

Терминальные службы в Windows Server 2008

Андрей Бирюков

Приложения, требующие одновременного доступа множества пользователей, всегда были головной болью системных администраторов. Служба терминалов в Windows Server 2008 позволит решить ряд проблем, связанных с работой таких приложений.

Службы удаленного доступа к приложениям являются неотъемлемой частью любой современной операционной системы. В семействе Windows Server служба терминалов появилась еще в версии NT 4.0, а в недавно вышедшей версии Windows Server 2008 реализация централизованного доступа к приложениям получила существенное развитие за счет новых функций и систем.

Зачем нужны службы терминалов

Для начала хочу немного рассказать, зачем нужны терминальные сервисы. Например, возможность существенно сэкономить административные ресурсы, так как гораздо проще установить приложение на одном сервере и предоставить к нему клиентский доступ, чем разворачивать это же приложение на каждой клиентской рабочей станции. Это особенно полезно для устаревших программ и приложений, которые не поддерживают клиент-серверную архитектуру, однако до сих пор довольно активно используются в организациях.

Другая причина – это возможность сэкономить на оборудовании, так как

достаточно приобрести один мощный терминальный сервер, и требования к клиентским рабочим станциям существенно снижаются, потому что основные вычислительные нагрузки берет на себя сервер.

Что нового

Рассмотрим более подробно, о каких новых функциях идет речь. Прежде всего, это возможность работы с удаленными приложениями служб терминалов. Теперь пользователи могут запускать удаленные приложения на своем рабочем столе наряду с обычными локальными приложениями. (Тем, кто знаком с аналогичными решениями от Citrix, думаю, такая технология понравится.) Для этого необходим клиент подключения к удаленному рабочему столу версии 6.0. Данный клиент встроен в Windows Server 2008 и Vista, для XP и 2003 версии клиенты доступны для бесплатной загрузки.

Другим нововведением является шлюз служб терминалов (TS Gateway), который позволяет получить безопасный доступ к службам терминалов и общим рабочим столам из-за пределов межсетевого экрана предприятия без необходимости развертывания

инфраструктуры виртуальной частной сети (VPN).

Также имеется возможность использования протокола HTTPS для доступа к службам терминалов без необходимости настройки на стороне клиента.

Комплексная модель безопасности TS Gateway позволяет администраторам контролировать доступ к определенным ресурсам в сети. В частности, возможно ограничение доступа пользователей только к определенным серверам и рабочим станциям, а не ко всей сети предприятия, как это происходит в случае использования подключений к виртуальной частной сети.

Еще данная технология позволяет подключаться пользователям к серверам терминалов и удаленным рабочим станциям через межсетевые экраны и преобразователи сетевых адресов (NAT).

Еще одной новой возможностью является веб-клиент служб терминалов (TS Web Access), который позволяет осуществлять работу с удаленным столом пользователя через веб-интерфейс. С помощью веб-клиента служб терминалов пользователи могут полу-

чить список доступных приложений через веб-узел. Выглядит это примерно следующим образом.

Когда пользователь запускает одно из удаленных приложений, для этого пользователя автоматически создается сеанс служб терминалов на сервере под управлением Windows Server 2008, также для пользователя в этом интерфейсе доступно централизованное меню, в котором отображаются все доступные удаленные приложения. Чтобы запустить удаленное приложение, достаточно выбрать нужную программу в меню.

Как видно, использование веб-клиента служб терминалов позволяет снизить затраты на администрирование, так как отпадает необходимость в администрировании отдельных экземпляров используемых приложений.

И, наконец, это возможность единого входа (также известная Single Sign On), технология, улучшающая взаимодействие с пользователями, избавляя от необходимости многократно вводить свои учетные данные.

Установка

Обсудив в теории новые возможности службы терминалов Windows Server 2008, рассмотрим этот функционал на практике.

Прежде всего, установка. Надо сказать, что процесс установки немного изменился по сравнению с терминальными службами в предыдущих версиях Windows Server. Для того чтобы развернуть терминальные службы, необходимо добавить соответствующую роль в списке ролей сервера (см. **рис. 1**).

