

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

- [Восстановление из резервной копии](#)
- [Восстановление при шифровании конфигурационного файла](#)
- [Восстановление Принтум из резервной копии](#)
- [Сценарии аварийного восстановления](#)
- [Проверка резервных копий](#)
- [Откат после неудачного обновления](#)

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

Предусловия Чистый сервер с той же ОС IP-адрес или доменное имя совпадают с адресом на момент создания копии Свободное место  $\geq$  размер архива резервной копии Шаги  
Переместите архив на целевой сервер. Разархивируйте: `tar xzvf printum_backup_date-month-day_hour-minute.tar.gz` Запустите восстановление: `sudo printum_backup_date-month-day_hour-minute/restore.sh` Результат После успешного восстановления выводится: `Restoration complete` Подождите несколько минут для запуска системы. Проверка Корректность отображения данных МФУ в ЛК. Загрузка страниц технических кабинетов Мониторинга и ПринтМенеджер. Работа печати, копирования и сканирования. Очистка `sudo rm -f printum_backup_date-month-day_hour-minute.tar.gz` `sudo rm -fr printum_backup_date-month-day_hour-minute` Ограничения при восстановлении Восстановление возможно только при соблюдении следующих требований. Нарушение любого из них может привести к неработоспособности системы после восстановления. Требование Причина Та же ОС и версия Совместимость Docker и системных компонентов Тот же hostname Внутренние ссылки и сертификаты Тот же IP или FQDN Синхронизация между компонентами Восстановление выполняется только на чистый сервер. Требования к серверу описаны в руководстве администратора.

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

???????????

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

??????????

Если конфигурационный файл зашифрован, восстановление должно выполняться с указанием пароля шифрования.

?????

Вместо стандартной команды восстановления используйте:

```
sudo -E ENV_VAULT_PASSWORD=<password> printum_backup_date-month-day_hour-minute/restore.sh
```

Где `<password>` — пароль шифрования, использованный при установке системы.

?????

Указание правильного пароля критически важно для успешного восстановления зашифрованных данных. При неверном пароле восстановление завершится с ошибкой.

??????????

- Вывод `Restoration complete` в терминале.
- Работоспособность всех компонентов системы.

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

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

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

Инструкция описывает порядок восстановления Принтум после отказа серверов, повреждения инфраструктуры, потери данных или критических инцидентов.

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

- Отказ NFS, HAProxy, Мониторинга или одного сервера ПринтМенеджера;
- Повреждение PostgreSQL;
- Потеря NFS;
- Повреждение Docker volumes;
- Критический отказ системы (2 и более серверов).

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

Все серверы должны восстанавливаться из резервных копий, созданных в один временной интервал. Несогласованные копии могут привести к потере синхронизации, повреждению статистики и ошибкам очередей.

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

Восстановление выполняется строго по следующему порядку:

1. Сервер Мониторинга
2. Сервер базы данных ПринтМенеджера
3. Сервер NFS-хранилища ПринтМенеджера
4. Сервер балансировщика HAProxy
5. Сервер ПринтМенеджера №1
6. Сервер ПринтМенеджера №2
7. Сервер ПринтМенеджера №3
8. Сервер ПринтМенеджера №N

## ??? 1. ????????????

Сначала восстанавливается сервер Мониторинга — он используется как центральная конфигурация, источник пользователей и устройств.

## ??? 2. ??????? ???????

Восстановить PostgreSQL. Проверить: запуск сервиса, доступность порта, корректность данных. При отказе сервера базы данных после восстановления — перезапустить все сервисы СУП на серверах ПринтМенеджера.

## ??? 3. NFS-??????????

Восстановить NFS storage и stunnel. Проверить: export, mount, доступность volumes.

## ??? 4. HAProxy

Восстановить балансировщик. Проверить: healthcheck, backend status, routing.

## ??? 5. ????????? ???????????????????

Восстановить все ноды ПринтМенеджера. После запуска:

```
cd /opt/printmanager
docker-compose down
docker-compose up -d
```

Проверить sync и очереди.

??

??

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

Проверить доступность: Личного кабинета, панелей администратора, Встроенных приложений на МФУ.

