CommView Remote Agent

Руководство пользователя

Введение

О программе CommView Remote Agent

Программа CommView Remote Agent предназначена для наблюдения трафика в удалённой сети. Она позволяет пользователям программы CommView анализировать сетевой трафик на компьютере, где запущен Remote Agent, где бы физически этот компьютер ни был расположен. Эта новая, уникальная технология расширяет ваши возможности: вы не ограничены только вашим компьютером или сегментом сети. Находясь, на пример, в Токио, вы можете отлаживать сетевые установки, скажем, в Амстердаме. Запустите CommView Remote Agent на отлаживаемой системе и работайте из своего офиса, как бы находясь возле неё!

Достаточно провести установку, несложную конфигурацию, и, CommView Remote Agent готов принять подключение со стороны CommView. Как только соединение будет установлено и произойдёт успешная проверка пароля, CommView Remote Agent сможет собирать трафик в своём сегменте сети и передавать его на CommView. Передаваемые пакеты "сжимаются" для уменьшения нагрузки на сеть и шифруются для обеспечения безопасной передачи по открытым сетям. Программа CommView оснащена гибким набором фильтров, чтобы отсеивать ненужные пакеты, минимизируя служебный TCP трафик между CommView и CommView Remote Agent.

CommView Remote Agent - незаменим для профессионалов в области сетевых технологий, программирования и безопасности, поможет решить широкий круг задач, таких как наблюдение многосегментных сетей или дистанционная отладка сетевых программ.

CommView Remote Agent работает с любой версией Windows - 95/98/ME/NT/2000/XP, ему требуется сетевой адаптер Ethernet или Wireless Ethernet, с драйвером, соответствующим стандарту NDIS 3.0, или обычный адаптер удалённого доступа (dial-up adapter).

Что нового

Версия 1.1

- В этой версии исправлены ошибки предыдущих версий и улучшена совместимость с Windows .NET. Кроме того, обновлён драйвер для совместимости с последней версией CommView и другими продуктами, выход которых ожидается вскоре.

Лицензионное соглашение

Пожалуйста, прежде чем использовать это программное обеспечение, внимательно прочтите данные условия. Ваше использование этого программного обеспечения означает Ваше согласие с этим лицензионным соглашением. Если Вы не согласны с условиями этого лицензионного соглашения, Вы должны удалить это программное обеспечение с Вашего устройства хранения и перестать использовать продукт.

Авторское право
Авторские права этого программного обеспечения принадлежат TamoSoft, Inc 1999-2002. CommView Remote Agent - торговая марка TamoSoft, Inc. Использование этого программного обеспечения и авторские права на него охраняются международными договорами об авторском праве. TamoSoft, Inc. владеет всеми правами на это программное обеспечение и документацию, и предоставленная лицензия ни каким образом не уменьшает права на интеллектуальную собственность TamoSoft, Inc. Вы не должны распространять регистрационные коды, предоставляемые на бумаге, в электронном виде, или другой форме.

Демонстрационная Версия
Это не бесплатное программное обеспечение. Настоящим Вам разрешается использовать это программное обеспечение для испытательных целей бесплатно в течение 30 дней. Использование этого программного обеспечения после данного срока является нарушением законов об авторских правах и может закончиться серьезным гражданским и уголовным наказанием.

Зарегистрированная Версия
Лицензия на один компьютер даёт право установить и использовать программу на одном компьютере. Чтобы установить программу на несколько компьютеров, необходимо приобрести многокомпьютерную лицензию.

Отказ от гарантий
Это програмное обеспечение предоставляется "как есть" без гарантий любого типа, явных или не явных; включая, но не ограничиваясь, гарантиями комерческими или пригодности для конкретной цели. Ни в каком случае tamosoft, inc. не будет нести ответственность перед вами за любой ущерб, включая случайный, или вытекающие ущербы, возникающие при использовании этого програмного обеспечения, даже если бы было предупреждено о возможных таких ущербах. Вы подтверждаете, что вы прочитали эту лицензию, понимаете и согласны быть в рамках его условий.

Законодательная поддержка
Данное Соглашение будет рассматриваться в рамках законов Республики Кипр.

Распространение
Это программное обеспечение может свободно распространятся в оригинальной немодифицированной и незарегистрированной форме. Дистрибутив должен включать все файлы его оригинальной поставки. Дитрибьютеры не могут брать деньги за это. Распространяющий это программное обеспечение за любое вознаграждение должен предварительно связаться с нами и получить разрешение.

