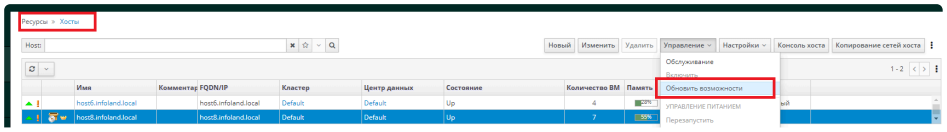
Список USB-устройств на хосте zVirt не обновляются после добавления - извлечения USB устройства (USB-Flash)

1. Вопрос

Список USB-устройств на хосте zVirt не обновляются после добавления/извлечения USB устройства (USB-Flash)

2. Ответ

Подключение/извлечение устройства - это аппаратные изменения хоста, мониторинг хоста происходит с определенным периодом. Если необходимо форсировать эту процедуру можно воспользоваться функцией **Обновить возможности**.



В Chrome не работает HTML5-консоль. Ошибка "WebSocket error Can’t connect to websocket on URL"

1. Вопрос

При использовании Chrome не работает HTML5-консоль. Ошибка:

```
WebSocket error: Can't connect to websocket on URL...
```

2. Решение

Перевыпустите TLS сертификат "Портала Администрирования" с соответствующим SAN (subject alternative name) или использовать Firefox.

Архитектура

Типы развертывания

- «Standalone» — тип развертывания, который не требует высокой доступности и отказоустойчивости системы. Такой режим подходит для тестовой инсталляции.
- «High Availability» — тип развертывания, который требует высокую доступность брокеров для обеспечения непрерывной работы системы. Если один из брокеров выйдет из строя, другие смогут взять на себя его функции и обеспечить бесперебойное обслуживание запросов пользователей. Такой режим подходит для продуктивной инсталляции.

Типы пользователей

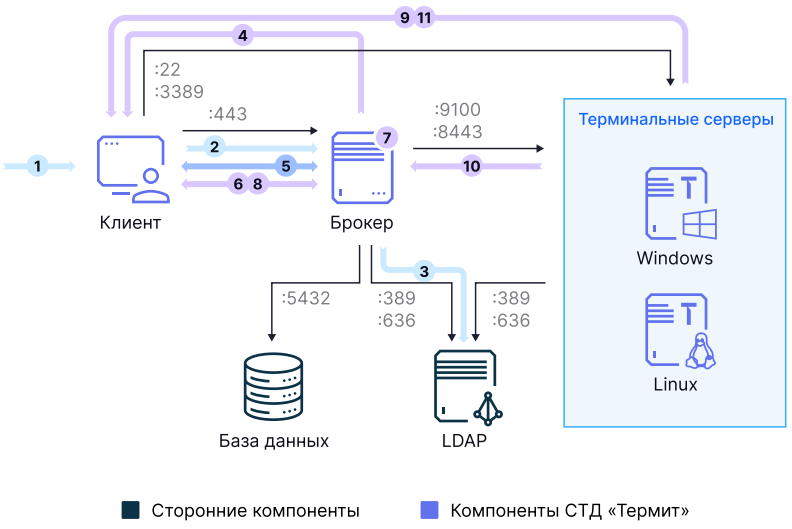
- Внутренние пользователи — пользователи, которые подключаются к СТД «Термит» из внутренней (корпоративной) сети или через корпоративное VPN-решение.
- Внешние пользователи — пользователи, которые подключаются к СТД «Термит» из внешней (вне корпоративного сегмента) сети и не используют корпоративное VPN-решение.

В этом разделе представлены:

- базовая архитектура;
- архитектура с внутренними пользователями;
- архитектура с внутренними и внешними пользователями.

Базовая архитектура

Ниже представлена схема базовой архитектуры в режиме «Standalone»: с одним брокером, без балансировщика нагрузки и шлюза.



