

Проверено: PRTG Network Monitor 12.2

В поле зрения – вся сеть

Д-р Готц Гутих

PRTG Network Monitor компании Paessler AG работает на платформе Windows и собирает данные о работе компьютеров, приложений и других, находящихся в сети компонентов инфраструктуры. Вся информация хранится в центральной БД и в любое время может быть использована для комплексного анализа. Приложение администратора запускается на мощном веб-интерфейсе или как приложение Windows. PRTG опирается на ряд разных технологий сбора данных, а именно: WMI, SSH, SNMP, NetFlow, JFlow и Sflow, а также перехват пакетов. IAIT решил проверить удобство и производительность данного решения в своей повседневной работе.

PRTG Network Monitor Paessler активно информирует администраторов о состоянии сетевой инфраструктуры, тем самым предупреждая их о потенциальных проблемах и помогая их предотвращать. В решение включено свыше 130 типов датчиков, предназначенных для мониторинга таких параметров, как загрузка процессоров отдельных систем, наличие свободного места на диске и утилизация сетевого интерфейса. Также имеются датчики для сетевых служб, таких как HTTP, SMTP, POP3, FTP и т.д. В данном контексте термин «датчик» не следует понимать буквально: PRTG работает без агентов – т.е. без программных компонентов, устанавливаемых на контролируемых клиентских системах. Датчики работают на центральном «зонде» (в случае необходимости, в сети может быть создано несколько зондов), регулярно опрашивая оттуда состояние клиентов по вышеупомянутым протоколам, например, WMI, SNMP или SSH. Полученные данные сохраняются в центральной БД и могут использоваться для развернутого анализа, результаты которого, в свою очередь, могут быть использованы для оптимизации сети. При возникновении каких-либо трудностей, PRTG может отправлять уведомления по электронной почте, в виде текстовых сообщений (SMS) или на пейджер, помимо остальных способов.



PRTG Network Monitor с самого начала

Тип лицензии зависит от количества датчиков. До десяти датчиков – это бесплатно. Дополнительные датчики могут докупаться по мере необходимости. Любая лицензия PRTG включает в себя полный функционал, независимо от ее размера. Также имеется 30-дневная ознакомительная версия с неограниченным количеством датчиков.

Архитектура

PRTG использует главный сервер, работающий с веб-интерфейсом Ajax. Этот интерфейс является основным инструментом управления и предлагает самый широкий набор функций. Windows-приложение администрирования Enterprise Console представляет собой альтернативный интерфейс, обладающий почти полным набором функций (по данным компании Paessler, он охватывает 95% функций веб-интерфейса). Также есть мобильный графический веб-интерфейс, представляющий данные в оптимизированном для мобильных устройств виде.

Приложения для iOS и Android завершают палитру интерфейсов данной системы сетевого мониторинга. Android-приложение (PRTGdroid) обеспечивает простой доступ к мобильному веб-интерфейсу ПО Paessler и может информировать администраторов о любых ошибках.

iOS приложение (iPRTG) получает данные от веб-сервера через API и отображает их в обычном для iPhone стиле. PRTG рекомендует использовать для работы на десктопе браузеры Chrome и Firefox, однако мы также проверили возможность использования Internet Explorer, который тоже отлично работал.

Как упоминалось выше, помимо главного сервера PRTG также использует зонды, получающие информацию от клиентов. При необходимости можно устанавливать удаленные зонды, что особенно полезно для контроля удаленных частей инфраструктуры, помимо находящихся в локальной сети. При этом вся информация собирается в одном месте. В случае установки нескольких копий PRTG, ими можно

будет управлять централизованно, с помощью Enterprise Console.

Датчики имеют так называемые каналы, собирающие информацию об отдельных параметрах. В случае датчиков памяти, например, это общий объем памяти и объем доступной памяти в процентах.

Между датчиками могут быть настроены взаимосвязи. Это позволяет, например, использовать для мониторинга веб-сервера как датчик Ping, так и датчик HTTP. При получении сообщения об ошибке от датчика Ping, система приостановит работу соответствующего датчика HTTP. Это правильно, поскольку соответствующая служба HTTP будет недоступна, если проблемный сервер не отвечает по сети. При этом администратор получит только одно сообщение об ошибке, указывающее на недоступность веб-сервера, вместо двух. Это значительно улучшает наглядность информации, особенно для систем с большим количеством датчиков.

Как правило, датчики – по областям применения – имеют очень мощную и развитую функциональность. Например, можно не только определить тот факт, что веб-сервер отвечает на запрос. Администратор может настроить систему таким образом, что она будет запрашивать конкретный контент и даже имитировать покупку в интернет-магазине, чтобы иметь гарантии того, что служба на самом деле работает так, как надо. Например, если веб-сайт был взломан, то веб-сервер по-прежнему продолжит работать, хотя показываемый им контент может полностью отличаться от того, что намеревалась показывать пострадавшая компания. Это может быть обнаружено только в том случае, если программное обеспечение для мониторинга оценивает не только доступность веб-службы, но и контент.

В качестве датчиков в PRTG в любой момент могут быть интегрированы пользовательские сценарии (скрипты). По умолчанию, все собранные данные хранятся до года, а при необходимости можно указать в настройках и больший срок хранения.