Другие Ограничения
Вы не можете изменять, переделывать, декомпилировать или дизассемблировать это программное обеспечение любым путём, включая изменение или удаление любых сообщений или окон.

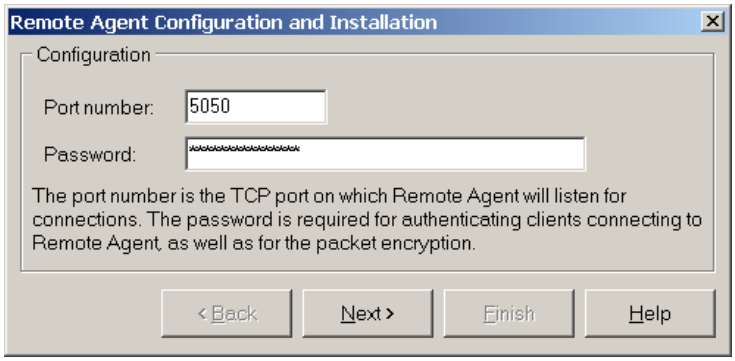
Работа с программой

Установка и настройка

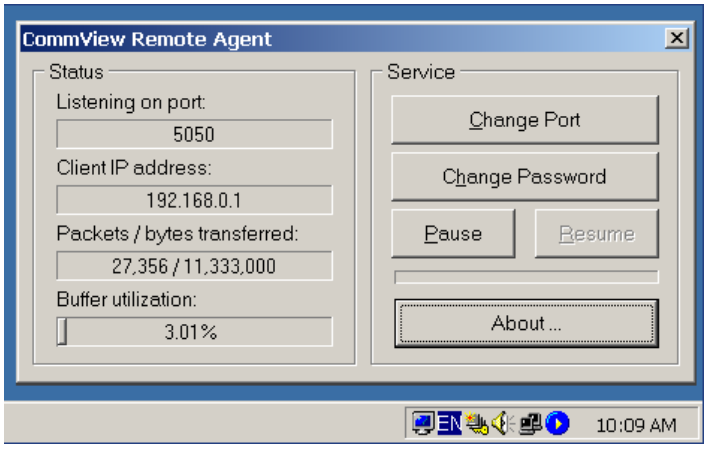
CommView Remote Agent следует устанавливать на компьютер(ах), чей трафик вы намерены отслеживать. Как и CommView, он может захватывать пакеты, проходящие через любой сетевой интерфейс - сетевой адаптер или адаптер удалённого доступа. CommView Remote Agent можно устанавливать как на подключенные к сети, так и изолированные компьютеры. Для установки программы под Windows NT/2000/XP требуются права администратора, после установки и конфигурирования программы - такой уровень привилегий для работы с ней не требуется. Не устанавливайте ОДНОВРЕМЕННО и CommView и CommView Remote Agent на одном и том же компьютере, поскольку это бессмысленно.

Настройка программы

Для установки программы - запустите SETUP.EXE и следуйте инструкциям. Когда копирование необходимых файлов завершится, вы увидите окно Установки и Конфигурации (Installation and Configuration), где необходимо указать номер порта TCP и пароль доступа. По умолчанию выбран порт 5050, к нему будет подключаться клиентская программа CommView. Пароль требуется для идентификации клиента и последующей шифрации трафика. Выбирайте **хороший** пароль (достаточно длинный, содержащий буквенно-цифровые комбинации, который трудно угадать), иначе, если кто-либо посторонний угадает пароль, он получит ПОЛНЫЙ доступ к сетевому трафику данного компьютера.



Нажмите **Next**, чтобы продолжить, программа установит необходимые драйверы и произведёт первый запуск CommView Remote Agent. Иконка программы появится в панели уведомлений, как показано на рисунке внизу. Для вызова окна приложения CommView Remote Agent, щёлкните по ней:

