Российская сервисная платформа виртуализации РУСТЭК

Руководство по работе с vTPM

Релиз 2.6.2

2024

Виртуальный Trusted Platform Module (vTPM) является своеобразным генератором и одновременно хранилищем ключей шифрования, использующихся в работе систем защиты данных.

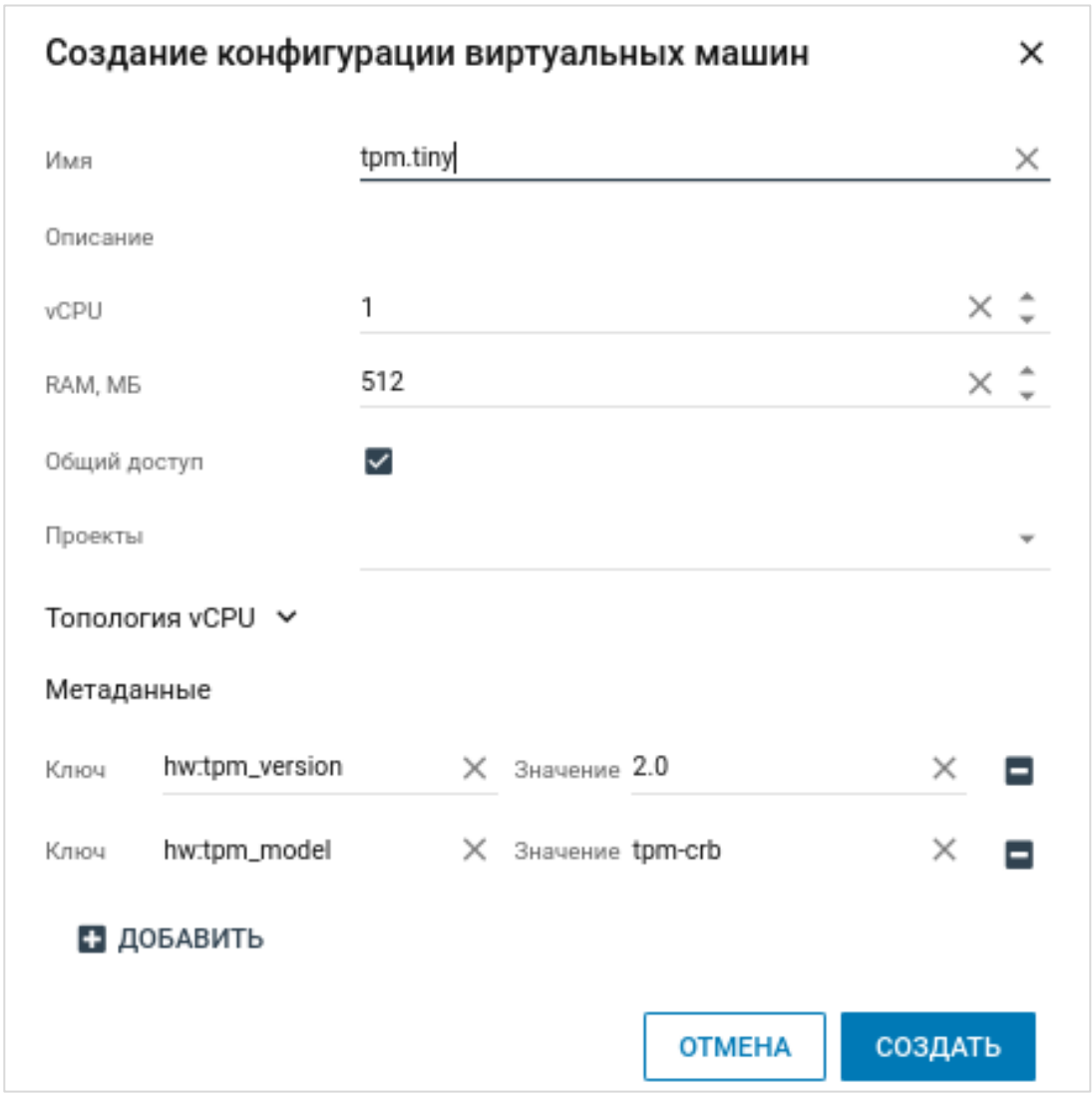
1. Включение

Для активации vTPM в РУСТЭК.Конфигураторе минимум на 1 узле включите роль "Служба хранения ключей шифрования" и примените конфигурацию. После этого на всех вычислительных узлах появится возможность запускать ВМ с vTPM.

2. Создание конфигурации

При создании конфигурации для поддержки TPM на ВМ укажите метаданные:

- hw:tpm_version – версия TPM: 1.2 или 2.0;
- hw:tpm_model – модель TPM: tpm-tis (по умолчанию) или tpm-crb (только для версии 2.0).



3. Проверка

При создании ВМ выберите конфигурацию с поддержкой TPM как описано выше. Дальше, например, в ОС Linux после загрузки в директории `/dev` будет устройство `/dev/tpm0`.

4. Использование с различными ОС

Для ОС windows 11 и новее использование TPM обязательно. Для установки выберите конфигурацию с tpm_version – 2.0, так как 1.2 windows 11 не поддерживает.

5. Ограничения

- Поддерживаются только операции сервера, выполняемые его владельцем, поскольку для разблокировки файлов виртуального устройства на хосте необходимы учетные данные пользователя. Администратор может предоставить пользователю дополнительные роли политики; в противном случае эти операции фактически отключаются.
- Динамическая миграция, эвакуация, хранение и восстановление серверов с vTPM в настоящее время не поддерживаются.

6. Безопасность

Эмулируемый TPM – это файл на диске, который libvirt должен иметь возможность предоставить гостю. В состоянии покоя этот файл зашифрован с использованием парольной фразы, хранящейся в службе диспетчера ключей. Парольная фраза в диспетчере ключей связана с учетными данными владельца сервера – пользователя, который его изначально создал. Кодовая фраза извлекается и используется libvirt для разблокировки эмулируемых данных TPM при каждой загрузке сервера.

Подробнее: https://docs.openstack.org/nova/latest/admin/emulated-tpm.html