

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.
