??????????

- Rootless режим контейнера
- Отсутствие SUID-SGID файлов и утилит повышения привилегий
- Соответствие рекомендациям CIS Benchmark
- Фиксированные теги контейнерных образов
- Хранение секретов в контейнерных образах

Rootless ????? ???????????

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Основные контейнеры Printum запускаются от непривилегированных пользователей и не требуют запуска процессов внутри контейнера от root. Поддержка rootless-режима контейнерного рантайма зависит от используемой инфраструктуры.

???????????

Контейнеры не должны запускать прикладные процессы с привилегиями суперпользователя без необходимости.

Использование непривилегированных пользователей снижает риск повышения привилегий и ограничивает последствия компрометации контейнера.

??? ??? ???????????? ? Printum

Основные контейнерные образы Printum используют непривилегированных пользователей для запуска сервисов.

Базовые образы создают пользователя **printum** с идентификатором пользователя, отличным от root. В Dockerfile компонентов явно задаётся запуск процессов от непривилегированного пользователя:

- Мониторинг — пользователь printum;
- ПринтМенеджер — пользователь printum;
- File Server ПринтМенеджера — пользователь printum;
- Nginx ПринтМенеджера — пользователь nginx;
- PostgreSQL — пользователь postgres.

Для доступа к подсистеме печати пользователь printum в контейнерах ПринтМенеджера дополнительно включается в группу lp.

Базовые инфраструктурные образы Printum используют rootless-варианты образов, включая PostgreSQL, ClickHouse, Redis и Nginx.

Контейнеры Printum не требуют запуска в privileged-режиме. Дополнительные Linux capabilities через cap_add не используются.

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

Использование rootless-режима контейнерного рантайма определяется используемой инфраструктурой и средствами контейнеризации заказчика.

При необходимости эксплуатации в режиме Podman Rootless или аналогичных сценариях настройка контейнерного рантайма выполняется администраторами инфраструктуры заказчика.

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

В текущей версии отдельные служебные компоненты (CUPS и Mailcatcher) используют образы, для которых rootless-варианты ещё не реализованы.

Для основных компонентов Printum запуск процессов от непривилегированных пользователей обеспечивается штатно.

?????????? SUID-SGID ?????? ? ?????? ?????????? ??????????

Зона ответственности: Printum

Коротко: Контейнерные образы Printum не содержат файлов с установленными битами SUID/SGID и не включают утилиты повышения привилегий, позволяющие получить дополнительные права внутри контейнера.

??????????

Контейнерные образы не должны содержать механизмы, позволяющие повысить привилегии процесса или пользователя внутри контейнера.

Удаление SUID/SGID-файлов и утилит повышения привилегий снижает риск несанкционированного получения дополнительных полномочий при компрометации контейнера.

??? ??? ??????????? ? Printum

При сборке производственных контейнерных образов Printum выполняется удаление файлов с установленными битами SUID и SGID.

Аналогичная обработка применяется для основных компонентов системы:

- Мониторинг;
- ПринтМенеджер;
- File Server ПринтМенеджера;
- CUPS.

Дополнительно из образов удаляются утилиты повышения привилегий, включая su.

Такой подход исключает использование механизмов повышения привилегий через SUID/SGID-бинарники и ограничивает возможности получения дополнительных прав внутри контейнера.

Удаление выполняется на этапе сборки образов и входит в стандартный процесс подготовки production-версий контейнеров.

??? ????????????? Printum

Printum обеспечивает:

- отсутствие файлов с установленными битами SUID и SGID в производственных образах;
- отсутствие утилит повышения привилегий;
- соответствие принципу минимально необходимых привилегий для контейнерных компонентов.

?????????? ?????????? CIS Benchmark

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum реализует ряд рекомендаций CIS Benchmark для контейнерных сред, включая использование непривилегированных пользователей, удаление SUID/SGID-файлов, применение профилей безопасности SELinux и отказ от хранения секретов внутри контейнерных образов.