Список устройств и состояний отдельных датчиков

Тестирование

Для проведения теста мы установили в своей сети PRTG Network Monitor версии 12.2 на систему Windows Server 2008 R2, после чего использовали его для мониторинга компьютеров под управлением ОС Windows XP, Windows Server 2008, Windows 7, Windows Server 2008 R2, Red Hat и Fedora Linux, Ubuntu Linux, Mac OS и Solaris. Мы также вели мониторинг различных сетевых компонентов, включая, например, коммутаторы Cisco, маршрутизаторы Netgear и LANCOM, и даже несколько веб-сайтов, например веб-сайт IAIT, онлайн-сервисы Dropbox, Twitter, а также Skype. Учитывая, что PRTG поддерживает IPv6, мы также вели мониторинг различных систем, использующих этот протокол.

После установки ПО и настройки необходимых нам датчиков, мы уделяли особое внимание мониторингу наших сервера Exchange и среды виртуализации (на базе VMware). Мы исследовали весь набор функций ПО для мониторинга, в том числе – деревья устройств, библиотеки, карты, отчеты и уведомления о проблемах. И наконец, что не менее важно, мы пользовались приложением PRTGdroid для удаленного доступа к системе мониторинга.

Установка

Идеальным местом для установки сетевого монитора является современная ОС Windows на специально выделенном компьютере. Чтобы обеспечить высокую производительность системы, Paessler не рекомендует устанавливать PRTG Network Monitor на виртуальных машинах.

Для достижения максимальной производительности, рекомендуется использовать систему с ОЗУ 4 ГБ и несколькими сотнями ГБ свободного места на жестком диске. На используемом для мониторинга компьютере должен быть установлен пакет .NET Framework 4.0.

Установка продукта контролируется с помощью Мастера – как и при установке любого другого ПО для Windows, – и не представляет проблемы для любого администратора. От него требуется указать требуемый язык, ввести ключ лицензии и указать свой адрес (учетную запись) электронной почты. При необходимости, позднее можно будет установить отказоустойчивый кластер.

После завершения настройки откроется браузер с экраном авторизации PRTG и можно будет в первый раз войти в систему мониторинга. Как правило, здесь открывается «Гуру настройки», чтобы помочь администратору выполнить первоначальную настройку системы. В нашем случае, так как использовался сервер Windows с браузером Internet Explorer и расширенными настройками безопасности, сначала потребовалось указать страницу PRTG в качестве надежного узла, чтобы система все правильно отображала.

Гуру настройки

Гуру настройки помогает администраторам выполнить первоначальную настройку PRTG. На первом шаге он предложил нам включить SSL-шифрование доступа к веб-интерфейсу. Пользователю предоставляется возможность активировать шифрование SSL, или пропустить этот шаг. Такая возможность – принять или пропустить

рекомендации – есть на всех шагах Гуру настройки.

После выбора шифрования SSL, мы ввели с помощью Гуру настройки наш пароль администратора и вошли в учетные данные для систем Windows, включая и наш сетевой домен. Этот шаг является обязательным, поскольку дает PRTG возможность доступа к соответствующим компьютерам для запроса и получения информации. Наконец, Гуру попросил ввести учетные данные для SNMP, VMware, Xen и систем Linux, и предложил задействовать мониторинг подключения к Интернету со шлюзом и DNS серверами. На следующем шаге было необходимо указать серверы, которые PRTG должен будет контролировать в сети. Для этого Гуру предложил нам указать контроллеры домена, серверы Exchange или другие почтовые серверы, а также имена или адреса других серверов. Мы указали наш контроллер домена и сервер Exchange, а также пожелали воспользоваться поиском по сети, чтобы PRTG смог сам добавить другие наши системы.

На этом установка сервера мониторинга была закончена, и настал момент настройки мониторинга веб-сайтов и интернет-магазинов, а также подключения мониторинга облачных сервисов, таких как Google (поиск, диск и почта), Office 365, Salesforce, Dropbox, iCloud, Facebook, Twitter и Skype. И в заключение, Гуру настроек завершил автоматический поиск всех систем в нашей локальной сети. В ходе этого поиска были обнаружены все активные компоненты нашей сетевой инфраструктуры. Что касается систем VMware, PRTG также опознал хост-системы виртуальных машин и сразу представил в виде датчиков все виртуальные машины, установленные на этих хостах.



Для дополнительных устройств можно выбирать значки, которыми они будут показаны в списках.

Автоматический поиск в сети

Автоматический поиск в сети может запускаться как вручную (в любое время), так и автоматически (по заданному графику). Этот поиск представляет собой хороший

