??????????????

- Обновление сертификатов Мониторинга и ПринтМенеджера
- Обновление сертификатов балансировщика
- Изменение пароля шифрования конфигурационного файла
- Настройка шифрованного соединения для Мониторинга, ПМ и клиента ПМ
- Настройка IPPS для МФУ
- Шифрование конфигурационного файла .env
- Подключение стороннего балансировщика к кластеру

??????????? ????????????? ??????????? ? ??????????????

????? ??????????

По окончании срока действия SSL-сертификатов их необходимо заменить.

????

По окончании срока действия сертификаты потребуется заменить. Для этого выполните обновление Мониторинга и ПринтМененджера с помощью разделов выше и добавьте в команды следующие ключи: SSL_CERT, SSL_KEY и SSL_CERT_CA с указанием новых файлов.

Например, онлайн обновление Мониторинга будет выглядеть так:

```
sudo curl -L https://s3.printum.io/box/monitoring/install.sh | sudo -E
SSL_CERT=/directory/cert.crt SSL_KEY=directory/cert.key SSL_CERT_CA=/directory/ca.crt  bash -s
agent
```

Где:

- `SSL_CERT` — полный путь до сертификата.
- `SSL_KEY` — полный путь до ключа.
- `SSL_CERT_CA` — полный путь до корневого сертификата.

??????????? ????????????? ??????????????????

????????

Обновление сертификатов в конфигурации с балансировщиком нагрузки (HAProxy). Сертификаты обновляются для всех компонентов: балансировщика, Мониторинга и каждого сервера ПМ.

??????????? ??????????? ???????????? (????? config.ini)

1. Укажите новые пути в конфигурационном файле `config.ini`:

```
Секция [General]

SSL_CERT_CA – полный путь до корневого сертификата (CA certificate).

Секция  [Balancer]

SSL_CERT – Полный путь до сертификата
SSL_KEY – Полный путь до ключа сертификата.

Секция [Monitoring]

SSL_CERT – Полный путь до сертификата
SSL_KEY – Полный путь до ключа сертификата.

Секции [PrintManager_1], [PrintManager_2], …, [PrintManager_N]

SSL_CERT – Полный путь до сертификата
SSL_KEY – Полный путь до ключа сертификата.
```

2. Запустите скрипт установки повторно:

```
sudo ./install_all_offline.sh
```

??????????? ??????????????? ???????????? (????????)

1. Удалите старые сертификаты на сервере балансировщика:

```
sudo rm -fr /opt/printum_balancer/certificates
```

2. Выпустите новый корневой сертификат:

```
sudo /opt/printum_balancer/scripts/generate_ca_cert.sh
```

3. Перегенерируйте сертификаты:

```
cd /opt/printum_balancer/scripts
sudo ./regenerate_all_certs.sh -balancer <BALANCER_ADR> -pm <PM_1> -pm <PM_2> -pm <PM_3>
```

4. Появится архив с новыми сертификатами. Повторите установку всех серверов ПринтМенеджер с новым архивом `printum_certs.tar.gz`.

Важно: необходимо переписать только `printum_certs.tar.gz`. При установке использовался printum_config.tar.gz - его устанавливать не нужно.

????????? ?????? ??????????? ?????????????????? ?????

????????

Смена пароля для шифрования файла `.env.enc` выполняется с помощью утилиты `env-vault`.

??? ???????????

1. Сбросьте переменную среды

   ```
   unset ENV_VAULT_PASSWORD
   ```

2. Запустите смену пароля

   ```
   env-vault rekey /opt/printum/.env.enc
   ```

3. Введите текущий пароль, затем новый дважды
4. После смены запустите систему с новым паролем:

   ```
   cd /opt/printum
   sudo -E ENV_VAULT_PASSWORD=<password> env-vault .env.enc docker-compose -- up -d
   ```

??? ??????????????

1. Сбросьте переменную среды

   ```
   unset ENV_VAULT_PASSWORD
   ```

2. Запустите смену пароля

   ```
   env-vault rekey /opt/printmanager/.env.enc
   ```

3. Введите текущий пароль, затем новый дважды
4. Перезапустите систему с новым паролем:

```
cd /opt/printmanager
sudo -E ENV_VAULT_PASSWORD=<password> env-vault .env.enc docker-compose -- up -d
```

?????

- После смены пароля все последующие операции (обновление, бекап, восстановление) должны выполняться с новым паролем.
- Сохраните новый пароль в надёжном месте.

????????? ???????????? ??????????? ??? ???????????, ?? ? ??????? ??

??????????

При установке системы автоматически создаётся самоподписанный SSL-сертификат, стандарта SHA-256 с длиной ключа шифрования RSA 2048 бит. Для работы мониторинга и управления печать в сети организации этого достаточно, но при необходимости (например, требования ИБ) допускается установка доверенного сертификата организации.

