Добрый день уважаемые читатели. Сегодня хочу вас познакомить с новой развивающейся системой мониторинга — **Veliam**. С ее помощью можно не только мониторить инфраструктуру, но и подключаться к наблюдаемым хостам по rdp, ssh или winbox. Возможность управления сразу показалась мне любопытной, поэтому я решил, что продукт найдет своего пользователя и будет востребован.

Содержание:

Введение

Сразу говорю, что данная статья заказная и мне оплатили ее написание. О системе ранее я не слышал. Впервые узнал, когда ко мне обратился заказчик и предложил написать обзор. Каких-то жестких требований по написанию нет. Я пишу в свободной форме так, как привык писать статьи. Я разверну систему в своей тестовой лаборатории, посмотрю как она работает. Процесс установки и настройки опишу в статье. В заключении выскажу свое мнение о продукте.

Так как продукт только разрабатывается, функционал ограничен и может показаться скудным, в сравнении с более зрелыми системами. Но при этом программа пока полностью бесплатна. Если она закрывает ваши потребности, почему бы ее не попробовать. Плюс к этому система очень легко и быстро разворачивается. Не нужны специальные знания и навыки, как с многими популярными системами мониторинга.

Сайт программы — https://veliam.com, Там описание, основные возможности, видео, документация.

Что умеет Veliam

Для работы системы мониторинга Veliam, необходимо зарегистрироваться в личном кабинете https://lic.veliam.com. После подтверждения почтового адреса, можно будет зайти в личный кабинет. Основные возможности программы:

1. **Мониторинг базовых метрик** серверов и компьютеров с операционной системой Windows. В комплекте готовые триггеры и оповещения.
2. **Удаленный доступ** через сервер мониторинга к наблюдаемым хостам по rdp, ssh или winbox для роутеров Mikrotik.
3. Готовые **оповещения в Telegram**. Работают из коробки, настраиваются легко и быстро.
4. Проверка доступности с помощью **icmp (пинг)** любых узлов сети, которые на него отвечают.
5. **Простая и быстрая установка** сервера мониторинга на любую Windows систему. Справится продвинутый пользователь, не обязательно системный администратор.
6. **Мониторинг без агентов**. На целевые сервера ничего ставить не нужно. Мониторинг выполняется с помощью службы WMI.

Еще раз отмечу, что на текущий момент система может мониторить только Windows хосты. Система мониторинга Veliam завязана на взаимодействие серверной части, установленной у вас, с облачной частью мониторинга, расположенного у авторов программы. Удаленные подключения к серверам работают через облачную службу системы. Благодаря этому подключаться можно без всяких пробросов портов и разрешение на firewall. Целевые сервера могут быть за NAT.

Система сделана с заделом на интеграцию с helpdesk. Уже сейчас это видно по автоматически создаваемым инцидентам, на основе сработанных триггеров. Инциденту можно поменять статус, назначить исполнителя или просто закрыть его. То есть в будущем это будет не просто система мониторинга, а комплекс по мониторингу и управлению инфраструктурой с helpdesk системой, с распределением ролей между техническими специалистами.

Установка системы мониторинга Veliam

Установка системы очень проста. Справится практически любой пользователь. Вам надо будет выполнить несколько шагов:

1. Зарегистрироваться в личном кабинете на сайте.
2. Установить клиентское приложение, которое устанавливается на машину оператора системы. Связать это приложение с личным кабинетом.
3. Установить серверную часть на Windows машину в локальной сети, за которой будет вестись наблюдение. Все данные будут поступать на нее.

Итак, скачиваем клиент, ссылка на который есть на главной странице сайта, в шапке.

Устанавливаем его на виндовую машину. В принципе, это может быть тот же компьютер, где будет установлена серверная часть. Но чтобы было удобно пользоваться удаленным подключением к серверам со своей рабочей машины, устанавливать клиент лучше сразу на нее. Приложение под Windows, используется стандартный установщик. Проблем нет никаких.

Дальше скачиваете серверную часть и устанавливаете ее куда-то в локальную сеть, за которой будете наблюдать. Я поставил на обычную систему Windows 10. Сама серверная часть, судя по компонентам, которые устанавливаются, построена на базе:

- Apache
- Php 7.2
- Maria DB

Теоретически, возможно появление версии под Linux. После установки серверной части, вам нужно будет ее связать с личным кабинетом, просто введя свои данные для подключения к нему.

Сервер мониторинга появится в клиенте с очень длинным ID. Его можно сразу переименовать. На этом установка закончена. Никаких заморочек и сложностей. Вникать ни во что не надо. Можно воспользоваться документацией на сайте, которая предельно короткая, потому что реально все просто и интуитивно понятно.