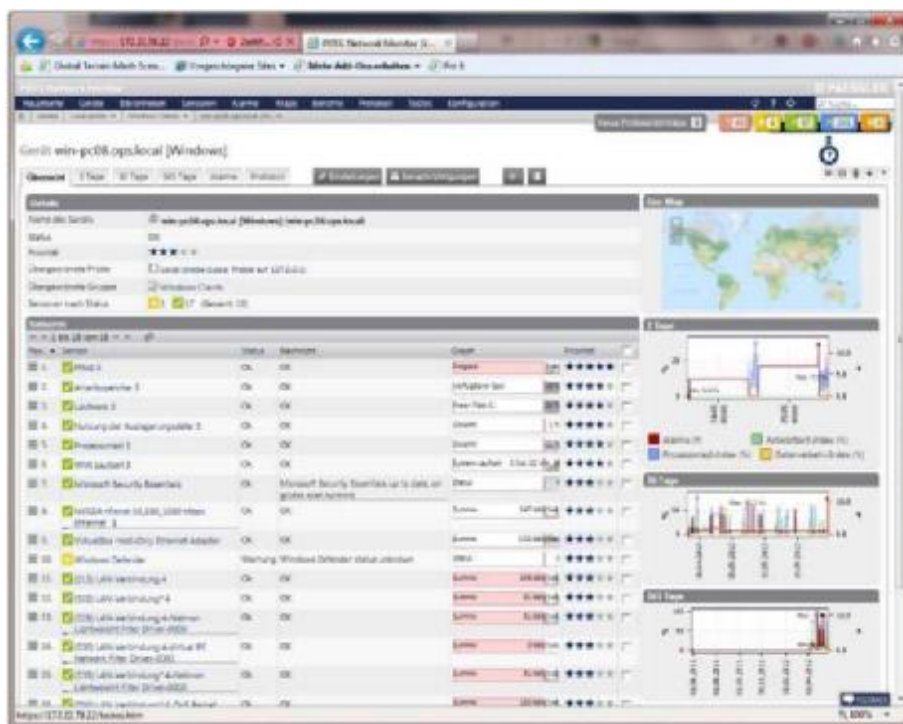
способ для поддержания актуальности настроек PRTG и добавления в него новых систем. Если пользователь захочет создать новую группу, например, со всеми серверами Windows, то все, что он должен будет сделать – это создать автоматический поиск по сети, выбрать подходящий датчик, ввести имя группы и определить способ создания датчика. Есть четыре способа: создание вручную, автоматическое создание в соответствии с устройством, подробное автоматическое создание в соответствии с устройством (этот метод позволяет создавать большое количество датчиков) и создание с помощью шаблонов устройств.

Последний способ особенно удобен, если в сети есть несколько одинаковых систем. В большинстве случаев достаточно автоматического создания датчиков и ручного добавления имеющихся датчиков, например, с функциями мониторинга для конкретных типов серверов.

Следующим шагом стало создание расписания автоматического поиска и указание диапазона адресов, для которых необходимо выполнить поиск. Есть несколько вариантов, а именно: диапазоны адресов IP класса C (IPv4), перечень отдельных адресов IP или имен DNS (IPv4 или IPv6), сетевой адрес с подсетью (IPv4) или IP с диапазоном октета (IPv4). С их помощью любой администратор сможет найти то, что относится именно к его сети.

Как только администратор введет необходимую информацию о своем диапазоне адресов, он сможет активировать разрешение имен в адреса с помощью DNS, WMI или SNMP, и отменить автоматический поиск для уже найденных адресов устройств, чтобы ускорить этот процесс.

Заключительные шаги включали в себя ввод учетных данных для систем Windows, Linux, VMware/Xen и для SNMP, а также параметров доступа к HTTP прокси. Вся эта информация может наследоваться из имеющихся настроек, так что автоматический поиск может использовать учетные данные, введенные через Гуру настроек, если это применимо. Права доступа определяют то, учетные записи каких пользователей PRTG получают доступ к результатам (найденным объектам) текущего поиска. После завершения поиска, в списке устройств автоматически появятся новые датчики, что позволит сразу же получить к ним доступ.



Развернутый список для отдельной системы содержит полный перечень контролируемых служб.

Веб-интерфейс

Завершив установку и начальную настройку, мы перешли к набору функций этого инструмента мониторинга. После входа в рабочий веб-интерфейс открывается экран приветствия, имеющий возможность вызова Гуру конфигурации, запуска автоматического поиска по сети, перехода к списку устройств, загрузки Enterprise Console, установки смартфон-приложения, вызова справки или обращения в техническую поддержку.

В верхней части окна инструментов настройки находится строка меню с основными разделами настроек, в том числе: список устройств, библиотека, оповещения о проблемах и т.д. Подпункты главного меню доступны с помощью мыши.

Меню «Home», например, содержит четыре подпункта, ведущих к разным обзорным страницам. Его (как и любую другую страницу) можно задать в качестве домашней страницы, после чего оно будет открываться сразу же после входа в систему. На обзорных страницах представлены сводные данные, содержащие наиболее важные датчики (пользователь может отметить их как «избранное»), журналы, задачи, уведомления о проблемах, предупреждения, группы, устройства, датчики, датчики с «необычными» состояниями и недавние записи журнала.

Также доступна карта сайта со всеми ссылками, доступными для активной учетной записи пользователя, возможностью вызова мобильного веб-интерфейса и вышеупомянутым экраном приветствия. Т.о., в меню «Home» находится широкий спектр параметров настройки, позволяющих PRTG Network Monitor предоставлять пользователю расширенную информацию о сети сразу же после его входа в систему.

На правой стороне находится функция контекстной справки, поясняющая почти все

параметры настройки. Данная справка имеется на каждой странице инструмента настройки.