При необходимости используйте доверенный сертификат одного из типов:

- Сертификат, приобретённый или полученный у внешнего доверенного центра сертификации.
- Сертификат, выданный внутренним центром сертификации организации (Enterprise CA).

????????? HTTPS

Клиент ПринтМенеджера, отправляющий задания на печать с ПК пользователей, имеет параметр `verify_SSL_cert`, отвечающий за включение проверки сертификата безопасности. По умолчанию параметр установлен в `false`, т.е. проверка отключена.

Для включения проверки и обеспечения шифрованного соединения клиента ПМ с сервером ПринтМенеджера выполните настройки, описанные в разделах ниже, в соответствии с операционной системой на пользовательском АРМ.

????????? ???????? HTTPS-??????????? ??? ?????? ? Linux

Для корректной проверки сертификата и работы Клиента ПринтМенеджер по протоколу HTTPS выполните следующие действия:

1. Остановите службу Клиента ПМ:

```
sudo systemctl stop printum-printmanager-client.service
```

2. Откройте файл корневого сертификата, который подтверждает подлинность SSL-сертификата, используемого сервером ПМ. Скопируйте из него весь текст, вместе с `BEGIN`, `END` и дефисами.
3. Откройте с правами на редактирование файл:

```
/opt/printum/printmanager_client/venv/lib/python3.10/site-packages/certifi/cacert.pem
```

Для более ранних версий службы для Linux замените `python3.10` на `python3.8`.

4. В конец файла вставьте скопированное из шага 2 и сохраните файл.
5. Запустите службу Клиента ПМ:

```
sudo systemctl start printum-printmanager-client.service
```

????????? ???????? HTTPS-???????????? ??? ?????? ? Windows

1. Откройте файл корневого сертификата, который подтверждает подлинность SSL-сертификата, используемого сервером ПМ. Скопируйте из него весь текст, вместе с `BEGIN`, `END` и дефисами.
2. Откройте с правами на редактирование файл:

```
C:\Program Files\printum\printmanager_client\lib\certifi\cacert.pem
```

3. В конец файла вставьте скопированное из шага 1 и сохраните файл.
4. Перезапустите службу или перезагрузите компьютер.

??????????? ?????? ????? ????????????

Данные между пользователем и системой, а также между компонентами (Мониторинг и ПринтМенеджер) передаются по протоколу HTTPS.

Тип пароля	Метод	Описание

Пользовательские пароли (вход в систему)	PBKDF2	Хэширование с уникальной «солью» и несколькими десятками итераций
Пароли принтеров, доступа к каталогам и др.	AES CBC 128-bit + PKCS7	Шифрование с 128-битным ключом

?????????? ?????????

- Настройка IPPS для МФУ
- Обновление сертификатов Мониторинга и ПринтМенеджера
- Переменные .env Мониторинга

????????? IPPS ??? ???

??????????

IPPS (Internet Printing Protocol over SSL) обеспечивает шифрование при отправке заданий печати на МФУ. Настройка требуется при использовании отложенной печати с шифрованием или при требованиях ИБ к защите потока печати.

????????? IPPS ??? ??????????? ??????

1. Перейдите в раздел **«Серверы печати»** по адресу:

```
https://адрес_принтменеджера:8080/config/web/printserver/
```

2. Для всех используемых серверов печати установите галочку **«Использовать SSL»** и сохраните форму.

Для прямой печати через IPPS используйте Клиент ПМ со стандартными настройками — при стандартных настройках IPPS включён по умолчанию.

????????? ???????????? ??????????? ??? ??? ???????? ??????? ?? ??????

1. Убедитесь, что в настройках МФУ включён доступ с использованием SSL для IPP-соединений, а сертификат сервера загружен в МФУ (или проверка серверного сертификата на МФУ не требуется / выключена).
2. Перейдите в панель администратора ПринтМенеджера, во вкладку **«Настройки принтеров в CUPS»**.
3. Найдите нужный принтер и нажмите на него.
4. Установите адрес для защищённого подключения в соответствии с вендором:

Вендор	Адрес
Fplus	`https://{hostname}/ipp/print`
Lexmark	`https://{hostname}/ipp/print`
Xerox	`ipps://{hostname}/ipp`
Konica Minolta	`ipps://{hostname}/ipp`

Где `hostname` — доменное имя или IP-адрес МФУ.

5. Сохраните настройки. Обновление займёт до 1 минуты.

?????????? ?????????

- Настройка SSL для служб Мониторинга на Linux
- Обновление сертификатов Мониторинга и ПринтМенеджера

??????????? ??????????????????? ????? .env

????????

