МИРАЖ

Система раннего обнаружения внутренних угроз

Руководство по установке

Версия документа: 2.0.1
Дата редакции: 13 ноября 2026 г.
Разработчик: ООО «Ти Хантер»

Санкт-Петербург
2026

Содержание

1 Назначение документа 3

2 Схема и предварительные требования 3

3 Проверка и распаковка дистрибутива 4

4 Установка Data Plane 4

4.1 Проверка DP 4

5 Установка Control Plane 4

5.1 Проверка CP 5

6 Регистрация Data Plane 5

7 Сети и профили ловушек 5

8 Первый вход и лицензия 5

9 Проверка установки 6

10 Обновление и устранение ошибок 6

11 Передача сведений об ошибке 6

1 Назначение документа

Руководство описывает типовую установку Mirage 2.0.1 с отдельными Control Plane (CP) и Data Plane (DP). Оно предназначено для системного администратора, имеющего доступ root или sudo к подготовленным Linux-серверам.

Установочный архив и инструкция должны относиться к Mirage 2.0.1. Не используйте команды из документации для других версий.

2 Схема и предварительные требования

- два Linux-сервера или виртуальные машины: CP и DP;
- постоянные адреса управления, настроенные DNS и синхронизация времени;
- сетевые интерфейсы или VLAN на DP для сегментов, где будут размещены ловушки;
- сетевой доступ между CP и DP по портам из таблицы ниже;
- архив Mirage 2.0.1 и контрольная сумма, полученная по отдельному доверенному каналу.

Таблица 1 - Сетевые соединения.

Источник	Получатель	Порт	Назначение
Администратор	CP	443/tcp	Веб-интерфейс
CP	DP	8443/tcp	LXD API
Ловушки	Relay на DP	9443/tcp	Передача телеметрии, если relay включён
DP	CP	443/tcp	Передача телеметрии
CP	Внешний сервис	По настройке	Интеграция с AD, SMTP или SIEM

Не открывайте PostgreSQL, Redis, backend-порт и LXD API в недоверенные сети. Ограничьте управление CP и DP административными сегментами.

3 Проверка и распаковка дистрибутива

Скопируйте один и тот же архив на оба сервера. Сверьте контрольную сумму с отдельным доверенным источником, затем распакуйте архив:

```
sha256sum mirage-installer-v2.0.1.tar.gz
mkdir -p /tmp/mirage-installer-v2.0.1
tar -xzf mirage-installer-v2.0.1.tar.gz -C /tmp/mirage-installer-v2.0.1
cd /tmp/mirage-installer-v2.0.1
```

В release bundle должна успешно пройти встроенная проверка подписи. При ошибке проверки остановите установку и запросите корректный архив.

4 Установка Data Plane

Сначала установите DP. Это позволит CP подключиться к готовому LXD API и использовать созданные сертификаты.

```
sudo bash install-mirage.sh
```

В меню выберите установку Data Plane и укажите параметры, запрошенные установщиком: management IP, адрес и порт будущего CP, интерфейсы и параметры сети ловушек, параметры relay, если он используется.

Не вводите адреса целевых сетей в качестве management-адреса. Не включайте интерфейс с default route в trap bridge без проверки схемы сети.

4.1 Проверка DP

```
sudo lxc version
sudo lxc image list
sudo lxc profile list
sudo ss -lntp | grep -E ":(8443|9443)\b"
sudo systemctl status mirage-relay --no-pager
sudo lxc config trust list
```

Сверьте установленные образы и профили с выбранной конфигурацией. Храните закрытый ключ клиентского сертификата с ограниченными правами и не передавайте его по незащищённому каналу.

5 Установка Control Plane

На CP распакуйте тот же bundle и запустите установщик:

```
sudo bash install-mirage.sh
```

Выберите Control Plane и укажите management IP CP и endpoint DP. Установщик создаёт каталог /opt/mirage, конфигурацию и Compose-стек.

5.1 Проверка CP

```
cd /opt/mirage
sudo systemctl status mirage --no-pager
sudo docker compose ps
curl -kSsi --fail https://127.0.0.1/api/v1/users/system/status
```

Для oneshot-службы mirage.service статус active (exited) может быть штатным. Проверяйте состояние контейнеров и ответ HTTP endpoint.

6 Регистрация Data Plane

В веб-интерфейсе откройте раздел Data Planes и добавьте DP. Укажите понятное имя, LXD endpoint вида https://<адрес-DP>:8443, пути к клиентскому сертификату и ключу в контейнере backend, и relay URL, если настроен relay.

После регистрации выполните предусмотренный интерфейсом выпуск relay token. Передайте его в окружение службы relay согласно инструкции релиза, ограничьте доступ к файлу и перезапустите службу. Не помещайте значение токена в этот документ.

7 Сети и профили ловушек

Создайте или проверьте LXD bridge и профиль для каждого целевого сегмента. Management-интерфейс, DNS и default route DP должны оставаться доступными после изменения сетевой конфигурации. Следуйте инструкции DP_NETWORK_PROFILE_SETUP.md для версии 2.0.1 и проверяйте bridge/profile командами LXD.

8 Первый вход и лицензия

Откройте HTTPS-адрес CP и загрузите файл лицензии на странице настройки лицензии. На странице первоначальной настройки создайте учётную запись администратора. Передайте пароль безопасно и не записывайте его в документацию или shell history.

9 Проверка установки

- CP endpoint отвечает по HTTPS; обязательные контейнеры работают;
- в интерфейсе отображается ожидаемая лицензия;
- DP доступен, его профили загружаются;
- тестовая ловушка получает ожидаемый адрес и отображается в состоянии running;
- heartbeat или иной доступный показатель состояния обновляется;
- контрольное обращение к тестовому сервису появляется в журнале событий;
- при включённой SIEM-интеграции контрольное событие поступает в выбранный канал.

10 Обновление и устранение ошибок

Перед обновлением прочитайте release notes и руководство RELEASE_AND_UPDATE.md версии назначения. Сделайте резервную копию данных и конфигурации согласно регламенту организации. Используйте только инструкции для установленной версии.

При ошибке сохраните вывод установщика, состояние контейнеров и соответствующие журналы. Не удаляйте базу данных, сертификаты, образы и каталог установки при разборе ошибки.

11 Передача сведений об ошибке

При обращении в поддержку укажите версию системы, время ошибки, номер задачи и приложите текст сообщения. Пароли, токены и закрытые ключи в обращение не включайте. Порядок и сроки поддержки определяются договором.