Список устройств

Второй пункт меню – вышеупомянутый список устройств. Это ядро Network Monitor, отображающее каждую контролируемую систему с ее датчиками в виде древовидной структуры и соответствующих групп. Пользователи сразу могут увидеть, где появились ошибки, какие выданы предупреждения и т.п., так как датчики с ошибками становятся красными, с предупреждениями – желтыми, а датчики без каких-либо проблема отображаются зеленым цветом. Список устройств – это не только способ отображения данных. При необходимости сюда же могут добавляться удаленные зонды, а также новые группы, устройства и датчики. Кроме того, географическая карта показывает местонахождения каждой контролируемой системы, а обзорные графики показывают информацию об уведомлениях, использовании процессора, трафике данных и времени отклика. В стандартной конфигурации каждый график показывает состояние за 2, 30 и 365 суток.

При нажатии на группу, компьютер или зонд, открывается соответствующий развернутый список. Если, например, все имеющиеся у компании серверы Windows объединены в одну группу, то при нажатии на эту группу будут отображаться только внесенные в эту группу системы. Таким образом, ИТ-персонал может ограничивать показ отдельными компьютерами и даже отдельными датчиками.

Если система показывает данные для одного компьютера, то все найденные на этом компьютере датчики отображаются в виде списка. Дополнительно к данным датчиков, включая название и состояние, этот список содержит небольшие диаграммы, наглядно показывающие важную информацию (например, загрузку вычислительных мощностей).



Радиально-лучевая диаграмма обеспечивает наглядность и доступность

представления информации о контролируемых компонентах. Детализация увеличивается при движении от центра наружу, а индивидуальные системы передают свой статус к центру. Тем самым Paessler гарантирует, что внутреннее кольцо, представляющее всю сеть, будет показывать отсутствие проблем только тогда, когда проблем нет ни с одной из внешних систем.

Список индивидуальных датчиков отображает подробную информацию, в том числе в реальном времени за 2 и 30 дней. Кроме того, пользователи могут настраивать параметры датчика и менять имена, интервалы сканирования, приоритет (это определяет порядок отображения объектов в списке) и права доступа.

Датчики также можно настроить таким образом, чтобы они отправляли уведомления при превышении определенных порогов или достижении определенных состояний. Например, если состояние датчика изменилось «вниз», то по истечении заданного промежутка времени администратору может быть отправлено сообщение. Отдельным каналам датчиков могут быть назначены пределы, и они могут быть настроены на отображение в диаграммах и таблицах. И наконец, администраторы могут добавлять сюда свои комментарии и просматривать историю показаний по каждому датчику.

Помимо вышеперечисленных возможностей, имеются вкладки в списках устройств и группах, в которых данные отображаются в режиме реального времени в виде графиков и таблиц, а также может быть просмотрена история их изменений. Доступны 2-дневный, месячный и годичный варианты отображения, а также возможность просмотра истории изменения за произвольный период времени.

Пункт меню «Management» (управление) также присутствует в списках устройств и групп. Здесь пользователь может расположить датчики по своему усмотрению, используя функцию перетаскивания.

На вкладке настроек, пользователи могут приостановить работу всех датчиков группы или устройства, и указать вариант управления датчиком (автоматический, ручной и т.д.). Кроме того, можно изменять учетные данные устройства, задавать расписание и менять другие параметры, заданные по умолчанию в ходе первоначального поиска по сети. Вкладки для создания уведомлений, ввода комментариев и просмотра истории завершают набор функций для настройки групп и устройств.

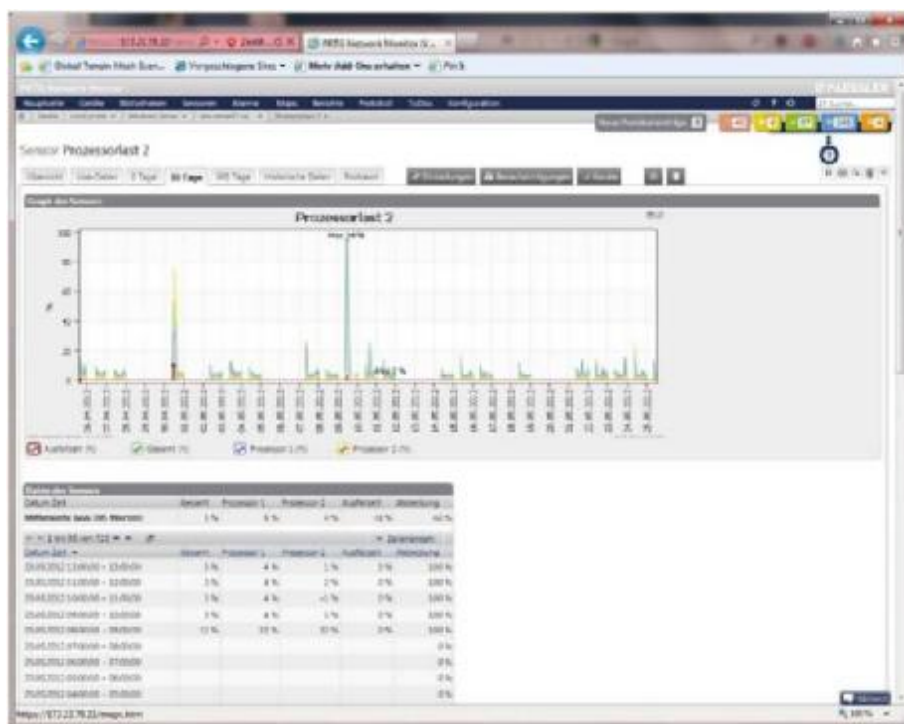
И еще один момент, который стоит отметить: функция Multi-Edit, которую можно использовать для одновременного выбора и редактирования нескольких объектов в датчике и списках устройств. Она особенно полезна одновременной настройке или приостановке нескольких датчиков.