Принтум поддерживает шифрование конфигурационного файла `.env` с помощью переменной `ENV_VAULT_PASSWORD` и утилиты `env-vault`. При включённом шифровании файл хранится в зашифрованном виде (`.env.enc`), а все команды запуска системы требуют указания пароля.

?????????? ??????????? ??? ?????????? ???????????

Для активации шифрования при установке дополнительно задайте переменную `ENV_VAULT_PASSWORD`.

??????-??????????

По доменному имени:

```
sudo curl -L https://download.printum.io/box/monitoring/install.sh | sudo -E
MON_HOSTNAME=<hostname> ENV_VAULT_PASSWORD=<password> bash -s agent
```

По IP-адресу:

```
sudo curl -L https://download.printum.io/box/monitoring/install.sh | sudo -E IP_ADDRESS=<ip>
ENV_VAULT_PASSWORD=<password> bash -s agent
```

??????-??????????

По доменному имени:

```
sudo MON_HOSTNAME=<hostname> ENV_VAULT_PASSWORD=<password> -E ./install.sh agent
```

По IP-адресу:

```
sudo IP_ADDRESS=<ip> ENV_VAULT_PASSWORD=<password> -E ./install.sh agent
```

В процессе установки необходимо будет повторно ввести пароль.

?????????? ??????????? ??? ?????????? ??????????????

Онлайн-установка:

```
sudo curl -L https://s3.printum.io/distrib/printum-printmanager/install.sh | sudo -E
PM_HOSTNAME=<ip> ENV_VAULT_PASSWORD=<password> bash
```

Офлайн-установка:

```
sudo PM_HOSTNAME=<ip> ENV_VAULT_PASSWORD=<password> -E ./install.sh
```

Без указания переменной `ENV_VAULT_PASSWORD` установка ПринтМенеджера на зашифрованный сервер мониторинга невозможна.

?????????? ????????? ??????????? ? ????????????? .env ?????

??? ???????????

1. Перейдите в каталог установки:

```
cd /opt/printum
```

2. Остановите контейнеры:

```
sudo -E ENV_VAULT_PASSWORD=<password> env-vault .env.enc docker-compose down
```

3. Откройте зашифрованный файл для редактирования:

```
sudo -E ENV_VAULT_PASSWORD=<password> env-vault edit .env.enc
```

Откроется системный редактор по умолчанию (например, vim). Внесите изменения и сохраните файл (в vim: введите `:wq`).

4. Перезапустите контейнеры:

```
cd /opt/printum
sudo -E ENV_VAULT_PASSWORD=<password> env-vault .env.enc docker-compose -- up -d
```

??? ??????????????

Следуйте аналогичной инструкции, заменяя путь к каталогу:

```
cd /opt/printmanager
```

????? ?????? ??????????

??? ??????????

1. Сбросьте переменную среды:

```
unset ENV_VAULT_PASSWORD
```

2. Запустите процесс смены пароля:

```
env-vault rekey /opt/printum/.env.enc
```

3. Введите текущий пароль, затем новый пароль дважды для подтверждения.
4. После смены пароля запустите систему с новым паролем:

```
cd /opt/printum
sudo -E ENV_VAULT_PASSWORD=<password> env-vault .env.enc docker-compose -- up -d
```

??? ??????????????

1. Сбросьте переменную среды:

```
unset ENV_VAULT_PASSWORD
```

2. Запустите процесс смены пароля:

```
env-vault rekey /opt/printmanager/.env.enc
```

3. Введите текущий пароль, затем новый пароль дважды для подтверждения.
4. Перезапустите систему с новым паролем:

```
cd /opt/printmanager
sudo -E ENV_VAULT_PASSWORD=<password> env-vault .env.enc docker-compose -- up -d
```

?????????? ??????????? ??? ??????????

При создании резервной копии на зашифрованной системе необходимо передавать пароль:

Для Мониторинга:

```
sudo -E ENV_VAULT_PASSWORD=<password> /opt/printum/backup.sh /home/user/backup
```

Для ПринтМенеджера:

```
sudo -E ENV_VAULT_PASSWORD=<password> /opt/printmanager/backup.sh /home/user/backup
```

При отсутствии указания переменной `ENV_VAULT_PASSWORD` резервная копия может быть создана некорректно.

??????????

- Для работы с шифрованными файлами необходимо наличие утилиты `env-vault` на сервере.
- При работе с конфигурационными файлами рекомендуется заранее создать резервную копию.

?????????? ?????????

- Переменные .env Мониторинга
- Переменные .env ПринтМенеджера
- Резервное копирование при шифровании конфигурационного файла
- Изменение пароля шифрования конфигурационного файла

??????????? ??????????? ??????????????? ? ????????

??????????? ??????????? ??????????????

