Оглавление

Установка Колибри-АРМ.МФЦ

1. Предварительные требования и соглашения

Ниже приведены общие рекомендации по установке системы Колибри-АРМ.МФЦ (далее Система).

1.1. Поддерживаемые операционные системы

• Debian 11 Bullseye 64 bit - предпочтительный вариант

• Astra Linux Special Edition 1.7.3-1.7.5 64 bit

!ВАЖНО!

Имя хоста, куда устанавливается Система, должно совпадать с именем в файле /etc/hosts для 127.0.1.1 или 127.0.0.1.

Отключение на основном сетевом интерфейсе функционала IPv6 приводят к ошибкам в процессе установки, несмотря на то, что IPv6 зарезервирован в Системе для будущих нужд, оставьте его включенным, даже если он не используется в инфраструктуре.

В случае развертывания Системы ***в закрытом контуре, необходимо настроить репозитории пакетов на сервере Системы на использование локальных зеркал****. Архив с установочным пакетом содержит в себе только те компоненты, которые невозможно*

установить из стандартных репозиториев. Рекомендуется настроить следующие репозитории:

• *для* ***Astra Linux*** *- main, base, extended, update;*

• *для* ***Debian 11 Bullseye*** *- bullseye, bullseye-updates, bullseye-security.*

Подключение репозиториев на оптических носителях при отсутствии носителей в приводе сервера приводит к ошибке при установке*, проверьте, что они либо отключены, либо носитель смонтирован в привод.*

1.2. Аппаратные требования

Система может быть развернута как на физической, так и на виртуальной машине. При развертывании на виртуальной машине KVM необходимо включить эмуляцию процессора минимум Intel Ivy Bridge.

	Минимально	Рекомендуемое
Процессор	2.2 ГГц и выше, 2 ядра	2.2 ГГц и выше, 4 ядра
Оперативная память	8192 МБ	16384 МБ
Жесткий диск	120* ГБ	120* ГБ

* - требуемый размер жёсткого диска напрямую зависит от объёма пакетов ПО и образов ОС, которые в дальнейшем будут загружены в хранилище Системы

1.3. Инфраструктурные требования

Основным требованием к инфраструктуре является создание ресурсных записей на DNS сервере (полный список приведён в таблице ниже). Ресурсные записи должны быть созданы **до развертывания Системы.** Система поддерживает две нотации записей:

- <service>.<prefix>.<domain.name>
- <service>-<prefix>.<domain.name>

где:

• <service> - название сервиса. Все требуемые сервисы перечислены в таблице ниже;

• <prefix> - название системы. Рекомендуемое название - colibri;

• <domain.name> - домен организации в котором расположена Система;

• "." или "-" - разделитель.

!ВАЖНО!

Основной домен <domain.name> должен быть не выше второго уровня (техническое ограничение платформы). Иными словами: company.ru - валидный основной

домен, ru - нет. Учитывайте этот фактор при создании записей и использовании скрипта установки.

После запуска установщика в интерактивном режиме, Оператор установки задает значения переменных <prefix> (например, *colibri*), разделитель [.|-] и <domain.name> (например, *company.local*). Если необходимо установить Систему в домен 4го уровня, например, *colibri.kazan.company.ru*, то для <domain.name> нужно будет указать *kazan.company.ru.*

Касательно DNS записей, если задан домен *company.local*, название системы *colibri* и разделитель ".", то, к примеру, для сервиса *reporting* нужно внести следующую ресурсную запись на DNS сервере - *reporting.colibri.company.local.*

1.3.1 Полный список ресурсных DNS записей, которые необходимо добавить на DNS сервере

Записи с <service>-<prefix>.<domain.name> (префикс задан с тире)	Записи с <service>.<prefix>.<domain.name> (префикс задан с точкой)
<prefix>.<domain.name>	<prefix>.<domain.name>
reporting-<prefix>.<domain.name>	reporting.<prefix>.<domain.name>
setup-<prefix>.<domain.name>	setup.<prefix>.<domain.name>
api-<prefix>.<domain.name>	api.<prefix>.<domain.name>
vault-<prefix>.<domain.name>	vault.<prefix>.<domain.name>
auth-<prefix>.<domain.name>	auth.<prefix>.<domain.name>
queue-<prefix>.<domain.name>	queue.<prefix>.<domain.name>
db-<prefix>.<domain.name>	db.<prefix>.<domain.name>
storage-<prefix>.<domain.name>	storage.<prefix>.<domain.name>
orchestrator-<prefix>.<domain.name>	orchestrator.<prefix>.<domain.name>
agentapi-<prefix>.<domain.name>	agentapi.<prefix>.<domain.name>
signalr-<prefix>.<domain.name>	signalr.<prefix>.<domain.name>
Пример DNS записи API для префикса *colibri*, разделителя “-” и домена *company.ru* *api-colibri.company.ru*	Пример DNS записи API для префикса *colibri*, разделителя “.” и домена *company.ru* *api-colibri.company.ru*
Пример DNS записи WEB-интерфейса Системы для префикса *colibri*, разделителя “-” и домена *company.ru* *colibri.company.ru*	Пример DNS записи WEB-интерфейса Системы для префикса *colibri*, разделителя “.” и домена *company.ru* *colibri.company.ru*