Во время теста мы обратили внимание, что деление администрируемой сети на группы, приборы и датчики помогло нам сохранять четкое представление об инфраструктуре даже при работе в среде с множеством компонентов. С одной стороны, сигнал и уведомление могут быть настроены на активацию ошибкой, возникающей в любом месте в пределах всей группы компьютеров.

С другой стороны, уведомления могут быть настроены таким образом, чтобы в качестве триггера использовался только один датчик в одной системе. Таким образом, параметры уведомлений и анализа могут гибко перенастраиваться под требования конкретных ситуаций и сотрудников, не снижая при этом понятность всей системы.

Библиотеки

В отличие от списка устройства, библиотеки позволяют пользователям создавать собственные списки по различным критериям. Списки, объединяющие устройства по техническим аспектам, таким как операционная система и роль в сети, могут быть организованы так, чтобы отражать организационную структуру компании и ее отделов (маркетинг, бухгалтерия, ИТ, управление, и т.п.). Отдельные библиотеки могут создаваться и редактироваться непосредственно в браузере, с помощью перетаскивания.



ПО для мониторинга в графической форме отображает данные и результаты измерений по каждому датчику. На иллюстрации показана загрузка процессора сервера за один месяц.

Чтобы вставить библиотеку, пользователю достаточно ввести имя и права доступа для объекта, после чего новая библиотека сразу станет доступна для дальнейшего использования. Изменения в существующие библиотеки могут вноситься в любое время. В ходе тестирования у нас не возникло никаких трудностей с использованием библиотек.

Датчики

Список датчиков содержит все датчиков с их состояниями и небольшой график, отображающий использование пропускной способности сети и другую важную информацию. При создании нового датчика, PRTG Network Monitor сначала спрашивает у администратора, должен ли датчик принадлежать новому или уже имеющемуся устройству, какой символ у устройства, использует ли соединение протокол IPv4 или IPv6, какие учетные данные и должен ли датчик создаваться вручную или с помощью автоматического поиска.

Если администратор принимает решение о создании датчика вручную, он может

выбрать один из 131 типа стандартных датчиков. Компания Paessler использует категории, позволяющие упростить этот процесс.

Пользователь может ответить на вопросы, чтобы найти соответствующий тип датчиков. Такими вопросами являются: «Monitor what?» (что контролируем: доступность/время безотказной работы, пропускную способность/трафик, скорость/производительность, загрузка процессора, использование дискового пространства, использование памяти, параметры оборудования, сетевую инфраструктуру, пользовательские датчики), «Target System Type?» (тип системы: Windows, Linux/MacOS, виртуализация ОС, файловый сервер, сервер электронной почты, SQL Server), «Technology Used?» (используемая технология: Ping, SNMP, WMI, HTTP, SSH, перехват пакетов, NetFlow, Sflow, jFlow). С помощью этих категорий мы смогли быстро и эффективно настроить датчики, которые требовались для мониторинга наших систем Exchange и среды vSphere.

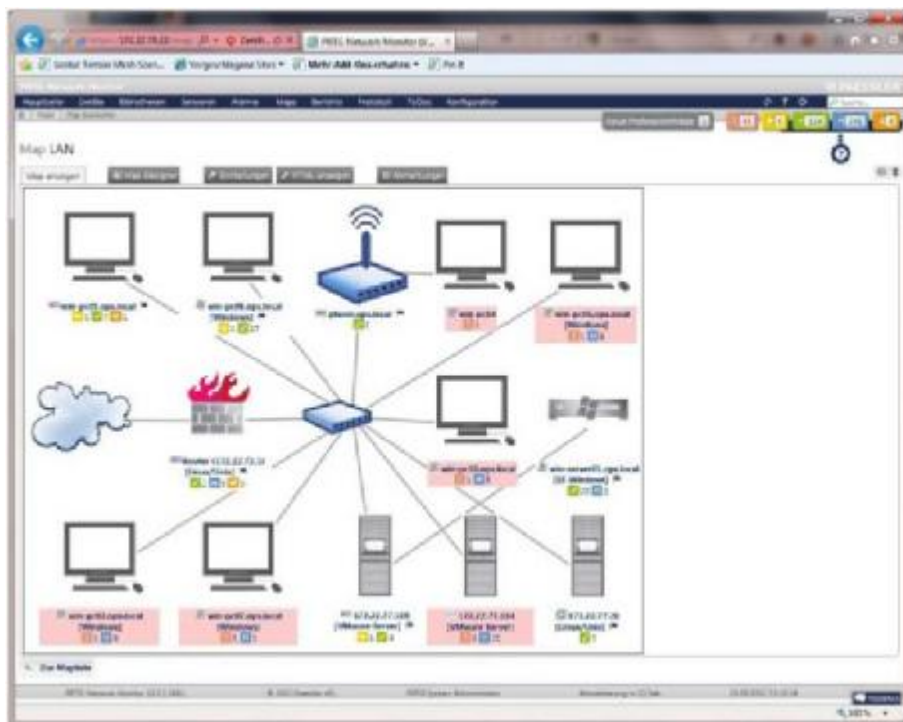
В меню датчиков (Sensors) имеются различные параметры и варианты визуализации данных и результатов датчиков. Сюда относятся списки топ-10 по разным параметрам, включая «Best Availability» (самый доступный), «Fastest Ping» (самый быстрый Ping), «Worst Downtimes» (худшие простои), «Slowest Ping» (самый медленный Ping), «Lowest Bandwidth Usage» (минимальное использование полосы пропускания), «Fastest Website» (самый быстрый веб-сайта) и т.д. Списки упорядочены в соответствии с текущим состоянием, временем работы/простоя, по группам и типам, а также по доступности. Также есть возможность сравнения датчиков и просмотра исторических данных. В ходе тестирования это дало нам очень интересную информацию о нашей сети.

