



РУСТЭК.VDI

Функциональные возможности

Релиз 4.1

2024

Оглавление

1. Введение	3
2. Общий функционал	4
3. Функционал клиента РУСТЭК.VDI	5
4. Функционал панели управления.....	6
5. Функционал, связанный с защитой информации от несанкционированного доступа	7

Список сокращений и терминов приведён в общем для всех документов **Глоссарии**

1. Введение

Программный комплекс **РУСТЭК.VDI** (*Virtual Desktop Infrastructure*) – продукт компании ООО «РУСТЭК» (<https://rustack.ru/rustack-vdi>). Представляет собой комплекс серверных и клиентских программных решений для создания и управления инфраструктурой виртуальных рабочих мест.

Функционал программного комплекса позволяет разворачивать полноценные виртуальные рабочие места.

РУСТЭК.VDI может использоваться как для построения небольших инсталляций до 200 виртуальных рабочих мест (3 хоста), так и для больших VDI сред (2 000 – 10 000 виртуальных рабочих мест), гарантируя стабильную работу пользовательских подключений.

РУСТЭК.VDI может быть развернут на виртуальной машине или на серверах архитектуры x86_64.

2. Общий функционал

1. Создание и управление виртуальными рабочими местами (далее BPM).
2. Управление публикацией рабочих столов и приложений на основании членства пользователей в группах безопасности Active Directory/Open LDAP/eDirectory.
3. Масштабирование без остановки работы платформы.
4. Централизованное распространение настроек на все виртуальные машины (далее VM) и все терминальные VM, входящие в систему терминального доступа.
5. Поддержка нескольких режимов работы: профили приложений, терминальная архитектура, VDI.
6. Возможность работы с персональными дисками. Возможно закрепление за пользователем своего постоянного диска. Диск автоматически подключается к VM.
7. Поддержка тонких клиентов.
8. Шифрование трафика с использованием криптоалгоритмов, в том числе шифрование данных аутентификации пользователей.
9. Работа с наиболее популярными российскими и зарубежными ОС.
10. Возможность объединения структурных компонент платформы в кластеры для повышения отказоустойчивости.
11. Наличие механизмов отказоустойчивости.
12. Организация работы с графическими 3D-ускорителями (vGPU) и в режиме прямого проброса - Pass Through.
13. Встроенные механизмы балансировки нагрузки.
14. Работа на медленных каналах.
15. Наличие лицензий двух типов: конкурентные пользовательские и индивидуальные пользовательские.

3. Функционал клиента РУСТЭК.VDI

1. Настройка подключения локальных и сетевых принтеров с использованием универсального драйвера печати.
2. Подключение локальных дисков и буфера обмена.
3. Выбор монитора и режима отображения удаленного рабочего стола.
4. Передача звука из сессии ВРМ в пользовательскую сессию, включая поддержку микрофона и аудио устройств.
5. Проброс USB-устройств, smart-карт, веб-камер для ВМ под управлением ОС Windows и Linux.
6. Подключение к запущенной сессии и оптимизация для медленных каналов с низкой пропускной способностью (менее 256 кбит/с) и большой задержкой (более 150 мс).
7. Восстановление подключения в случае разрыва соединения.

Функции работы с мониторами:

1. Поддержка нескольких дисплеев (более 4).
2. Поддержка цветности 8-bit, 16-bit, 24-bit, 32-bit.
3. Поддержка разрешения 7680×4320 с возможностью разделения на два экрана монитора.
4. Поддержка разрешения 4К и выше, в том числе при использовании нескольких мониторов.
5. Максимальная частота кадров – до 60 кадров в секунду (FPS).

4. Функционал панели управления

1. Создание ВМ в панели управления.
2. Создание эталонного образа ВРМ.
3. Выбор эталонного образа из сетевого хранилища.
4. Создание ВРМ из эталонного образа.
5. Создание и управление различными типами пулов ВРМ: персональный, терминальный и по требованию.
6. Задание индивидуальных настроек для каждого пула.
7. Возможность задания политики обновления пулов по требованию: мягкая или жесткая. Мягкая политика – обновляются только свободные ВМ, жесткая политика – все ВМ обновляются сразу вне зависимости от подключения пользователей. При смене параметров в пуле, изменения распространяются на все ВМ.
8. Поддержка инит-скриптов при создании ВМ.
9. Управление доступом пользователей с использованием графического интерфейса.
10. Управление доступом пользователей с использованием командных сценариев.
11. Механизмы разграничения прав администраторов на уровне пулов, ВМ, сессий и других объектов инфраструктуры ВРМ.
12. Встроенные средства проверки работоспособности и мониторинга событий.
13. Встроенные механизмы балансировки нагрузки пользователей между ВРМ и терминальными ВМ.
14. Механизмы сбора информации о потреблении аппаратных ресурсов при работе терминальных ВМ и ВРМ.
15. Поддержка подключений нескольких администраторов.
16. Управление пользовательскими сессиями.
17. Использование физических серверов в качестве терминальных ВМ.
18. Использование ВМ в качестве терминальных.
19. Автоматическая установка и настройка необходимого ПО на выбранной ВМ для создания полноценного ВРМ.
20. Создание отдельного балансировщика для каждого пула.
21. Создание и управление терминальными ВМ на базе Linux и Windows.
22. Загрузка и проверка лицензии.
23. Разделение сетей для пула и участников балансировщиков.
24. Настройка подключения к NFS серверу в терминальных пулах.
25. Создание и управление профилями приложений, позволяющими запускать различные программы при подключении к одной и той же терминальной ВМ.
26. Настройка единого входа в панель управления с помощью механизма Single Sign-On (SSO).
27. Отключение приостановленных сессий по достижению лимита времени для терминальных пулов и пулов по требованию.
28. Настройка расписания включения и выключения ВМ.
29. Настройка ограничения времени сессии для всех видов пулов.

5. Функционал, связанный с защитой информации от несанкционированного доступа

1. Гибкая настройка ролевой модели администраторов, ограничивающая доступ на уровне пулов, ВМ, сессий и других объектов инфраструктуры ВРМ.
2. Разграниченный доступ в зависимости от прав пользователей.
3. Ограничение доступа пользователей в зависимости от времени суток (задание расписания работы пулов).
4. Управление политикой доступа на основе HWID для авторизации устройства доступа. Во время запуска клиентское приложение собирает информацию об устройстве, на котором запущен. На основе неизменяемых аппаратных параметров формируется HWID. При подключении клиент передает HWID и информацию об устройстве Брокеру, производится авторизация устройства согласно настроенной политике.
5. Встроенный функционал регистрации вносимых изменений с указанием времени и учетной записи администратора, инициировавшего изменение.
6. Защита клиентского и управляющего трафика посредством защищенных соединений.
7. Поддержка интеграции с AD, OpenLDAP, FreeIPA в том числе множества доменов в рамках одного леса.
8. Запрет на хранение привилегированных учетных данных службы каталога (MS AD) в РУСТЭК.VDI.
9. Авторизация по сертификатам безопасности.
10. Настройка TLS-туннелей, обеспечивающих безопасное соединение.
11. Встроенный механизм УЦ для генерации сертификатов для агентов, балансировщиков, панели управления и брокеров.
12. Поддержка двухфакторной аутентификации.

Технология VDI повышает информационную безопасность компании. Во-первых, отсутствие дисковых накопителей и возможность установки запрета на использование USB-устройств ограничивает доступ третьих лиц к корпоративным данным. Во-вторых, секретные сведения не попадут в чужие руки даже при краже компьютерной техники, поскольку вся информация хранится на серверах.