Описание работы СТД «Термит»

Аутентификация

1. Пользователь запускает десктоп-клиент. Далее вводит адрес брокера.
2. Пользователь вводит имя доменной учетной записи и пароль.
3. Брокер проверяет эти данные на сервере LDAP.
4. Брокер возвращает десктоп-клиенту токен для аутентификации в REST API.

Получение списка приложений

5. Десктоп-клиент запрашивает у брокера список приложений, доступных пользователю. Брокер проверяет права пользователя (сравнивая его группы с теми, которые назначены на приложения) и отдает список доступных приложений.

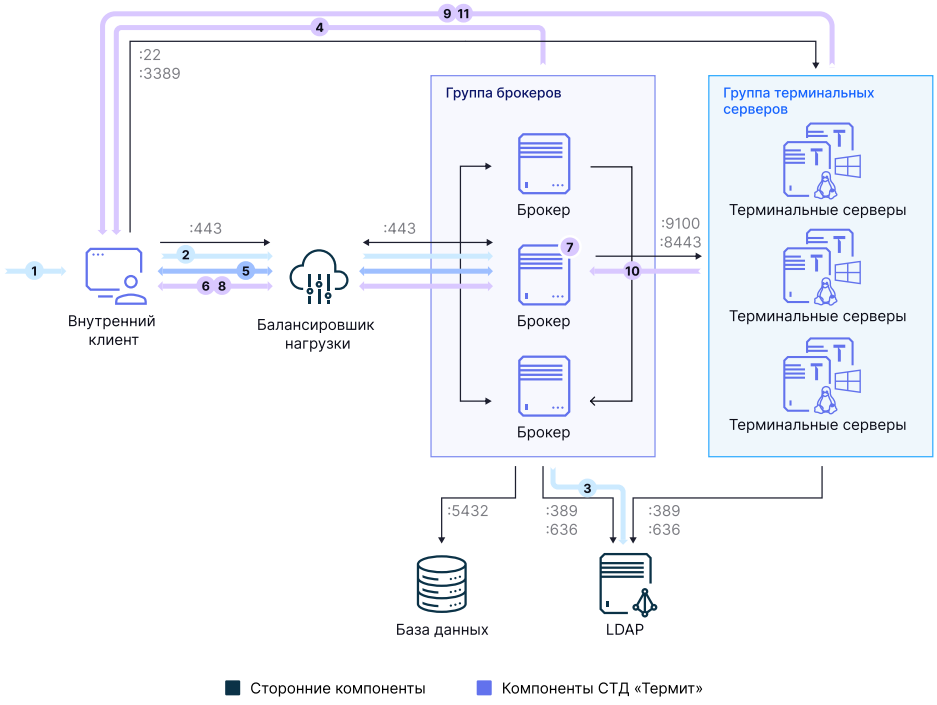
Старт сессии

6. Пользователь запускает нужное приложение или рабочий стол. Десктоп-клиент отправляет брокеру запрос на старт новой терминальной сессии.
7. Брокер выбирает терминальный сервер, который может обслужить запрос.
8. Брокер создает сессию в базе данных (БД) и отдает десктоп-клиенту профиль подключения, включающий в себя адрес шлюза удаленного доступа, адрес терминального сервера, порт подключения, команду для запуска и другие параметры.
9. Десктоп-клиент стартует сессию на терминальном сервере. В процессе старта десктоп-клиент запрашивает у пользователя имя учетной записи и пароль и отправляет их терминальному серверу. Терминальный сервер проводит аутентификацию пользователя. Десктоп-клиент настраивает перенаправление звука, файловой системы, печати и запускает приложение/рабочий стол в сессии.

10. На стороне терминального сервера агент завершает создание сессии: уведомляет брокер о том, что создана сессия с X2Go/RDP ID. Далее происходит синхронизация этого ID с ID из БД.
11. Сессия готова к работе.

Архитектура с внутренними пользователями

Ниже представлена схема архитектуры в режиме «High Availability» с внутренними пользователями, несколькими брокерами, балансировщиком нагрузки и отсутствует шлюз удаленного доступа.