Выбираем «Terminal Services». Далее указываем необходимые службы терминального сервера, которые должны быть установлены. Обратите внимание, что для функционирования некоторых из них требуется включение сервера в домен Active Directory.

Затем нужно определиться с методом аутентификации (см. **рис. 2**). В случае если вы выбрали вариант «Require Network Level Authentication», только рабочие станции, на которых установлены совместимые версии операционной системы и терминального клиента, смогут устанавливать удаленные сессии с данным сервером. В случае если Network Level Authentication не тре-

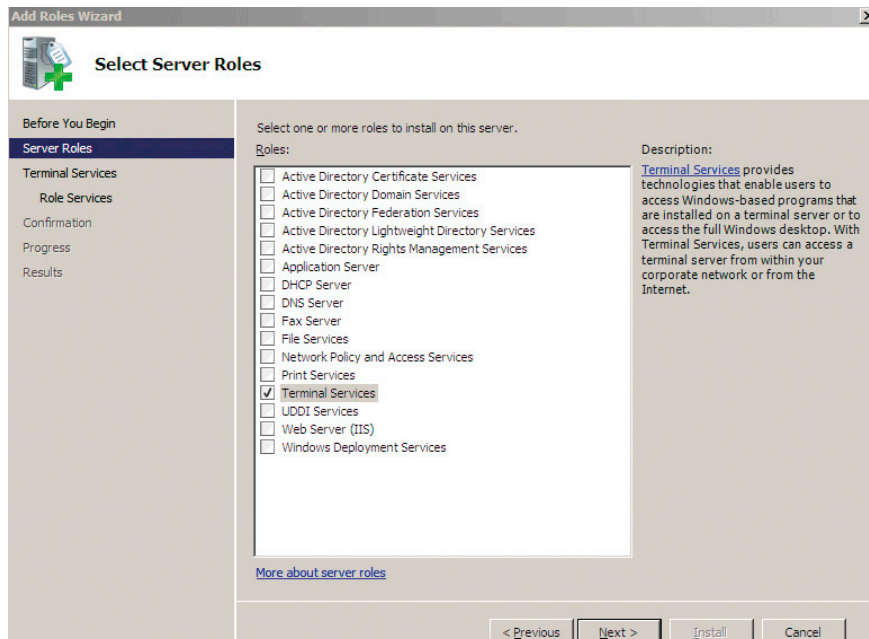


Рисунок 1. Список ролей сервера

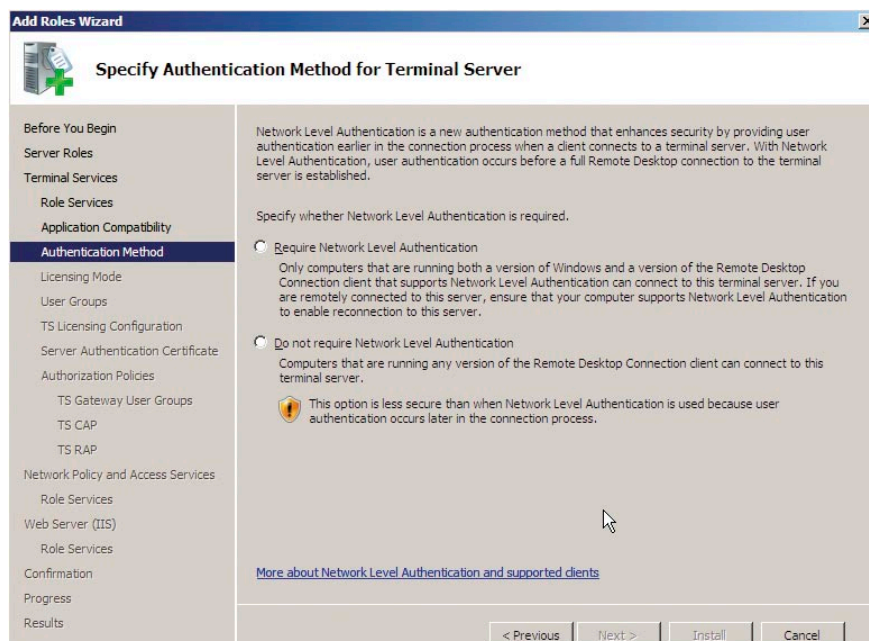


Рисунок 2. Выбор метода аутентификации

буется, рабочие станции с любыми версиями терминальных клиентов могут подключаться. Данная функция позволяет увеличить защищенность терминального сервера, так как предыдущие версии клиентов содержат множество уязвимостей, и отказ от их использования существенно повысит защищенность.