Сигнализация и уведомления

PRTG Network Monitor предлагает расширенные функции сигнализации в виде уведомлений. Аварийные сигналы также можно использовать для автоматизации перезагрузки и выполнения сценариев PowerShell, командных файлов и библиотек DLL. PRTG также содержит список текущих аварийных сигналов и предупреждений. При наведении указателя мыши на список (это справедливо и для других списков), веб-интерфейс показывает в обзорном окне наиболее важные данные и диаграммы, относящиеся к соответствующей записи. Это очень полезно, т.к. позволяет быстро просмотреть несколько записей, избавляя от необходимости открывать каждую из них по отдельности.

Карты

Карты обеспечивают графическое представление сети, которое может быть улучшено с помощью фоновых изображений. Например, может быть создана карта размещения всех компьютеров в здании, на которой состояние каждой из систем отображается рядом с ее обозначением на карте. Новые карты могут создаваться в любой момент и даже могут публиковаться, предоставляя доступ к находящейся на них информации третьим лицам. Карта также является идеальным вариантом для домашней страницы браузера, открываемой сразу же после входа в систему. Также карты могут легко встраиваться во внешние веб-сайты. Карты могут создаваться – как и библиотеки – путем перетаскивания объектов с дерева устройств.



Карта сети в качестве домашней страницы

Raessler предоставляет дополнительные символы для карт, изображающие прозрачные компоненты, такие как неуправляемые коммутаторы и внешние системы (например, Интернет). Это позволяет без проблем строить на карте связи между отдельными системами. Мы решили, что в целях тестирования будет полезно создать общую карту нашей локальной сети, и использовали ее в качестве домашней страницы.

Отчеты

Система мониторинга позволяет формировать отчеты, в которых используются и данные, и графики. Имеются как разовые, так и периодические отчеты. Периодичность выдачи отчетов может быть указана вручную. Отчеты могут отображаться в формате HTML, записываться в формате PDF и пересылаться по электронной почте. В ПО включены различные стандартные отчеты, такие как «100 Fastest HTTP Sensors», «100 Slowest Ping Sensors» и т.п. Также предусмотрены отчеты о пропускной способности, загрузке процессора, использовании памяти, дискового пространства и о доступности. Все отчеты могут быть полностью перенастроены.

Отчеты могут сохраняться, чтобы при необходимости использоваться вновь. Датчики, используемые в отчете, могут выбираться вручную или по тегам. При выборе по тегу создаются динамические отчеты: если администратор назначит одну из таких меток датчику или группе, то они будут включены в соответствующий отчет.

Для удаления компонента отчета, администратору будет достаточно удалить нужный тег. Отчеты могут формироваться и рассылаться по расписанию. Мы не встретили в этом месте никаких проблем.

Журналы

PRTG отображает свой журнал в виде списка. Интервал и число строк, которые должны быть показаны в списке записей журнала, могут задаваться в любое время. Записи могут быть показаны все сразу, или могут быть отфильтрованы по группам, системным событиям, или по изменениям статуса (таким, как: «OK», «down», «paused/resumed», «acknowledged» или «unusual»).

Задачи (To-Dos)

Задачи играют роль службы уведомлений для пользователя. Они включают в себя сведения о том, что должен подтвердить администратор, в том числе о доступности новых версий ПО или об активации новых датчиков. Система также использует их для помощи пользователям новых отчетов.