Описание работы СТД «Термит»

Аутентификация

1. Пользователь запускает десктоп-клиент и вводит адрес балансировщика нагрузки. Балансировщик нагрузки определяет, какой брокер будет обслуживать этого пользователя, и в дальнейшем перенаправляет все запросы на выбранный брокер.
2. Пользователь вводит имя доменной учетной записи и пароль.
3. Брокер проверяет эти данные на сервере LDAP.
4. Брокер возвращает десктоп-клиенту токен для аутентификации в REST API.

Получение списка приложений

5. Десктоп-клиент запрашивает у брокера список приложений, доступных пользователю. Брокер проверяет права пользователя, сравнивая его группы с теми,

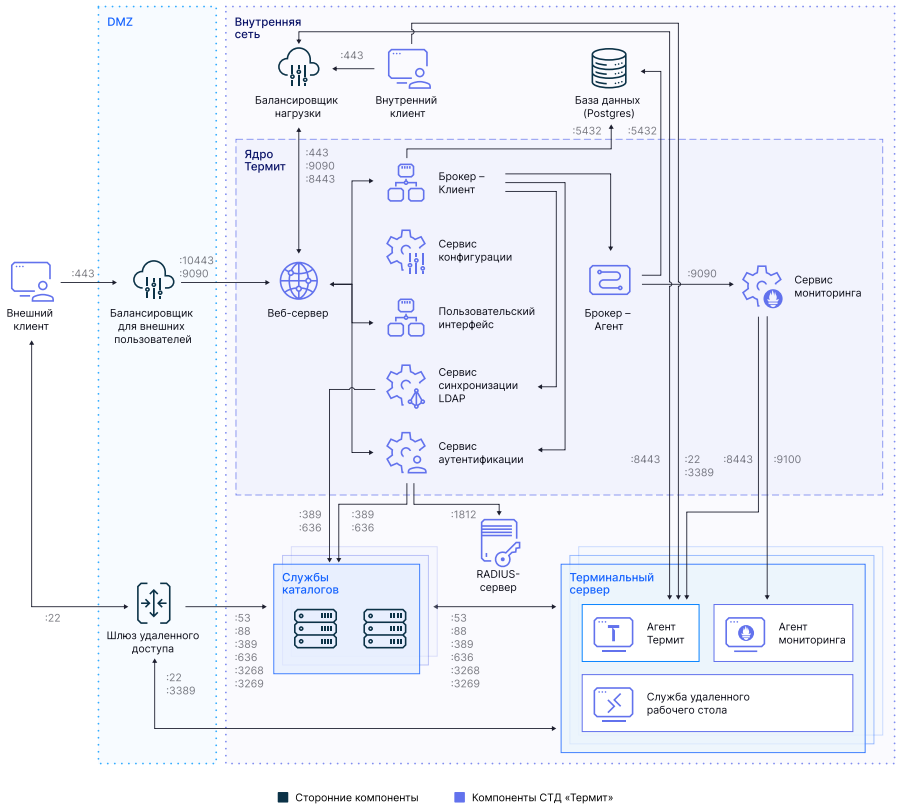
которые назначены на приложения, и отдает список доступных приложений.

Старт сессии

6. Пользователь запускает нужное приложение или рабочий стол. Десктоп-клиент отправляет брокеру запрос на старт новой терминальной сессии.
7. Брокер выбирает терминальный сервер, который может обслужить запрос.
8. Брокер создает сессию в БД и отдает десктоп-клиенту профиль подключения, включающий в себя адрес шлюза удаленного доступа, адрес терминального сервера, порт подключения, команду для запуска и другие параметры.
9. Десктоп-клиент начинает сессию на терминальном сервере. В процессе старта десктоп-клиент запрашивает у пользователя имя учетной записи и пароль и отправляет их терминальному серверу. Терминальный сервер проводит аутентификацию пользователя. Десктоп-клиент настраивает перенаправление звука, файловой системы, печати и запускает приложение/рабочий стол в сессии.
10. На стороне терминального сервера агент завершает создание сессии: уведомляет брокер о том, что создана сессия с X2Go/RDP ID. Далее происходит синхронизация этого ID с ID из БД.
11. Сессия готова к работе.