На следующем этапе нужно определиться с режимом лицензирования. Делать это при установке необязательно, можно доустановить потом, главное не забыть, что без лицензий терминальный сервер будет работать

только 120 дней, после чего вы сможете только устанавливать не более двух административных сессий.

На следующем этапе требуется указать группы пользователей, которым разрешен доступ к данному терминальному серверу. Затем идут настройки, требующиеся для работы по протоколу HTTPS. В частности, необходимо указать сертификат, который будет использоваться для создания SSL-соединения (см. **рис. 3**). Данный сертификат можно экспортировать из файла.

Такой способ рекомендуется для

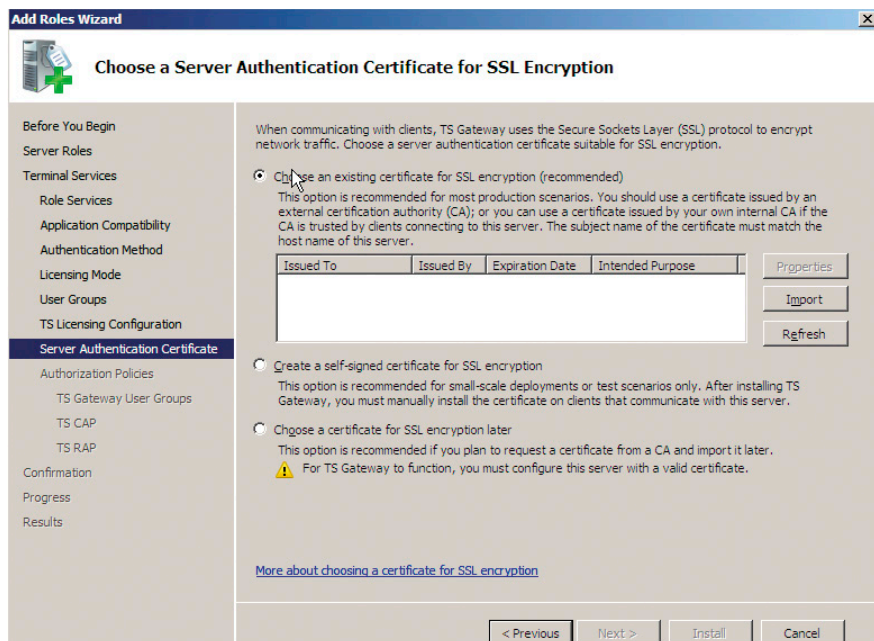


Рисунок 3. Настройки SSL

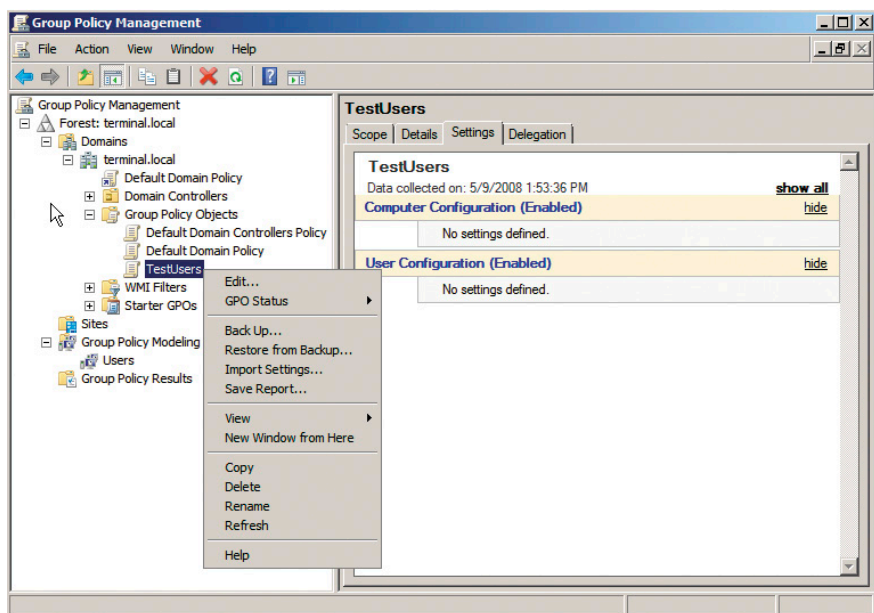


Рисунок 4. Управление групповыми политиками

крупных сетей, где используется свой центр сертификации (Certification Authority), так как таким образом можно обеспечить довольно высокую степень защиты терминальной сессии.

Другой способ – это использование самоподписанного (Self Signed) сертификата, правда, данный способ рекомендуется только для небольших организаций или в тестовых целях.

Далее нам предлагается создать так называемую Authorization Policy для TS Gateway, то есть политику авторизации, которая определяет, каким группам пользователей можно осуществлять подключение к серверу

шлюза терминальных служб. По умолчанию разрешено подключение только для группы Administrators. В качестве способов авторизации помимо традиционного ввода пароля можно также использовать Smart Card. Также можно определить, к каким именно терминальным серверам могут подключаться пользователи.

На этом установка служб терминальных сервисов в Windows Server 2008 завершается.

Настройка

Теперь приступим к настройке созданного терминального сервера.

Для этого необходимо открыть консоль Server Manager, затем Terminal Services. В этом разделе можно просмотреть суммарную статистику по событиям, связанным со службой терминалов, при этом можно использовать различные фильтры для поиска новых интересующих событий. Следует отметить, что это новшество теперь добавлено во все компоненты Windows Server 2008.