1.4 Сетевые требования (порты и прочее)

1.4.1 Порты на стороне клиента

На стороне клиентских машин необходимо открыть следующие порты:

Описание	Порт
Первоначальная установка по SSH. Администрирование по SSH	22/TCP
Первоначальная установка по WMI (для Windows клиентов)	135/TCP
Администрирование по RDP	3389/TCP
Обмен файлами (SMB)	139/TCP, 445/TCP

1.4.2 Порты на стороне сервера

На стороне сервера Системы правила брандмауэра создаются автоматически, однако на уровне сети следует проверить возможность коммуникации с сервером Системы по следующим портам:

Описание	Порт
Протокол SSH	22/TCP
Протокол FTP	21/TCP
Сервер TFTP	69/UDP
Пассивный FTP	5000-10000/TCP
Сервис очереди сообщений	15672/TCP, 5671/TCP, 5672/TCP
Сервис аутентификации	8189/TCP, 9444/TCP
Сервис управления чувствительными данными	8443/TCP
Сервис отчетности	8088/TCP
Сервис управления конфигурациями	14505/TCP,14506/TCP
Протокол SMB	137/TCP,UDP,138/UDP,139/TCP,445/TCP
Веб-интерфейсы	80/TCP,443/TCP
Сервис точек распространения	5001/TCP, 5002/TCP
Сервис баз данных	5432/TCP
API сервиса управления конфигурациями	18000/TCP

1.5 Требования к клиентам на базе ОС Linux

1. На машине должен быть запущен демон SSH клиента на стандартном порту 22

2. Пользователь, который используется для подключения к машине должен иметь право на повышение привилегий в процессе выполнения команд через sudo

3. Установлен sudo

2. Процесс установки Системы

2.1 Дистрибутив Системы

Дистрибутив поставляется в виде архива - *colibriARM_installer_24.7.tar.gz* - содержащего все необходимые компоненты для оффлайн-инсталляции (образы контейнеров и сервис удаленного управления машинами). Обратите внимание, что **оффлайн инсталляция не отменяет необходимости подключения стандартных репозиториев пакетов для ОС**, установщик содержит только то, что необходимо было бы скачать из реестра контейнеров Docker и Node Package Manager при наличии интернета.

Архив необходимо распаковать в одну папку, получив в итоге каталог *./colibri-arm/* и указанную ниже структуру внутри:

```
.
├── common_scripts
│   ├── common_functions.sh
│   └── logger.sh
├── data
│   ├── agent.api
│   ├── checksum
│   ├── colibriagentpackage
│   ├── conjur
│   ├── docker
│   ├── elevated-server
│   ├── importservice
│   ├── jobservice
│   ├── keycloak
│   ├── nginx
│   ├── pgp
│   ├── portal_backend
│   ├── portal_frontend
│   ├── postgresql
│   ├── prerequisites
│   ├── proftpd
│   ├── salt
│   ├── samba
│   ├── signalr-server
│   ├── servicerepo
│   └── superset
├── install.sh
├── remove_all.sh
├── demo.lic
├── scripts
│   ├── agent.api.sh
│   ├── common_prerequisites.sh
│   ├── conjur.sh
│   ├── docker.sh
│   ├── elevated-server.sh
│   ├── gencert.sh
│   ├── importservice.sh
│   ├── jobservice.sh
│   ├── keycloak.sh
│   ├── nginx.sh
│   ├── portal_backend.sh
│   ├── portal_frontend.sh
│   ├── postgresql.sh
│   ├── proftpd.sh
│   ├── rabbitmq.sh
│   ├── salt.sh
│   ├── samba.sh
│   ├── servicerepo.sh
│   ├── signalr-server.sh
│   ├── superset.sh
│   ├── ufw.sh
│   └── users.sh
```

2.2 Предварительная проверка сервера на совместимость с Системой

Установщик предлагает функционал по предварительной проверке целевого сервера на совместимость с Системой. Данный функционал осуществляет только проверку и не вносит никаких изменений в реальную систему.

Для использования данного функционала, достаточно запустить с правами суперпользователя следующую команду:

./install.sh -C

дождаться её выполнения и изучить полученный отчёт.

!ВАЖНО!