Архитектура с внешними и внутренними пользователями

Ниже представлена схема архитектуры в режиме «High Availability» с внешними и внутренними пользователями, несколькими брокерами, балансировщиком нагрузки и шлюзом удаленного доступа.



Описание работы СТД «Термит»

1. Пользователь запускает десктоп-клиент и вводит адрес балансировщика нагрузки. Балансировщик нагрузки определяет, какой брокер будет обслуживать этого пользователя, и в дальнейшем перенаправляет все запросы на выбранный брокер.
2. Пользователь указывает адрес брокера. Открывается страница для ввода логина и пароля.
3. Пользователь вводит имя доменной учетной записи и пароль.
4. Сервис аутентификации проверяет введенные данные на LDAP-сервере.
5. Сервис аутентификации проверяет данные пользователей на RADIUS-сервере и возвращает токен.
6. Брокер и десктоп-клиент используют этот токен для взаимодействия по REST API.
7. Десктоп-клиент запрашивает у брокера список приложений, доступных пользователю. Брокер проверяет права пользователя (сравнивая его группы с теми, которые назначены на приложения) и отдает список доступных приложений.
8. Пользователь запускает нужное приложение или рабочий стол. Десктоп-клиент отправляет брокеру запрос на запуск новой терминальной сессии.
9. Брокер выбирает терминальные серверы на основе метрик, который предоставляет сервис мониторинга.
10. Брокер создает сессию в БД и отдает десктоп-клиенту профиль подключения, включающий в себя адрес шлюза удаленного доступа, адрес терминального сервера, порт подключения, команду для запуска и другие параметры.

11. Пользователь подключается к шлюзу удаленного доступа и проходит на нем аутентификацию.
12. Клиент X2Go/RDP с помощью шлюза удаленного доступа начинает сессию на терминальном сервере. В процессе старта клиент X2Go/RDP запрашивает у десктоп-клиента имя учетной записи и пароль и отправляет их терминальному серверу. Терминальный сервер проводит аутентификацию пользователя. Клиент X2Go/RDP настраивает перенаправление звука, файловой системы, печати и запускает приложение в сессии.
13. На стороне терминального сервера агент Термит завершает создание сессии: уведомляет брокер о том, что создана сессия с X2Go/RDP ID. Далее происходит синхронизация сессии с брокером.
14. Сессия готова к работе.

Требования к развертыванию

Требования к инфраструктурным сторонним компонентам

Для корректного развертывания и использования СТД «Термит» необходимы следующие сторонние сервисы и компоненты:

- Инфраструктура DNS

  Перед установкой брокера проверьте с помощью команд `nslookup`, `ping`, что все компоненты: база данных, LDAP-сервер, шлюз удаленного доступа, балансировщик нагрузки, брокер, десктоп-клиент (опционально) — зарегистрированы на DNS-сервере и доступны по зарегистрированным DNS-именам. В выводе команды не должно быть ошибок.

- Сервер каталогов (LDAP)

Рекомендуемые системные требования для продуктивной инсталляции

Компонент	**Требования**
Брокер (серверный вариант установки, без графической среды)	ОС: • РЕД ОС 7.3.4, 8.0 • Debian 12 и выше • Astra Linux 1.7.5, 1.8 • OpenSUSE 15.5 • ALT Linux 10.4
	vCPU — 4
	vRAM, ГБ — 8
	Хранилище, ГБ — 100

Компонент	**Требования**
Балансировщик нагрузки HAProxy (серверный вариант установки, без графической среды)	ОС: • РЕД ОС 7.3.4, 8.0 • Debian 12 и выше • Astra Linux 1.7.5, 1.8 • OpenSUSE 15.5 • ALT Linux 10.4
	vCPU — 4
	vRAM, ГБ — 8
	Хранилище, ГБ — 100