Также здесь можно наблюдать, какие системные службы запущены, какие роли сервера установлены, и еще здесь Windows 2008 предлагает некоторые рекомендации по настройке терминальных сервисов.

Теперь посмотрим, какие настройки доступны для компонентов терминальных сервисов.

Прежде всего это TS RemoteApp Manager. Здесь можно настроить, какие приложения будут доступны для работы через службы терминалов, при этом их можно будет запускать с локальной машины пользователя. Для того чтобы это сделать, необходимо добавить нужную программу в список RemoteApp Programs. В качестве примера мы выполним необходимые действия.

В роли приложения, которое нужно сделать доступным для локальных пользователей, будет выступать консоль администрирования сервера TS Licensing Service. Выбираем опцию «Add RemoteApp Programs». Далее в списке отмечаем «TS Licensing Manager». Работа мастера завершена, теперь нам необходимо сделать приложение доступным с рабочей станции пользователя.

Для этого нам надо сначала определить, каким способом мы хотим распространить доступ к данному приложению на рабочие станции. Возможны два варианта: создание RDP-файла и использование пакета Windows Installer. Мы рассмотрим оба варианта. Первый вариант удобен для использования в небольших сетях, тогда как второй лучше использовать в крупных корпоративных сетях, где с помощью групповых политик распространять приложение на рабочие станции.

Создадим RDP-файл. Для этого сначала выберите нужное приложение в списке программ в нижней части окна, в разделе «RemoteApp

Programs». Затем выберите опцию «Create .rdp file». В открывшемся окне мастера необходимо указать путь к каталогу, в котором будет храниться создаваемый файл, затем можно изменить адрес сервера и порт, которые будут использоваться для доступа к приложению через службу терминалов. Также можно сменить настройки TS Gateway, например изменить сервер, используемый по умолчанию, или отключить использование TS Gateway. И, наконец, можно настроить использование сертификатов для установки защищенных соединений. В результате работы мастера в каталоге C:\Program Files\Packaged Programs создается новый файл, который можно разместить на рабочей станции пользователя для доступа к удаленному приложению.