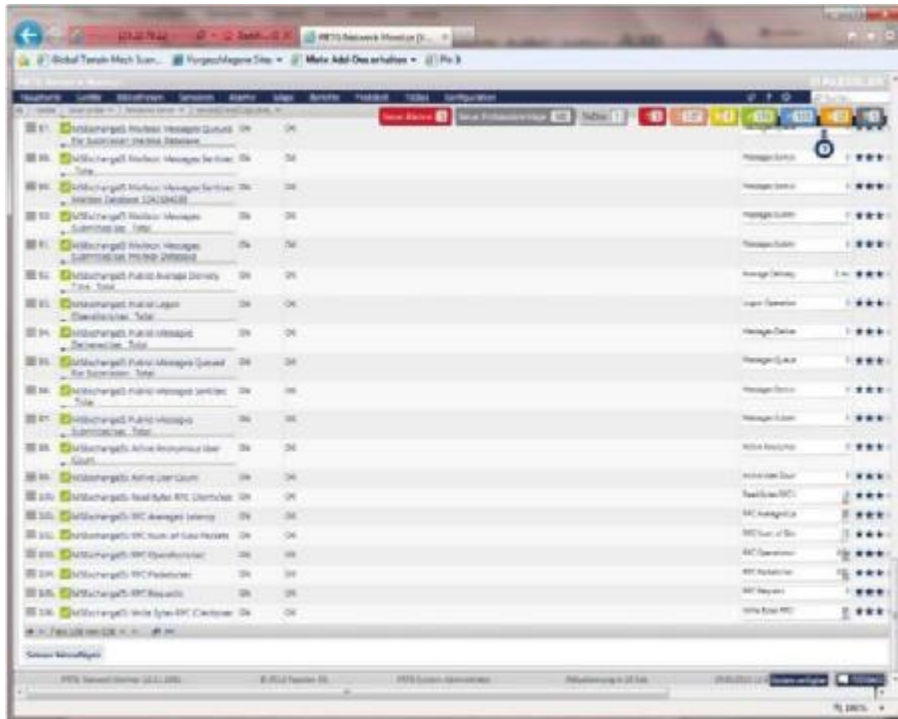
Настройка

В меню настроек собраны параметры управления PRTG Network Monitor. Тут же находятся настройки учетной записи (имя, пароль, часовой пояс, адрес электронной почты, настройки уведомлений и т.д.). Кроме того, в «PRTG status» отображается информация о версии ПО, ОС, времени, загрузке процессора, лицензии и т.д.

Администраторы могут использовать PRTG status для получения снимка БЛ, если им потребуется помощь службы поддержки компании Paessler, для перезапуска всех зондов и создания файл состояния зонда. Функция «автоматическое обновление» поддерживает актуальность версии PRTG Network Monitor. В нашем тесте она работала безупречно. Еще полезное: администрирование системы. Здесь администратор может настраивать графики и цвета, задавать имя сайта PRTG и выбирать провайдера карты (MapQuest, Nokia Maps, CloudMade или Google). Инструмент мониторинга также может интегрироваться в домен Windows, что даст ему возможность использовать существующие учетные записи пользователей внутри сети компании. Кроме того, здесь могут быть указаны пороговые значения, чтобы выявлять необычные инциденты и поведение систем.

Другие пункты отвечают за настройки для отправки уведомлений (через внутренний или внешний почтовый сервер), за связь с внешними датчиками и за работу с учетными записями пользователей. Для разных задач мониторинга могут создаваться разные учетные записи. Пользователи могут быть разбиты на группы, для которых могут быть настроены варианты уведомлений и права их обработки («Read/Write» или «Read only»). Команды меню для управления кластерами, загрузки дополнительного ПО (Enterprise Console, приложения для мобильных устройств и установочные файлы для удаленных датчиков).

Лицензия определяет набор функций инструмента, а также документации по PRTG API. Процедура настройки инструмента понятна и прозрачна, в том числе благодаря хорошей функции помощь, и необходим лишь короткий ознакомительный этап.



Функция мониторинга Exchange поставляется с большим количеством датчиков

Приложение для Android

PRTGdroid дал нам возможность безопасного доступа к PRTG Network Monitor, в любое время и из любого места. Потребовалась минимальная настройка, а мобильный веб-интерфейс прекрасно подошел для просмотра данных. Большие значки обеспечивают удобство сенсорного интерфейса. Учитывая возможность использования любых браузеров, устанавливать данное приложение не обязательно, но оно имеет более развитую функциональность, чем мобильный веб-интерфейс, и очень удобную функцию получения уведомлений на мобильное устройство.

Мониторинг Exchange

Paessler обеспечивает мониторинг очень большого числа параметров сервера Exchange. Система дает в распоряжение пользователей в общей сложности 97 датчиков, специально предназначенных для контроля различных параметров систем Exchange, включая память, БД и число активных пользователей.

Некоторые датчики очень просты и интуитивно понятны, например датчик, подсчитывающий количество уведомлений, отправляемых в секунду, или датчик, информирующий администраторов о числе подключений к серверу в секунду. Другие уже не столь просты, такие как «Database Cache % Hit edgetransport». Как правило, при мониторинге серверов Exchange важно держать под контролем отдельные почтовые очереди, что позволяет сразу же обнаруживать проблемы с отправкой электронной почты. Количество писем, отправляемых в секунду, так же важно: этот датчик используется для определения того, не используется ли находящийся в сети компьютер для рассылки спама.

Также должны контролироваться процессор, использование памяти, а также почтовые службы POP3, IMAP4, SMTP и очереди перераспределения внутренних сообщений по