Компонент	Требования
Терминальный сервер (серверный вариант установки, с графическим окружением)	ОС: • РЕД ОС 7.3.4 • Astra Linux 1.7.5, 1.8 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • ALT Linux 10.4 • Debian 12 и выше • OpenSUSE 15.5
	vCPU — 4
	vRAM, ГБ — 8
	Хранилище, ГБ — 100
	Требования к сессии: • Базовые: ◦ vCPU — 0,5 ◦ vRAM, ГБ — 1 ◦ Хранилище, ГБ — 0,5 • Расширенные: ◦ vCPU — 1 ◦ vRAM, ГБ — 2 ◦ Хранилище, ГБ — 2 Рекомендуется резерв 15-20% от полученных значений. Базовые требования подходят для работы с опубликованным приложением в режиме RemoteApp (текстовый редактор/ редактор таблиц/браузер). Расширенные требования подходят для работы с опубликованными приложениями в режиме RemoteApp или удаленным рабочим столом (текстовый редактор/редактор таблиц/браузер). Для получения более точных сведений требуется произвести базовый расчет, исходя из набора публикуемых приложений в рамках сессии пользователя.

Компонент	**Требования**
Шлюзы удаленного доступа OpenSSH (серверный вариант установки, без графической среды)	ОС: • РЕД ОС 7.3.4, 8.0 • Debian 12 и выше • Astra Linux 1.7.5, 1.8 • OpenSUSE 15.5 • ALT Linux 10.4
	vCPU — 4
	vRAM, ГБ — 8
	Хранилище, ГБ — 100

Среда рабочего стола терминального сервера	• Linux
	  ◦ MATE
	  ◦ XFCE
	  ◦ FLY
	• Windows
	  ◦ Explorer

База данных	PostgreSQL 11 и выше
	vCPU — 4
	vRAM, ГБ — 8
	Хранилище, ГБ — 100
	Дополнительный диск для базы данных, ГБ — 150
Десктоп-клиент	ОС: • РЕД ОС 7.3.4 • Astra Linux 1.7.5, 1.8 • Microsoft Windows 7 x32 и x64 • Microsoft Windows 8.1 x32 и x64 • Microsoft Windows 10 x32 и x64 • Microsoft Windows 11 x64 • MacOS X • ALT Linux 10.4

Компонент	Требования
Служба каталогов	• Microsoft Active Directory 2012 и выше (в качестве LDAP-каталога) • Samba DC 4.17 (необходимо отключить обязательное использование шифрования) • РЕД АДМ (Промышленная редакция) версии 1.0.2, РЕД АДМ DC 4.19.0 • FreeIPA 4.10.3 • ALD Pro 2.2.1 • OpenLDAP slapd 2.5.17

Минимальные системные требования для тестовой инсталляции

Компонент	Требования
Брокер (серверный вариант установки, без графической среды)	ОС: • РЕД ОС 7.3.4, 8.0 • Debian 12 и выше • Astra Linux 1.7.5, 1.8 • OpenSUSE 15.5 • ALT Linux 10.4
	vCPU — 2
	vRAM, ГБ — 8
	Хранилище, ГБ — 50
Балансировщик нагрузки HAProxy (серверный вариант установки, без графической среды)	ОС: • РЕД ОС 7.3.4, 8.0 • Debian 12 и выше • Astra Linux 1.7.5, 1.8 • OpenSUSE 15.5 • ALT Linux 10.4
	vCPU — 2
	vRAM, ГБ — 2
	Хранилище, ГБ — 50