Теперь создадим пакет Windows Installer. Здесь настройки будут аналогичные: путь к создаваемому файлу, настройки терминального сервера, настройки TS Gateway и настройки сертификатов. В следующем окне вы можете выбрать, где создавать яр-

лыки для доступа к приложению: на рабочем столе или в папке Start. Также можно ассоциировать расширения, используемые данным приложением, с другими файлами на рабочей станции пользователя.

Развертывание настроек с помощью GPO

Итак, созданные .rdp- и .msi-файлы можно различными способами поместить на рабочие станции пользователей. В качестве примера я разверну .msi-файлы с помощью групповых политик Windows Server 2008. Итак, у нас имеется домен terminal.mylcal, в котором требуется для группы компьютеров TestUsers развернуть .msi-файл для доступа к приложению через службу терминалов.

Следует сразу заметить, что настройка групповых политик в Windows Server 2008 несколько отличается от настроек в предыдущих версиях Windows Server. Прежде всего, теперь раздел «Group Policy Management» доступен в виде отдельной закладки, не через «Active Directory Users And Computers»,

как раньше. Сама консоль Group Policy Management также существенно изменилась. Теперь здесь доступны настройки для леса, доменов, входящих в данный лес. Также из этой консоли можно управлять политиками для доменов, контроллеров доменов. Еще одно полезное средство, появившееся в новой консоли, — это Group Policy Modeling. Это средство, позволяющее смоделировать последствия применения групповых политик к определенному объекту, может быть очень полезно в случае, если используется несколько политик и множество объектов.

Однако я несколько отвлекся описанием работы с групповыми политиками, вернемся к службам терминалов. Для выполнения поставленной задачи необходимо открыть раздел «Forest», выбрать «Domains» и указать имя домена (в данном случае это terminal.mylcal), затем «Group Policy Objects, TestUsers» (групповая политика, которая будет применена к машинам тестовой группы). После выполнения этих действий нажмите правую кнопку мыши и выберите «Edit». В от-

Самый удобный способ приобретения ПО

Интернет-супермаркет программного обеспечения

SOFTKEY



www.softkey.ru



открыто 24 часа

✓ **Круглосуточный интернет-супермаркет программного обеспечения**

www.softkey.ru

Телефон:
+7 (495) 661-3243



реклама

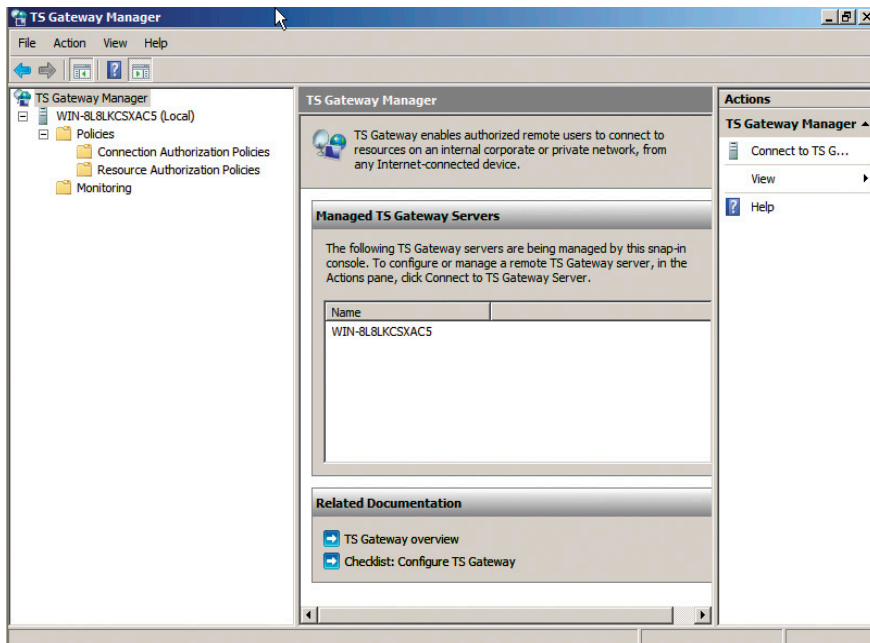


Рисунок 5. Управление TS Gateway

крывшемся окне нажимаем «Computer Configuration».