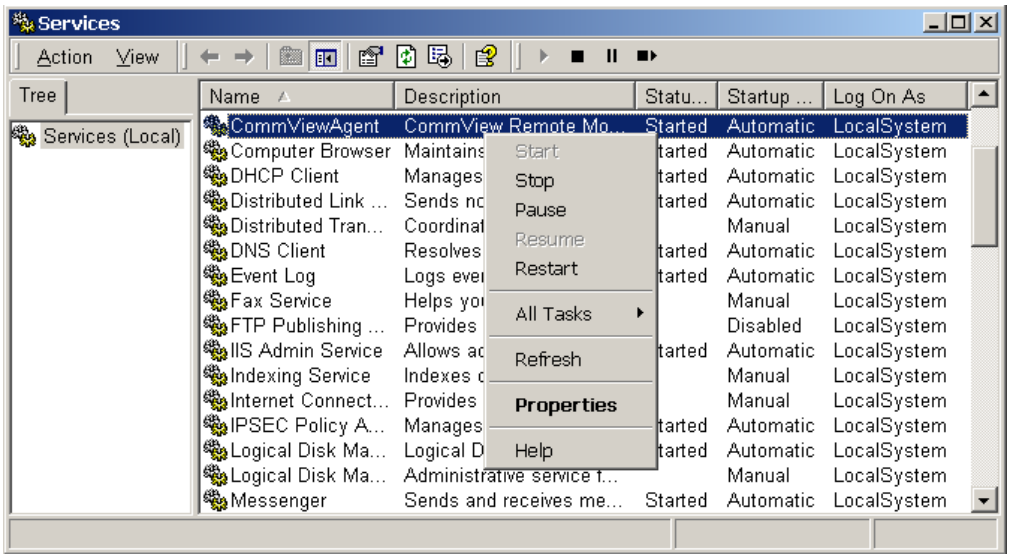


Поле **Status** показывает состояние программы: номер порта, на котором CommView Remote Agent ожидает подключения, IP адрес подключившегося клиента, статистику передачи пакетов, использование буфера. Поле **Service** содержит несколько настроечных кнопок. Изменить номер порта можно нажав **Change Port**. Изменить пароль можно нажав **Change Password**. Приостановить и продолжить работу можно нажав соответственно кнопку **Pause** или **Resume**. Нажав на кнопку **About**, можно узнать общие сведения о программе.

CommView Remote Agent способен устанавливать только одно клиентское подключение за раз.

Управление программой

CommView Remote Agent является **сервисом NT**. Это означает, что программа запускается и начинает работать автоматически, при загрузке компьютера, даже если ни один пользователь не зарегистрировался в операционной системе. Соответственно, как и любым другим сервисом, им можно управлять из Control Panel => Administrative Tools => Services. Там же можно установить режим запуска (автоматический/ручной), выключить/включить/приостановить/возобновить сервис.



В Windows 95/98/ME, CommView Remote Agent эмулирует сервис NT, то есть, работает независимо от регистрации/выхода пользователей.

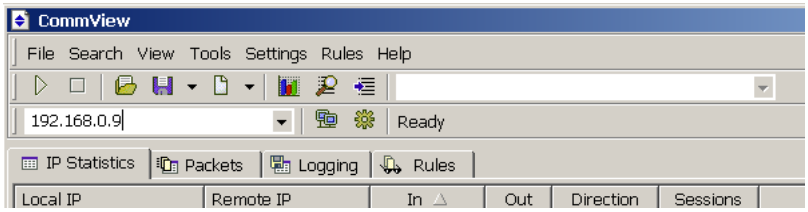
Для упрощения управления сервисом, прилагается утилита Service Indicator. Ей можно выключить/включить/приостановить/возобновить сервис, не заходя в Панель Управления. Утилита находится в папке CommView Remote Agent (Start => Programs => CommView Remote Agent => Service Indicator).

Наблюдение за трафиком

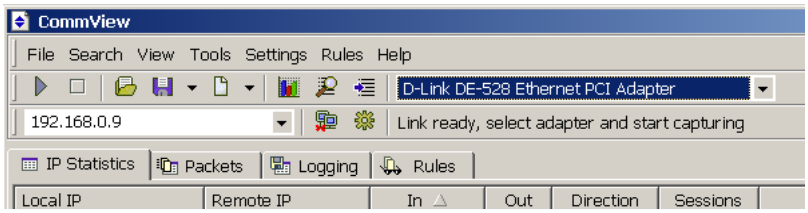
В этой главе объясняется, как использовать CommView для связи с CommView Remote Agent и наблюдения удалённого трафика. Для работы вам необходим CommView на вашем компьютере и CommView Remote Agent, запущенный на удалённом компьютере. Считаем, что Remote Agent уже успешно установлен и работает (подробности - в предыдущей главе), и, что вы знакомы с CommView. Если у вас нет копии программы CommView, возьмите её здесь и ознакомьтесь с ней, перед использованием CommView Remote Agent.