??????????

Контейнерная платформа должна соответствовать рекомендациям по безопасной настройке и эксплуатации контейнерных сред.

Рекомендации CIS Benchmark направлены на снижение рисков компрометации контейнеров, ограничения привилегий процессов и обеспечение безопасного развёртывания приложений.

??? ??? ????????? ? Printum

В составе контейнерной платформы Printum реализованы следующие меры безопасности:

- использование непривилегированных пользователей внутри контейнеров;
- отказ от запуска контейнеров в privileged-режиме;
- отсутствие дополнительных Linux capabilities через cap_add;
- удаление SUID/SGID-файлов и утилит повышения привилегий;
- применение профилей безопасности SELinux;
- отсутствие встроенных секретов, паролей и токенов в контейнерных образах;
- использование фиксированных версий контейнерных образов.

Подробная информация приведена в соответствующих статьях раздела «Контейнеры».

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

Часть рекомендаций CIS Benchmark относится к настройке контейнерной платформы и инфраструктуры заказчика.

К таким настройкам относятся:

- параметры контейнерного рантайма;
- ограничения CPU и памяти;
- использование read-only файловых систем контейнеров;
- аудит операционной системы;
- сканирование контейнерных образов;
- настройки оркестратора контейнеров.

Настройка указанных механизмов выполняется администраторами инфраструктуры заказчика.

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum использует контейнерные образы с фиксированными версиями компонентов. Теги latest для production-образов не используются.

??????????

Контейнерные образы должны использовать фиксированные версии компонентов, обеспечивающие воспроизводимость развёртывания и возможность контроля изменений между версиями.

Использование фиксированных тегов позволяет исключить непредсказуемое изменение состава программного обеспечения при повторном развёртывании системы.

??? ??? ???????????? ? Printum

Production-образы Printum собираются на основе контейнерных образов с фиксированными версиями.

Для основных компонентов используются версии, явно указанные в Dockerfile и конфигурации сборки.

Контейнерные образы публикуются с версионными тегами, позволяющими однозначно определить используемую версию программного обеспечения.

Фиксация версий обеспечивает воспроизводимость сборок и упрощает контроль изменений при обновлении системы.

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

Размещение контейнерных образов во внутреннем реестре организации, включая Nexus или иные корпоративные registry, определяется требованиями и политиками заказчика.

Организация хранения, репликации и контроля доступа к реестру контейнерных образов выполняется средствами инфраструктуры заказчика.

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

Зона ответственности: Printum

Коротко: Контейнерные образы Printum не содержат встроенных паролей, токенов, ключей API и других аутентификационных данных. Конфиденциальные параметры передаются в контейнеры во время запуска через переменные окружения.

??????????

Контейнерные образы не должны содержать аутентификационные данные, токены доступа, пароли и иные секреты в открытом виде.

Секреты должны передаваться в приложение отдельно от образа контейнера и не входить в состав публикуемых артефактов.

??? ??? ???????????? ? Printum

Production-образы Мониторинга и ПринтМенеджера не содержат встроенных паролей, токенов, ключей API и иных аутентификационных данных.

При сборке образов в них не копируются файлы конфигурации, содержащие секреты, включая файлы переменных окружения и ключи доступа.

Конфиденциальные параметры передаются контейнерам во время запуска через переменные окружения, определяемые в файлах конфигурации развертывания.

Для production-развертывания используются файлы .env, подключаемые средствами контейнерной платформы. В образах отсутствуют встроенные значения паролей баз данных, токенов интеграций и иных учётных данных.

Контейнерные образы публикуются отдельно от конфигурации конкретного заказчика и могут использоваться в различных инсталляциях без хранения индивидуальных секретов внутри образа.

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

Управление секретами, защита файлов конфигурации и контроль доступа к переменным окружения выполняются средствами инфраструктуры заказчика.

Конкретный способ хранения и передачи секретов определяется правилами эксплуатации и требованиями информационной безопасности организации.