Компонент	Требования
Шлюзы удаленного доступа OpenSSH (серверный вариант установки, без графической среды)	ОС: • РЕД ОС 7.3.4, 8.0 • Debian 12 и выше • Astra Linux 1.7.5, 1.8 • OpenSUSE 15.5 • ALT Linux 10.4
	vCPU — 2
	vRAM, ГБ — 2
	Хранилище, ГБ — 50
База данных	PostgreSQL 11 и выше
	vCPU — 2
	vRAM, ГБ — 4
	Хранилище, ГБ — 50
Терминальный сервер (серверный вариант установки, с графическим окружением)	ОС: • РЕД ОС 7.3.4 • Astra Linux 1.7.5, 1.8 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • ALT Linux 10.4 • Debian 12 и выше • OpenSUSE 15.5
	vCPU — 4
	vRAM, ГБ — 4
	Хранилище, ГБ — 50
	Базовые требования к сессии: • vCPU — 0,2 • vRAM, ГБ — 0,5 • Хранилище, ГБ — 0,2

Компонент	Требования
Десктоп-клиент	ОС: • РЕД ОС 7.3.4 • Astra Linux 1.7.5, 1.8 • Microsoft Windows 7 x32 и x64 • Microsoft Windows 8.1 x32 и x64 • Microsoft Windows 10 x32 и x64 • Microsoft Windows 11 x64 • MacOS X • ALT Linux 10.4
Служба каталогов	• Microsoft Active Directory 2012 и выше (в качестве LDAP-каталога) • Samba DC 4.17 (необходимо отключить обязательное использование шифрования) • РЕД АДМ (Промышленная редакция) версии 1.0.2, РЕД АДМ DC 4.19.0 • FreeIPA 4.10.3 • ALD Pro 2.2.1 • OpenLDAP slapd 2.5.17 Базовые требования подходят для работы с опубликованным приложением в режиме RemoteApp (текстовый редактор/ редактор таблиц/браузер). Для получения более точных сведений требуется произвести базовый расчет, исходя из набора публикуемых приложений в рамках сессии пользователя.

Порты

Источник	Назначение	Протокол	Порт	Описание
Брокер	База данных	TCP	5432	Связь с сервером баз данных PostgreSQL
	Служба каталогов	TCP/UDP	389/636	LDAP/LDAPS/LDAP StartTLS
	RADIUS-сервер	RADIUS	1812	Связь сервиса аутентификации и RADIUS-сервера
	Терминальный сервер	TCP	8443	Связь сервиса мониторинга, брокера и агента
		TCP	9100	Связь сервиса мониторинга и агента мониторинга
	Брокер (Межсервисная коммуникация)	TCP	9090	Связь брокера и сервиса мониторинга
Шлюз удаленного доступа	Терминальный сервер (Linux)	TCP	22	SSH подключение к терминальному серверу
	Терминальный сервер (Windows)	TCP	13389	RDP подключение к терминальному серверу через SSH-туннель между шлюзом и терминальным сервером
	Служба каталогов	TCP/UDP	389/636	LDAP/LDAPS/LDAP StartTLS
		TCP/UDP	53	DNS
		TCP/UDP	88	Kerberos
		TCP	3268/3269	Глобальный каталог/Глобальный каталог с SSL
Десктоп-клиент	Шлюз удаленного доступа	TCP	22	Связь десктоп-клиента и шлюза
	Терминальный сервер (Linux)	TCP	22	SSH подключение к терминальному серверу без использования компонента шлюз
	Терминальный сервер (Windows)	TCP	3389	RDP подключение к терминальному серверу без использования компонента шлюз
	Балансировщик нагрузки	TCP	443	HTTPS подключение к брокеру через балансировщик нагрузки
	Брокер	TCP	443	HTTPS подключение к брокеру

