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

- Мандатное управление доступом
- Профили безопасности

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

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.

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum поддерживает использование профилей безопасности SELinux для ограничения доступа компонентов системы к ресурсам операционной системы. Профили поставляются отдельно и предназначены для эксплуатации в инфраструктурах с повышенными требованиями информационной безопасности.

??????????

Система должна обеспечивать возможность ограничения доступа процессов к ресурсам операционной системы и выполнять только разрешённые действия.

Применение профилей безопасности позволяет снизить последствия ошибок конфигурации, эксплуатации уязвимостей и компрометации отдельных компонентов системы.

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

Для эксплуатации в защищённых контурах поставляются профили безопасности на базе SELinux.

Профили реализованы в виде SELinux-модулей и обеспечивают контроль доступа компонентов Printum к ресурсам операционной системы.

В комплект поставки входят следующие SELinux-модули:

- **printum_global** — общие правила безопасности для Мониторинга и ПринтМенеджера;
- **printum_agent** — профиль Агента Мониторинга;
- **printum_m_install** — профиль установки, обновления и восстановления Мониторинга;
- **printum_pm_install** — профиль установки, обновления и восстановления ПринтМенеджера.

Профили устанавливаются до развёртывания системы и применяются средствами SELinux.

Работа профилей предполагает использование режима SELinux Enforcing, при котором разрешены только действия, явно предусмотренные политиками безопасности.

Профили реализуют принцип минимально необходимых привилегий: компонентам Printum предоставляется доступ только к тем ресурсам операционной системы, которые требуются для их работы.

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

Для использования профилей безопасности необходимо:

- использовать операционную систему с поддержкой SELinux;
- включить SELinux;
- использовать режим Enforcing.

Установка и сопровождение профилей выполняются администраторами инфраструктуры заказчика.