По умолчанию система использует HAProxy для балансировки нагрузки. Рекомендуется использовать его в качестве балансировщика нагрузки, так как именно с ним система проходит все этапы тестирования и по умолчанию используется при установке у клиентов. Однако, если необходимо использовать сторонний балансировщик, выполните настройку в соответствии с этой инструкцией.

Важно: При использовании сторонних балансировщиков испытания системы на совместимость не проводились. Мы не можем гарантировать стабильную и бесперебойную работу системы с другими решениями. Использование сторонних балансировщиков осуществляется под вашу ответственность.

Перед началом убедитесь, что ознакомились с разделом "Подготовка к установке кластера Active-Active". Этот раздел актуален для настройки любого балансировщика.

?????????? ? ?????????? ?????????????

1. **Проксирование сообщений**: балансировщик должен корректно обрабатывать следующие типы соединений:
   - **FTP-соединения**: порты 20–21 и 30000–30199.
   - **HTTP-соединения**: порты 1631, 8010, 8080.
   - **WebSocket-соединения** (при использовании TCP-конвертера): порты 7776, 7777.

   Если стандартные порты изменены при установке ПМ, укажите новые значения.
2. **Проверка доступности (healthcheck)**:
   - Балансировщик должен выполнять HTTP-запросы на адрес `/health/`.
   - Если ответ имеет статус **200**, сервер считается исправным. Любой другой ответ означает неисправность.
   - Настройте механизм оповещений о сбоях серверов, доступный в вашем балансировщике.
3. **Параметры настройки**:
   - Используйте алгоритм **Round Robin** с включением **Sticky Session**.

- Настройки таймаутов:
  - **Таймаут сервера (timeout server)**: 30 секунд.
  - **Таймаут клиента (timeout client)**: 30 секунд.
  - **Таймаут соединения (timeout connection)**: 5 секунд.
- **Повторы (retries)**: не требуются.
- Используйте сгенерированные SSL-сертификаты для балансировщика.

После подготовки настроек установите ваш балансировщик.

????????? ? ????????? ????????????????

????? ?????????? ??????? ?????????????

Выполните команды для экспорта переменных окружения:

```
export NFS_ADDR=<NFS_ADDR>
export NFS_PATH=<NFS_FOLDER_PATH>
export
DATABASE_URL=postgres://<POSTGRES_LOGIN>:<POSTGRES_PASSWORD>@<DB_HOST>:<PORT>/<BASE_NAME>
```

Или с указанием конкретной схемы базы данных:

```
export 
DATABASE_URL=postgres://<POSTGRES_LOGIN>:<POSTGRES_PASSWORD>@<DB_HOST>:<PORT>/<BASE_NAME>?curr
entSchema=<POSTGRES_SCHEMA>
```

Если используется табличное пространство, то добавьте команду:

```
export DATABASE_TABLESPACE=<DATABASE_TABLESPACE>
```

Укажите настройки Redis и других сервисов (эти команды обязательны):

```
export REDIS_ROLE=master
export REDIS_SENTINEL_LIST=<IP_1>,<IP_2>,<IP_3>
export REDIS_MASTER_IP=<IP_1>
export PM_HOSTNAME=<IP_1>
export DRIVER_OPTS_TYPE="nfs"
export DRIVER_OPTS_O="addr=<NFS_ADDR>,nolock,soft,rw"
export DRIVER_OPTS_DEVICE=":/scratch"
export EXT_HOSTNAME=<IP_BALANCER>
export REDIS_PASSWORD=<REDIS_PASSWORD>
export CUPS_PASSWORD=<CUPS_PASSWORD>
```

```
export FTPD_PASSWORD=<FTPD_PASSWORD>
export WEBDAV_PASSWORD=<WEBDAV_PASSWORD>
```

Где:

- **<NFS_ADDR>**: IP-адрес или доменное имя сервера NFS.
- **<NFS_FOLDER_PATH>**: путь к директории NFS.
- **<POSTGRES_LOGIN>, <POSTGRES_PASSWORD>, <POSTGRES_SCHEMA>**: данные для подключения к базе.
- **<IP_1>, <IP_2>, <IP_3>**: IP-адреса серверов ПринтМенеджера.
- **<IP_BALANCER>**: IP-адрес балансировщика.

Важно: Оставайтесь в этом же терминале до завершения установки, иначе переменные окружения будут потеряны.

Запустите установку первого ПринтМенеджера.

????????? ??????? ? ??????????? ??????????????

Повторите команды экспорта переменных окружения, изменив:

```
export REDIS_ROLE=slave
export PM_HOSTNAME=<IP>
```

Где **<IP>** — IP-адрес устанавливаемого сервера.

Запустите установку.

???????? ???????????? ?????????

1. Проверьте систему по "Чек-листу для проверки корректной установки".
2. Исключите проверки, связанные с настройкой HAProxy.
3. Добавьте собственные проверки, актуальные для вашего балансировщика.