графана ит.д.)
mailion_internal_web_auth.password	str	Пароль для аутентификации для доступа к веб-интерфейсам инфраструктурных сервисов

Параметр	Тип	Описание
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:
  microsoft: false
  psn: false
mailion_internal_web_auth:
  enabled: true
  password: "rfkg7shtasjfha6vnd"
mailion_max_users: 100
mailion_service_accounts:
  ariadne: "Um6heiNie2doeshee2sa"
  atlas: "Gaezohg1Ad3naf5ahpef"
  clotho: "Hyrq5iedwemdLNRv47KT"
  elysion: "le0eelePhooghoughoopo"
  erakles: "Ui6ohDahLeitozughugh"
  hog: "shee8einoh4AivigePei"
  homeros: "ooph8Efu1eesu2quah1u"
  kongur: "aa6eizooguPhene9uifu"
  kronos: "iphuTh0eiY2ook4aeph5"
  leda: "72YjiCQmwUwCR32sVrL"
  lmtp: "aicae3yo7Aukaejeel2e"
  marker: "eer1edaecceJu6naiPom"
  paranoid: "Yoa4eNgahm0aeChu8uWe"
  perseus: "Oogh9ahroow2eicaeng7"
  razor: "Ohquietikenu2Aeloh6E"
  theseus: "eileixietai0cahQu3ma"
  viper: "Feir8uewie4Ieshu4thi"
  woof: "at6Ohdapohaitahtho2j"
  zeus: "fa4Ohxaithee0yae1eit"
mailion_supported_domains: []
```

#### 4.2.3.1.20 Настройка параметров unbound

Настройка параметров приведена в Таблице 32.

Таблица 32 – Настройка параметров **unbound**

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

Пример корректно настроенного параметра:

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

#### 4.2.3.1.21 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 <b>resolv.conf</b>

Пример корректно настроенного параметра:

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

#### 4.2.3.1.23 Настройка параметров **sophokles**

Настройка параметров приведена в Таблице 34.

Таблица 34 – Настройка параметров **sophokles**

Параметр	Тип	Описание
----------	-----	----------

sophokles_access_token:	Str	Токен для сервиса авторизации <b>minos</b> и <b>sophokles</b>
-------------------------	-----	---

Пример корректно настроенного параметра:

sophokles_access_token: "IeWoh9eateihuvoxekah":
---

#### 4.2.3.1.24 Настройка параметров **theseus**

Настройка параметров приведена в Таблице 35.

Таблица 35 – Настройка параметров **theseus**

Параметр	Тип	Описание
theseus_cipher_key:	Str	Ключ шифрования <b>theseus</b>

Пример корректно настроенного параметра:

theseus_cipher_key: "RWVmb21pZXhvbmfPZzZvaHlhaTR6aURhd2VpZzhlZW4="
--

#### 4.2.4 Настройка дополнительных параметров установки

Настройка дополнительных параметров установки не выполняется для ПО «Mailion».

#### 4.2.5 Настройка межсетевого экранирования



Во время установки на все сервера **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 36.

Таблица 36 – Установленные правила межсетевого экрана

Сервера	Таблица	Состояние	Порт	Протокол	Интерфейс	Разрешение
Сервера группы <b>ucs</b>	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
	INPUT				docker0	ACCEPT



Сервера	Таблица	Состояние	Порт	Протокол	Интерфейс	Разрешение
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
Сервера 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	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT	NEW	53	UDP		ACCEPT
Сервера группы ucs_infrast ructure	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
					docker0	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT		53	TCP		ACCEPT
INPUT		53	UDP		ACCEPT	
Сервера 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	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT			VRRP		ACCEPT
Сервера группы ucs_mail	INPUT					DROP
	FORWARD					DROP
	OUTPUT					ACCEPT

Сервера	Таблица	Состояние	Порт	Протокол	Интерфейс	Разрешение
	INPUT	RELATED, ESTABLISHED				ACCEPT
	INPUT			ICMP		ACCEPT
	INPUT				lo	ACCEPT
	INPUT	NEW	SSH	TCP		ACCEPT
					docker0	ACCEPT
	INPUT		2376	TCP		ACCEPT
	INPUT		9100	TCP		ACCEPT
	INPUT			VRRP		ACCEPT

#### 4.2.5.1 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 по отношению к контуру инсталляции стороны.

Во внешний контур должны быть доступны только:

- порты на виртуальные IP серверов с ролью **ucs\_frontend**:
  - 80/tcp;
  - 143/tcp;
  - 443/tcp;
  - 443/udp;
  - 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.