Подключение CommView к CommView Remote Agent

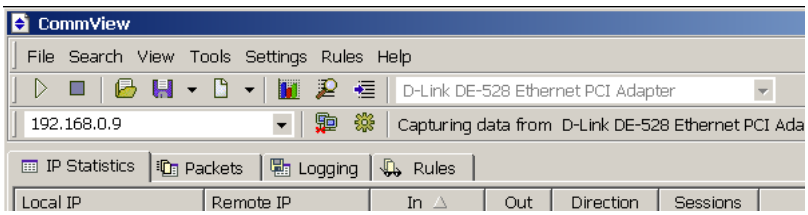
Чтобы включить режим удалённого наблюдения, выберите в меню **File(Файл)** => **Remote Monitoring Mode(Режим удалённого наблюдения)**. В дополнительной панели управления, появившейся под основной, укажите IP адрес компьютера, где запущен CommView Remote Agent, и нажмите кнопку **Connect** (Установить связь). Если вы работаете за брандмауэром (файрволом) или через прокси-сервер, или, если вы установили нестандартный номер порта на Remote Agent, вам придётся, нажав кнопку **Network Settings** (Сетевые установки), указать порт и/или ввести настройки прокси-сервера SOCKS5.



Во всплывающем окне укажите пароль доступа, заданный в установках Remote Agent. Если пароль указан верно, соединение будет сразу же установлено. Появится сообщение *Link Ready(Связь подготовлена)*, а в списке доступных адаптеров появятся все имеющиеся на удалённом компьютере адаптеры.



Теперь необходимо установить правила в закладке **Rules(Правила)**. Важно настроить их так, чтобы не превысить пропускную способность канала связи между Remote Agent и CommView, иначе вы заметите существенное замедление реакции системы. Обязательно отфильтровывайте неинтересующие вас пакеты (см. ниже). Когда всё готово, выберите в списке нужный адаптер и нажмите кнопку **Start Capture** (Начать сбор).



CommView начнёт сбор трафика удалённого компьютера, как если бы это был ваш локальный трафик, практически, нет разницы между этими двумя режимами работы CommView. Чтобы закончить удалённое наблюдение, нажмите кнопку **Stop Capture**. Можно или выбрать другой адаптер из списка или отключится от Remote Agent совсем, нажав кнопку **Disconnect**. Чтобы вернуться в стандартный режим, выберите в меню **File(Файл)** => **Remote Monitoring Mode(Режим удалённого наблюдения)**, и дополнительная панель управления исчезнет.

Советы по эффективному использованию CommView Remote Agent

Настоятельно рекомендуем обратить самое пристальное внимание на установки правил сбора пакетов (в закладке **Rules** основного окна CommView), чтобы они соответствовали целям ваших исследований. Пропускная способность канала связи между вашим и исследуемым компьютером не безгранична; чаще всего, если CommView Remote Agent установлен в сети с интенсивным трафиком, **вся** ёмкость канала будет занята попытками передавать **все** пакеты на ваш CommView. Если правила установлены так, что они не отбрасывают все нежелательные пакеты, весьма вероятна перегрузка канала связи CommView с CommView Remote Agent. Даже если вы связаны с CommView Remote Agent через каналы T1 или T3 (1.5 или 4.5 Mb/сек соответственно), удалённый компьютер может находиться в 100 Mb/сек сети; таким образом, при высокой сетевой активности, ваша линия связи может оказаться совершенно не соответствующей объёму подлежащего передаче трафика.

Если CommView Remote Agent захватывает данных больше, чем можно передать в сторону CommView, он использует буфер для пакетов, которые невозможно отправить немедленно. Размер буфера 5 Mb. Индикатор **Buffer utilization** в окне Remote Agent отображает текущее состояние буфера. Например, если в буфере находится 2.5 Mb данных, **Buffer utilization**(Занятость буфера) составит 50%. При достижении уровня занятости буфера в 100%, программа прекращает

добавлять туда новые данные и отбрасывает захватываемые пакеты, пока в буфере не появится свободное место. Не допустить потери данных можно, установив правила сбора пакетов так, чтобы буфер не переполнялся.

Безопасность

CommView Remote Agent разрабатывался с учётом требований сетевой безопасности. Доступ предоставляется только по паролю, который открытым текстом по сети НЕ передаётся, а проверяется по схеме "запрос-ответ" с использованием хэш-функции (как в сетях GSM). Если проверка пароля прошла успешно, весь передаваемый трафик компрессируется и шифруется этим же паролем. Храните пароль в строгой секретности. Если пароль попадёт в руки посторонним, они смогут получить широкие возможности по изучению вашей сети и перехвату сетевого трафика

Информация

How to Purchase CommView Remote Agent

Демо-версия имеет 30-дневный период. Ниже приведены цены на зарегистрированную, полнофункциональную версию программы:

Лицензия	**Цена, USD**
1 Компьютер	149
5 Компьютеров	499
10 Компьютеров	799

Программа CommView Remote Agent **лицензируется по компьютерам, а не по числу пользователей**. Лицензия на один компьютер даёт право установить и использовать программу на одном компьютере. Чтобы установить программу на несколько компьютеров, необходимо приобрести многокомпьютерную лицензию. Кроме того, чтобы связаться с CommView Remote Agent, необходима хотя бы одна лицензионная копия программы CommView.

