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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum поддерживает работу в средах, использующих мандатное управление доступом на базе SELinux. Ограничения доступа процессов реализуются средствами операционной системы и профилей безопасности.

??????????

Система должна обеспечивать возможность эксплуатации в средах, использующих мандатное управление доступом.

Мандатное управление доступом позволяет ограничивать действия процессов независимо от полномочий пользователя и предотвращать выполнение несанкционированных операций.

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

Поддержка мандатного управления доступом реализуется за счёт использования SELinux и специализированных профилей безопасности для компонентов Printum.

При использовании SELinux в режиме Enforcing процессы Мониторинга, ПринтМенеджера и Агентов работают в соответствии с установленными политиками безопасности и могут выполнять только разрешённые действия.

Ограничения доступа определяются профилями безопасности и контролируются средствами операционной системы.

Такой подход позволяет реализовать принцип:

> “ запрещено всё, что явно не разрешено политикой безопасности.

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

Для использования мандатного управления доступом необходимо:

- использовать операционную систему с поддержкой SELinux;
- включить SELinux;
- установить профили безопасности Printum;
- использовать режим Enforcing.

Настройка и сопровождение SELinux выполняются администраторами инфраструктуры заказчика.

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

Мандатное управление доступом обеспечивается средствами операционной системы и не функционирует при отключённом SELinux.

Revision #1
Created 2026-06-08 19:38:56 UTC by DD
Updated 2026-06-08 19:38:56 UTC by DD