Настоятельно рекомендуется выполнить проверку готовности инфраструктуры ***ДО ЗАПУСКА УСТАНОВКИ ПРОДУКТА*** *и, в случае необходимости, привести окружение в нужное для установки состояние.*

2.3 Запуск установки

После распаковки достаточно запустить с правами суперпользователя скрипт install.sh и ответить на несколько вопросов:

• Основной IP адрес машины (установщик сам находит адрес нулевого интерфейса, можно согласиться с адресом по умолчанию, убедившись, что DNS записи смотрят на этот интерфейс).

• Имя основного домена - правая часть домена, в котором вы разворачиваете Систему, например, *company.local*.

• Префикс установки, например, *colibri*.

• Разделитель, как говорилось ранее можно задать либо "." либо "-".

Именно из этих частей и преднастроенных имен сервисов, установщик будет составлять альтернативные объекты имен для сертификатов. Далее необходимо дождаться окончания установки

!ВАЖНО!

Оба значения (префикса и основного домена) ***должны быть заданы в lower case****, в ином случае корректность работы Системы не гарантируется*

!ВАЖНО! *Во время установки создается файл file.rsp, в который записываются все сервисные учетные данные.*

Если на момент начала установки в файле file.rsp уже заданы значения основного IP адреса, домена, префикса и разделителя, то установщик ***НЕ БУДЕТ*** *запрашивать ввод этих данных повторно. Если вам нужна интерактивная инсталляция с участием пользователя, убедитесь, что в файле file.rsp отсутствуют следующие параметры (или*

значения для них пусты): COLIBRIHOST, DOMAINNAME, DOMAINPREFIX, DOMAINDELIMITER

2.4 Пост-установочные шаги

• Перейти по адресу http:// <prefix>.<domain.name>:5001/service_repo/agent/ca/, сохранить файл colibriCA.crt и установить сертификат в доверенное хранилище сертификатов машины оператора. Это необходимо для того, чтобы использовать протокол https без предупреждений о небезопасном сайте.

• Найти в каталоге установки и перенести в безопасное место файл *file.rsp* - это файл со всеми сервисными учетными записями, которые использует Система.

• Выполнить вход в Систему по адресу https:// <prefix>.<domain.name> с логином и паролем.

2.5 Установка собственного сертификата

• **запускать ТОЛЬКО ПОСЛЕ успешной установки Колибри-АРМ**;

• Запустить с правами суперпользователя следующую команду:

./install.sh -S;

• в каталоге установщика будет создан каталог custom_certificates в который необходимо скопировать следующие файлы:

colibri.crt- сертификат x509 в формате crt,

colibri.key- ключ сертификата x509,

colibriCA.crt - корневой сертификат x509 в формате crt,

и нажать Enter.

• после этого будет предложен выбор типа вашего сертификата (выпущен внешним центром сертификации либо внутренним CA);

• проверить работоспособность Колибри-АРМ и ответить на вопрос “Все ли работает корректно?”;

В случае отрицательного ответа скрипт откатит сделанные изменения.

!ВАЖНО!

*Если ваш сертификат выпущен внешним доверенным центром сертификации, то в поле subjectAltName он должен содержать wildcard имя домена в формате *.<prefix>.<domain.name> (например, *.colibri.company.ru) и основной адрес сервера <prefix>.<domain.name> (например, colibri.company.ru);*

*либо, если использовался разделитель “-”, то *.<domain.name> (например, *.company.ru) и основной адрес сервера <prefix>.<domain.name> (например, colibri.company.ru)*

3. Удаление Системы

Для полного удаления продукта достаточно запустить скрипт remove_all.sh с правами суперпользователя.

!ВАЖНО!

*Скрипт **ПОЛНОСТЬЮ УДАЛЯЕТ ВСЕ ДАННЫЕ**, убедитесь, что сделаны резервные копии важных данных.*

4. Известные проблемы и особенности при настройке и эксплуатации Системы

4.1 Известные особенности клиентских машин под управлением РЕД ОС

Симптомы	Решение
При стандартной настройке сети (DHCP + DNS сервер в локальной сети), попытка распространения агента на машину заканчивается неудачей	Проверить, что с целевой машины корректно резолвятся DNS-адреса хотя бы сервера Системы, и если нет, но при этом в /etc/resolv.conf и в настройках сети корректно настроены DNS серверы, следует в файле /etc/nsswitch.conf (примерно на 65-67 строке) настроить порядок разрешений имен таким образом, чтобы dns параметр был сразу за параметром files, например: hosts: files dns resolve [!UNAVAIL=return] myhostname mdns4_minimal [NOTFOUND=return]

4.2 Известные особенности клиентских машин под управлением Windows

Симптомы	Решение
Попытка распространения агента на машину заканчивается неудачей с ошибкой невозможности коммуникации с целевой машиной	Обязательным условием корректной установки агента на Windows-машины является включенный доступ к административной общедоступной папке в корне системного раздела по пути \\\C$. ПО умолчанию, она включена на всех серверах Microsoft и выключена на клиентских ОС. Включить можно следующей командой: REG add HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f