Как зарегистрированный пользователь Вы получите:

- Полностью функциональную неограниченную временем использования копию программы.
- Бесплатные обновления, которые будут выпускаться в течение одного года со дня приобретения.
- Бесплатную техническую поддержку.

Покупатели из России могут приобрести программу за рубли у нашего российского дилера, компании Softkey:

http://www.softkey.ru/catalog/basket.php?prodid=3021

Покупатели из других стран могут заказать программу через наш веб сайт:

http://www.tamos.com/order/

Мы принимаем к оплате: кредитные карты, чеки, почтовые переводы и другие виды платежей. Цены и лицензионное соглашение могут быть изменены без предупреждения. Пожалуйста, посетите наш сайт для получения последней информации о продуктах.

Как с нами связаться

Web

http://www.tamos.ru/ (Российский сервер)

http://www.tamos.com/ (Сервер в США)

E-mail

sales@tamos.ru (По вопросам, связанным с продажами)
support@tamos.ru (По всем остальным вопросам)

Почта и факс

Почтовый адрес

PO Box 1385
Christchurch 8015
New Zealand

Факс: +643 359 0392 (Новая Зеландия)
Факс: +1 503 213-7764 (США)

Другие продукты компании Тамософт

CommView

CommView - это программа для проведения мониторинга сетевой активности, способная захватывать и анализировать пакеты сети Ethernet CommView собирает информацию о данных проходящих через LAN и декодирует проанализированные данные. С программой ComView вы сможете увидеть лист сетевых соединений, живую IP статистику и протестировать индивидуальные пакеты. IP пакеты декодируются вплоть до самого низкого уровня с полным анализом основных протоколов IP: TCP, UDP, и ICMP. Полный доступ к исходным данным также предусмотрен. Захваченные пакеты могут быть сохранны, чтобы в будущем провести полный анализ, а также экспортироваться в другие форматы. Гибкая система фильтров делает возможным сбрасывать пакеты, которые Вам не нужны или собирать только те пакеты, которые вы хотите захватить.

Подробнее...

SmartWhois

Удобная утилита для сбора информации о любом IP адресе или имени хоста. В отличие от стандартной Whois утилиты, SmartWhois автоматически предоставляет информацию, связанную с IP адресом вне зависимости от географического места его регистрации. За несколько секунд Вы можете узнать всё, что Вы хотите знать о пользователе: домен, сетевое имя, страну, штат или провинцию, город. Даже если по IP адресу не может быть определено имя хоста, SmartWhois будет работать.

Подробнее...

Essential NetTools

Полезный пакет для диагностики сетей и слежения за сетевыми соединениями Вашего компьютера. Он включает быстрый многопотоковый NetBIOS сканер, оболочку для NetBIOS Auditing Tool (NAT), утилиту netstat, которая отображает все сетевые соединения компьютера, монитор для слежения за внешними соединениями к открытым ресурсам Вашего компьютера, удобную утилиту для быстрого соединения к удалённым ресурсам, которая даёт пользователям Windows 95/98 возможности Windows NT при подключении на уровне пользователей, удобный редактор файла LMHosts, и другие полезные утилиты. Программа легка в использовании и является заменой таких Windows утилит, как nbtstat, netstat, NetWatcher. Она имеет много дополнительных возможностей, чем стандартные утилиты Windows похвастать не могут.

Подробнее...

DigiSecret

DigiSecret - простая, надёжная и мощная программа шифрования. В ней используется проверенный временем мощный алгоритм кодирования для создания шифрованных архивов, самораспаковывающихся EXE-файлов. В DigiSecret есть и средства сжатия файлов; Вам больше не потребуется zip-овать файлы, Вы сможете за один раз и зашифровать и заархивировать их в DigiSecret. Программа интегрируется в оболочку Windows, все операции доступны по щелчку правой кнопкой мышки по файлам. Поддерживается drag-and-drop работа с файлами.

Подробнее...