# ????????? ?????????? HAProxy

Убедиться, что статусы всех компонентов в панели администратора HAProxy — ярко-зелёные.

## ????????? Docker-?????????????????

На всех серверах Мониторинга и ПринтМенеджера:

```
docker ps
```

Проверить: нет restart loop, нет exited containers, нет unhealthy status.

## ???????????? ??????????????????

Проверить авторизацию пользователей в Личном кабинете и Встроенных приложениях на МФУ, а также LDAP/SSO и RFID-авторизацию.

## ???????????? ??????????????????????

Проверить доменную синхронизацию в Мониторинге. Проверить синхронизацию данных Мониторинга и ПринтМенеджера.

## ???????????? ??????????

Проверить: direct print, release print, queue processing, статистику, копирование и сканирование во Встроенных приложениях.

## ???????????? ??????????????????

Симптом	Возможная причина
ПринтМенеджер не запускается	NFS
Нет синхронизации	Мониторинг
Контейнеры unhealthy	PostgreSQL
Нет печати	HAProxy
Нет статистики	sync queue

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

- Порядок восстановления критически важен.
- NFS и PostgreSQL — ключевые зависимости.
- После восстановления требуется проверка синхронизации.
- После аварии статистика может догружаться постепенно.

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

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

Сценарии аварийного восстановления Назначение Описание типовых сценариев аварийного восстановления системы Printum: симптомы, порядок действий и ориентировочное время восстановления. Сценарий 1 — Отказ одного сервера ПринтМенеджера в кластере  
Симптомы Страница состояния HAProxy показывает один или несколько узлов как «DOWN». Часть заданий не обрабатывается; пользователи не замечают сбоя (если узлов  $\geq 2$ ). Порядок действий Проверить статус контейнеров на отказавшем сервере: `cd /opt/printmanager && docker-compose ps` Изучить логи: `docker-compose logs --tail=200` Перезапустить контейнеры: `docker-compose restart` Если не помогает — восстановить из резервной копии (см. «Восстановление из резервной копии»). После восстановления проверить страницу состояния HAProxy. Ориентировочное время: 15–30 минут при перезапуске; 60–120 минут при восстановлении из резервной копии. Сценарий 2 — Отказ нескольких серверов ПринтМенеджера  
Симптомы Большинство заданий не обрабатываются. HAProxy показывает менее половины узлов в статусе «UP» (кластер утратил кворум). Порядок действий Восстановить наибольшее число серверов ПринтМенеджер (перезапуск контейнеров или восстановление из резервной копии). Убедиться, что активно  $\geq (N/2 + 1)$  узлов (кворум), где N — общее число узлов. Проверить статус HAProxy и синхронизацию с Мониторингом. Ориентировочное время: 60–240 минут в зависимости от числа отказавших узлов. Сценарий 3 — Потеря базы данных PostgreSQL  
Симптомы Ошибки в логах ПринтМенеджер: `django.db.utils.OperationalError: connection to server failed` Веб-интерфейс Личного кабинета недоступен или отображает ошибки. Порядок действий Убедиться, что контейнер PostgreSQL запущен: `sudo docker ps | grep postgres` Если контейнер упал — перезапустить: `docker-compose up -d db` Если данные повреждены — восстановить базу из резервной копии. Для восстановления на чистый сервер выполнить команды (см. «Восстановление из резервной копии»): `sudo tar xzvf printum_backup_.tar.gz sudo printum_backup/_restore.sh` Подождать несколько минут для запуска системы. Ориентировочное время: 30–120 минут в зависимости от объёма данных. Важно: IP-адрес или hostname сервера должны совпадать с теми, что были при создании резервной копии. Сценарий 4 — Потеря NFS-хранилища (кластер)  
Симптомы Пользователи при попытке печати получают ошибку «Файл недоступен». Логи ПринтМенеджер содержат ошибки обращения к NFS-директории. Порядок действий Проверить доступность NFS-сервера с сервера ПринтМенеджер: попробовать смонтировать папку вручную. Убедиться в правильности параметров в `/opt/printmanager/.env`: `sudo cat /opt/printmanager/.env` Проверить `DRIVER_OPTS_DEVICE`, `DRIVER_OPTS_O`, `DRIVER_OPTS_TYPE`. После восстановления NFS перезапустить контейнеры: `docker-compose restart` Проверить, что задания в отложенной очереди обрабатываются. Ориентировочное время: 15–60 минут. Связанные страницы Восстановление из резервной копии Проверка резервных копий Резервное копирование — обзор

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

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

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

Регулярная проверка резервных копий гарантирует, что при аварии восстановление пройдет успешно. Проверку рекомендуется выполнять после каждого создания резервной копии и перед крупными обновлениями.