Как известно, приложение можно либо опубликовать, привязав к политикам пользователя (User Configuration), или же установить, привязав к политикам компьютера (Computer Configuration). Выполним второе действие. Для этого в разделе «Policies» указываем «Software Settings» и затем «Software Installation». Нажав правую кнопку мыши, выбираем «New Package». С помощью мастера выбираем нужный файл, затем «Assigned». Теперь групповая политика может применяться к рабочим станциям.

После применения групповой политики у пользователей появится яр-

лык, после нажатия на который запустится мастер RemoteApp, который после авторизации пользователя запустит на локальной машине приложение терминального сервера. Следует также отметить, что при необходимости удаленное приложение может быть доступно через Web Access. Также можно разрешить использовать аргументы командной строки.

Шлюзы терминального доступа

Теперь поговорим более подробно о другой интересной службе, входящей в состав терминальных сервисов. Это TS Gateway Manager. Как я уже упоминал выше, TS Gateway предназначен для подключения к различным терминальным серверам через единый шлюз. Думаю, удобства такого подхода очевидны. Пользователям не надо путаться среди множества различных терминальных серверов, достаточно сохранить настройки для доступа к единому шлюзу, с помощью которого уже подключаться к нужному приложению. Администраторам не надо настраивать политики доступа на множестве серверов, достаточно настроить на шлюзе.

Рассмотрим более подробно настройку TS Gateway. Для этого нам необходимо открыть консоль TS Gateway Manager. В основном окне можно наблюдать сервера, доступные для управления (см. рис. 5).

При нажатии на значок конкретного сервера вы можете получить информацию о его текущей загрузке, количестве подключений, применяемых политиках и так далее. Собственно, используемых по умолчанию политик авторизации две: Connection Authorization Policies и Resource Authorization Policies.

Первая используется для настройки пользователей, которым разрешено соединение с сервером TS Gateway. Здесь определяются, в частности, способ аутентификации (пароль и/или смарт-карта), а также группы пользователей, которым разрешен доступ. Еще здесь можно определить перенаправление устройств, подключенных к терминальному серверу. То есть пользователям может быть разрешено подключение принтеров, серийных портов, устройств Plug and Play, драйверов устройств и буфера обмена.

Вторая политика определяет рабочие станции, которым разрешено подключаться к серверу TS Gateway. Здесь также можно определить группы пользователей, которые могут подключаться к удаленным серверам через TS Gateway. Что касается управления доступом к терминальному шлюзу для рабочих станций, то тут можно воспользоваться двумя способами: указать уже созданную Active Directory Security Group или использовать существующую TS Gateway Managed Computer Group. По умолчанию пользователи могут подключаться к любому ресурсу.

Сетевые порты, используемые для установки терминальной сессии, также можно менять при необходимости. По умолчанию используется стандартный порт 3389.

Заключение

На этом я завершаю свой рассказ о службах терминального доступа в Windows Server 2008. Как видно, в новой операционной системе в эти службы также добавилось много новых возможностей, что позволит администраторам оптимизировать работу пользователей с удаленными приложениями с помощью служб терминалов.

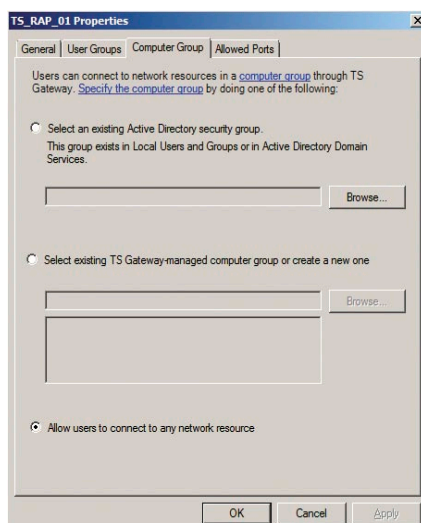


Рисунок 6. Управление доступом для рабочих станций

1. <http://www.microsoft.com/windows/server2008/en/us/default.aspx> – страница, посвященная Windows Server 2008.