#### 4.2.6 Разграничение доступа

Настройки по умолчанию.

## 4.2.7 Настройка удаленного доступа

Настройки по умолчанию.

## 4.3 Установка «Mailion»

### 4.3.1 Конфигурация без отказоустойчивости

#### 4.3.1.1 Запуск установки

Для установки необходимо запустить команду на установку «Mailion»:

```
[root@ucs-installer ~]# ansible-playbook playbooks/main.yml --diff
```

После этого запускаются роли, описанные в разделе 4.2.1.

#### 4.3.1.2 Проверка корректности установки

Для проверки корректности установки необходимо запустить установленный «Mailion»:

1. Открыть в поддерживаемом веб-браузере страницу по адресу, который указывался в **mailion\_external\_domain**.
2. Использовать для входа учетные данные созданных пользователей или администратора.
3. Отправить письмо самому себе внутри «Mailion» (от пользователя, если вход выполнен под администратором — сначала нужно создать пользователя, если он не был создан плейбуком **ministerium**).
4. Если письмо успешно отправилось и пришло — инсталляция настроена корректно.

#### 4.3.1.3 Добавление дополнительных доменов для обслуживания инсталляцией

Добавлена поддержка дополнительных доменов. Чтобы добавить дополнительный домен необходимо добавить 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 МТА, а также добавит dkim-ключи для доменов в **rspamd**.

## **4.3.2 Кластерная отказоустойчивая конфигурация**

### **4.3.2.1 Запуск установки**

См. п. 4.3.1.1.

### **4.3.2.2 Проверка корректности установки**

См. п. 4.3.1.2.

## **4.4 Установка в составе других продуктов «МойОфис»**

Установка в составе других продуктов «МойОфис» не выполняется.

## **4.5 Установка надстройки для Microsoft Outlook**

Подробное описание установки надстройки для Microsoft Outlook приведено в документе «Mailion. Руководство пользователя (надстройка для Microsoft Outlook)».

## **5 Обновление с предыдущих версий**

Данный дистрибутив предназначен для установки с нуля. Обновления возможны с версии 1.0.

### **5.1 Состав дистрибутива**

См. раздел 3.

### **5.2 Подготовка к обновлению**

#### **5.2.1 Описание ролей**

См. раздел 3.

#### **5.2.2 Проверка и настройка инфраструктуры установки**

См. раздел 3.

#### **5.2.3 Проверка и настройка основных параметров установки**

См. раздел 3.

#### **5.2.4 Проверка и настройка дополнительных параметров установки**

См. раздел 3.

#### **5.2.5 Проверка и настройка межсетевого экранирования**

См. раздел 3.

#### **5.2.6 Проверка и настройка разграничения доступа**

См. раздел 3.

#### **5.2.7 Проверка и настройка удаленного доступа**

См. раздел 3.

#### **5.2.8 Создание резервных копий**

См. раздел 3.

### **5.3 Обновление «Mailion»**

#### **5.3.1 Конфигурация без отказоустойчивости**

См. раздел 3.

##### **5.3.1.1 Запуск обновления**

##### **5.3.1.2 Проверка корректности обновления**

См. раздел 3.

##### **5.3.1.3 Миграция данных**

См. раздел 3.

## **5.3.2 Кластерная отказоустойчивая конфигурация**

См. раздел 3.

### **5.3.3.1 Масштабирование конфигурации**

См. раздел 3.

#### **5.3.3.2 Запуск обновления**

См. раздел 5.

#### **5.3.3.3 Проверка корректности обновления**

См. раздел 3.

## **6 Дополнительные возможности и рекомендации по установке**

### **6.1 Настройка мониторинга состояния**

Настройки по умолчанию.

### **6.2 Настройка взаимодействия со службой каталогов**

Настройки по умолчанию.

### **6.3 Настройка антивирусного программного обеспечения**

Настройки по умолчанию.

## 7 Техническая поддержка

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

- Адрес электронной почты: [support@service.myoffice.ru](mailto:support@service.myoffice.ru)
- Телефон: 8-800-222-1-888.