---

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

?????????

1. Убедиться, что файл резервной копии существует в указанном хранилище.
2. Проверить, что архив не повреждён (размер ненулевой и соответствует ожидаемому).
3. Распаковать архив вручную для проверки содержимого:

```
sudo tar tzvf printum_backup_<date>.tar.gz | head -50
```

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

1. Подготовить тестовый сервер с теми же IP-адресом/hostname, что и у рабочего сервера.
2. Перенести архив резервной копии на тестовый сервер.
3. Распаковать архив и запустить восстановление:

```
sudo tar xzvf printum_backup_<date>.tar.gz  
sudo printum_backup_<date>/restore.sh
```

4. После сообщения «**Restoration complete**» подождать несколько минут.
5. Проверить работоспособность системы:
  - Открыть Личный кабинет — страница должна загружаться.

- Проверить отображение устройств и пользователей.
- Выполнить тестовую печать (при возможности).

6. После проверки удалить тестовые данные:

```
sudo rm -f printum_backup_<date>.tar.gz  
sudo rm -fr printum_backup_<date>
```

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

Если используется шифрование .env, создание копии выполняется с паролем:

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

Восстановление — также с паролем:

```
sudo -E ENV_VAULT_PASSWORD=<password> printum_backup_<date>/restore.sh
```

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

- Система Мониторинга (переменные .env и базы данных)
- Система ПринтМенеджера (переменные .env и базы данных)
- Сетевой агент (конфигурация)
- Установочные пакеты

**Не копируется:** Локальный агент мониторинга.

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

- [Резервное копирование — обзор](#)
- [Создание резервной копии](#)
- [Восстановление из резервной копии](#)
- [Сценарии аварийного восстановления](#)

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

???????????

Откат после неудачного обновления Назначение Инструкция по откату системы Printum к предыдущей версии при сбое обновления. Когда выполнять откат После обновления система не запускается или недоступен Личный кабинет. Критичные функции не работают (печать, авторизация, отображение устройств). Ошибки в логах контейнеров, которые не удаётся устранить за разумное время. Обновление прервалось — контейнеры в нестабильном состоянии. Предварительная проверка Перед откатом убедитесь: Резервная копия была создана до обновления. Версии Мониторинга и ПринтМенеджер, которые были до обновления, известны: `cat /opt/printum/.version` `cat /opt/printmanager/.version` Резервная копия доступна и не повреждена. Порядок отката Остановить текущие контейнеры: `cd /opt/printum && sudo docker-compose down` `cd /opt/printmanager && sudo docker-compose down` Перенести резервную копию на сервер (если хранится внешне). Распаковать архив и запустить восстановление: `sudo tar xzvf printum_backup.tar.gz` `sudo printum_backup/restore.sh` Подождать сообщение «Restoration complete» . Подождать несколько минут для запуска системы. Проверить работоспособность: открыть Личный кабинет, проверить устройства и пользователей. Что проверить после отката Версию компонентов: `cat /opt/printum/.version` и `cat /opt/printmanager/.version` — должны показывать предыдущую версию. Статус контейнеров: `docker-compose ps` — все контейнеры должны быть Up. Логи: `docker-compose logs --tail=100` — не должно быть критических ошибок. Доступность Личного кабинета по URL. Тестовую печать (при возможности). Особенности при шифровании конфигурационного файла При восстановлении с шифрованием использовать команду: `sudo -E ENV_VAULT_PASSWORD= printum_backup/restore.sh` Связанные страницы Создание резервной копии Восстановление из резервной копии Проверка резервных копий Сценарии аварийного восстановления