Источник	Назначение	Протокол	Порт	Описание
Внутренний балансировщик нагрузки	Брокер	TCP	80* * Трафик, поступающий на порт 80, перенаправляется на порт 443	Связь балансировщика нагрузки и брокера
		TCP	443	Связь балансировщика нагрузки и брокера
		TCP	8443	Связь балансировщика нагрузки и брокера
		TCP	9090	Связь балансировщика нагрузки и брокера
Внешний балансировщик нагрузки	Брокер	TCP	9090	Связь балансировщика нагрузки и брокера
		TCP	10443	Связь балансировщика нагрузки и брокера
Терминальный сервер	Служба каталогов	TCP	3268/3269	Глобальный каталог/Глобальный каталог с SSL
		TCP/UDP	53	DNS
		TCP/UDP	88	Kerberos
	Внутренний балансировщик нагрузки	TCP	8443	Связь агента и внутреннего балансировщика нагрузки
	Брокер	TCP	8443	Связь агента и брокера
	Брокер	TCP	443	Связь терминального сервера и брокера
	Внутренний балансировщик нагрузки	TCP	443	Связь терминального сервера и внутреннего балансировщика нагрузки

Пропускная способность

Ниже приведены данные пропускной способности сети.

Разрешение Full HD

Сценарий	X2Go	RDP	Описание
Бездействие	0,2 Мбит/с	0,1 Мбит/с	Простой экрана (Рабочий стол)
Libre Office (Word)	0,2-1,2 Мбит/с	0,09-0,1 Мбит/с	Активный набор текста, копирование-вставка текста и изображений
Libre Office (Excel)	0,4-1,1 Мбит/с	0,05-0,1 Мбит/с	Активный набор текста, копирование-вставка текста и изображений
Просмотр веб-страниц	1,2-3,6 Мбит/с	1,9-4,7 Мбит/с	Просмотр веб-страниц браузером Mozilla Firefox с чередующимся содержимым (текст, изображения), переход по страницам
Коллекция изображений	0,7-1,9 Мбит/с	0,4-1,4 Мбит/с	Поочередный просмотр коллекции изображений (10 шт)
Воспроизведение видео	3,5-7,6 Мбит/с	2,5-6,3 Мбит/с	Просмотр Full HD видео в свернутом режиме (не на весь экран)
Воспроизведение видео в полноэкранном режиме	5,5-9,5 Мбит/с	3,8-9,7 Мбит/с	Просмотр Full HD видео на весь экран

При работе с разрешением 1920 x 1080 рекомендуемая максимальная задержка в пределах 150-200 мс с потерями до 10% потери пакетов. Пропускная способность для сотрудника офиса (работа с документами) должна составлять 0,6 Мбит/с на одну сессию.

Разрешение 4K

Сценарий	X2Go	RDP	Описание
Бездействие	0,2-0,4 Мбит/с	0,1 Мбит/с	Простой экрана (Рабочий стол)
Libre Office (Word)	0,4-0,7 Мбит/с	0,05-0,3 Мбит/с	Активный набор текста, копирование-вставка текста и изображений
Libre Office (Excel)	0,6-1 Мбит/с	0,09-0,3 Мбит/с	Активный набор текста, копирование-вставка текста и изображений
Просмотр веб-страниц	0,5-6 Мбит/с	3,8-9 Мбит/с	Просмотр веб-страниц браузером Mozilla Firefox с чередующимся содержимым (текст, изображения), переход по страницам
Коллекция изображений	0,5-2,5 Мбит/с	3,3-7,3 Мбит/с	Поочередный просмотр коллекции изображений (10 шт)

Сценарий	X2Go	RDP	Описание
Воспроизведение видео	27-32 Мбит/с	18-30 Мбит/с	Просмотр Full HD видео в свернутом режиме (не на весь экран)
Воспроизведение видео в полноэкранном режиме	28,5-34,5 Мбит/с	24-34 Мбит/с	Просмотр Full HD видео на полный экран

При работе с разрешением 3840 x 2160 рекомендуемая максимальная задержка в пределах 10-30 мс с потерями до 5%. Пропускная способность для сотрудника офиса (работа с документами) должна составлять 5 Мбит/с на одну сессию.

О системе

В этих разделах вы найдете описание системы терминального доступа «Термит» (СТД «Термит»):

- Обзор
- Архитектура
- Ограничения и особенности
- Требования к развертыванию