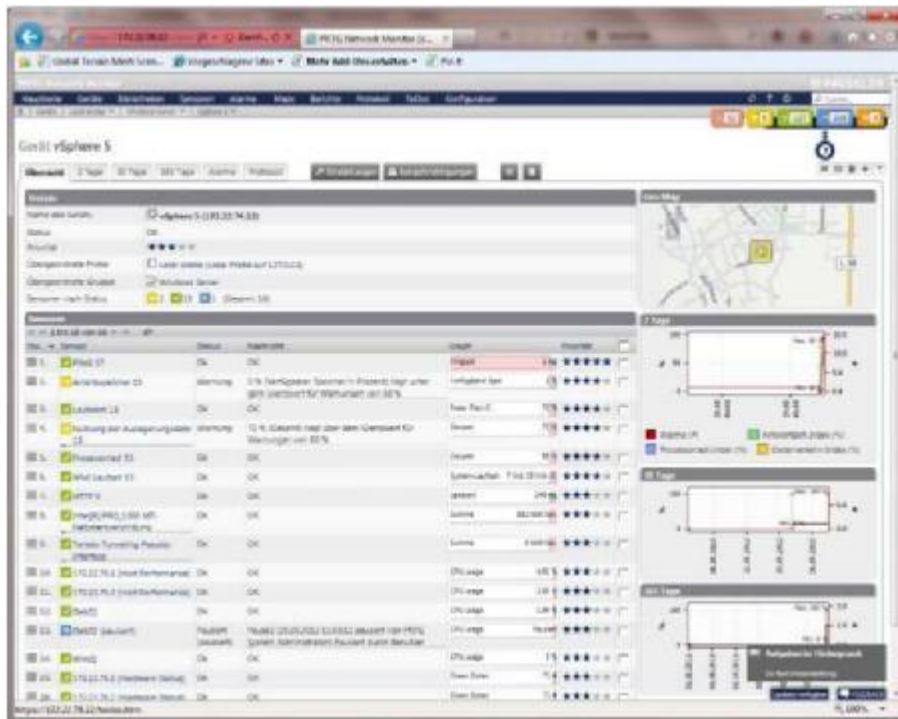
ящикам электронной почты. Если здесь нет никаких проблемы, то весьма вероятно, что сервер Exchange пребывает в хорошей рабочей форме.

Также не стоит забывать про датчик «Roundtrip Sensor» (проверка прохождения почтовых сообщений наружу и обратно). Он отправляет письмо на внешний почтовый сервис, который должен быть заранее настроен администратором на автоматическое возвращение письма. Это позволяет администратору определить, сколько времени требуется для отправки сообщения на выбранный почтовый сервис и его получения обратно. В ходе тестирования, мониторинг наших серверов Exchange 2010 работал безупречно.

Мониторинг vSphere

При мониторинге сред виртуализации на основе VMware (мы использовали в тесте системы VSPHERE 5 и ESXi 5) следует иметь в виду следующее: если учетные данные для узлов виртуализации введены правильно, то автоматический поиск по сети найдет систему, распознает ее в качестве хоста ESXi и мгновенно настроит датчики для мониторинга виртуальных машин, работающих в системе. Весь этот процесс невероятно прост и работает прямо «из коробки». При работе с серверами VSPHERE, управляющими несколькими системами ESXi и VMotion, используемой для перемещения виртуальных машин (VM) с одного узла на другой для балансировки использования вычислительных мощностей, вышеописанная процедура использоваться не может. Если VMotion перемещает VM с одного хоста на другой, то этот процесс включает в PRTG сигнал тревоги, т.к. VM внезапно исчезает с соответствующего хоста.

В этом случае хосты ESXi должны контролироваться через сервер VSPHERE, а не непосредственно. При этом PRTG рассматривает хосты ESXi с точки зрения VSPHERE и понимает, что VM по-прежнему работает, но на другом хосте. Чтобы все это настроить, потребуется немного поработать руками. Сервер VSPHERE – это программа для Windows, работающая на сервере Windows. При автоматическом поиске этого сервера, ПО Paessler устанавливает стандартные датчики для Windows, но не устанавливает датчики VMware и администратор должен установить их вручную. При этом учетные данные для сервера ESXi не могут использоваться в качестве таковых для окружения VMware. Вместо этого необходимо использовать одну из учетных записей пользователей Windows, имеющих доступ к серверу VSPHERE. В ходе нашего теста с этим не возникло никаких проблем.



При мониторинге окружения VMware важно контролировать сервер VSPHERE, а также отдельные хосты

Заключение

PRTG Network Monitor полностью убедил нас в своих возможностях. Система проста в установке, а благодаря Гуру настроек (Configuration Guru) обеспечивается удобство и быстрота процедуры установки и настройки. Главной особенностью является то, что данная система не использует установку агентов на контролируемых систем. Это не только экономит рабочее время ИТ-отдела, но и избавляет от необходимости как-либо касаться работающих в сети систем, что особенно важно в случае критически важных систем.

Мы также должны подчеркнуть невероятно широкую функциональность этого ПО. Компания Paessler вложила много усилий в создание эффективных, мощных датчиков для всех серверов и систем, используемых в современных ИТ-средах. Это относится не только к облачным службам, таким как Dropbox и Salesforce, но и к мониторингу виртуальных сред и стандартных приложений, таких как Exchange. Администратор может отслеживать даже сетевой трафик – с помощью NetFlow, Sflow, JFlow и перехвата пакетов. В большинстве случаев, автоматический поиск по сети способен самостоятельно установить все необходимые датчики. При необходимости установки дополнительных датчиков, это делается быстро и не должно представлять никакой сложности для сетевых специалистов. Другими положительными моментами являются библиотеки и карты. Они обеспечивают гибкость и большую понятность вариантов представления, что важно не только для технического персонала, но и для сотрудников из других отделов. Для этого не требуется каких-то значительных усилий, а созданные карты даже могут публиковаться на внешних веб-сайтах. Всеобъемлющая, высокопроизводительная функциональность в области уведомлений о событиях и создания отчетов довершают общее положительное впечатление, которое мы получили от тестирования PRTG Network Monitor.