Настройка мониторинга и добавление объектов

После установки серверной части, можно либо вручную добавить хосты для мониторинга, либо просканировать сегмент сети. Я выбрал сканирование, чтобы посмотреть, как это работает. Для этого выделяем в клиенте сервер мониторинга, нажимаем правую кнопку мыши и выбираем *Сканировать сети*.

Дальше указываете сегмент сети и ждете завершения. У меня просканировал быстро, секунд за 20. После этого автоматически появились новые хосты. В

качестве названий были ip адреса. Я их сразу переименовал для удобства.

Система автоматически просканировала хосты и определила сервисы, работающие на популярных портах. Они перечислены в колонке *Ресурсы*.

Для того, чтобы система начала собирать данные с Windows машины, необходимо добавить учетную запись от целевого сервера. Если у вас на всех серверах одна и та же учетная запись, например доменная, ее можно указать сразу для всего сегмента сети. Если данные отличаются, то отдельно для каждого сервера.

Если учетные данные верны и настроен, либо отключен, firewall на сервере, данные сразу же начнут поступать в течении минуты. В процессе тестирования, я заметил, что на один хост я добавил учетную запись в формате простого имени, без домена. На другом сервере при этом я получил ошибку:

```
Код ошибки: 80070005
Текст ошибки: Отказано в доступе
```

Ошибка ушла после того, как я добавил учетку в формате Имя сервера/Учетная запись. После этого информация стала поступать в систему.

Собираемые метрики

После того, как вы настроили учетную запись для сбора данных и убедились, что данные поступают, можете посмотреть на собираемую информацию. Для этого надо выбрать хост и перейти в раздел *Информация*.

Вам будут доступны следующие данные:

- Графики загрузка процессора, памяти, дисков.

- Версия системы.
- Подробное описание процессора, памяти, диска, сетевого адаптера.
- Список локальных пользователей.
- Сетевые папки.
- Установленное ПО.
- Остановленные службы в режиме запуска Auto.
- История входов пользователей в систему.

Информации не очень много, и она вся по делу. Ничего лишнего. Думаю, сюда имело бы смысл добавить основные системные журналы. Помимо этого о любом хосте доступна информацию по пингу.

А так же статистика недоступности.

Вот в целом и все по метрикам. Посмотрим теперь на уведомления и инциденты.

Инциденты и уведомления в Veliam

В программу зашиты несколько базовых триггеров, которые срабатывают при:

1. Сетевой недоступности хоста.
2. Высокой нагрузке на CPU.
3. Высокой загрузке RAM.
4. Заканчивающемся свободном месте на диске.

При этом я заметил небольшой баг — cd-rom тоже считается диском и на него постоянно срабатывает триггер, так как свободного места там всегда 0. Передал это разработчикам. Думаю, поправят через некоторое время.

При срабатывании триггера создается инцидент, который похож на тикет в системе регистрации заявок.

Заявку можно назначить либо себе, либо другому пользователю системы. Можно закрыть, отложить, написать комментарий и т.д. Все изменения заявки фиксируются в истории. Я узнал, что в настоящее время разрабатывается и тестируется расширенный функционал по этому направлению. Есть альфа версия, но она еще не готова к публичному тестированию.

Параллельно с инцидентом отправляется уведомление на почту с информацией о событии.

Уведомления могут быть отправлены как на почту, так и в telegram. Настройки очень простые, выполняются в клиенте, в разделе *Настройки -> Уведомления*.

Сначала я не мог найти информацию в инциденте о самом хосте, к которому он относится. Потом заметил, что надо прокрутить инцидент вниз, там будет вся его история и в том числе там же информация о хосте и сработавшем триггере. Список инцидентов выглядит примерно так.

В зависимости от того, в каком статусе инцидент находится, различается его цвет и поведение (мигает или нет). Этот функционал будет дорабатываться, так как он напрямую связан с Helpdesk.

Разграничение прав доступа

В системе имеется возможность заводить разных пользователей и назначать им права в зависимости от их обязанностей. Причем настройка прав достаточно гибкая.

Для добавления пользователя надо в клиенте перейти в раздел *Панель администратора -> Контроль доступа -> Пользователи*. Есть возможность самостоятельно создавать роли с предустановленными разрешениями.

Удаленное подключение к хостам

Теперь рассмотрим очень интересную возможность, которую я не видел в других системах мониторинга, с которыми доводилось встречаться — возможность удаленно подключаться к хостам. Напомню, что это возможно делать по протоколам rdp и ssh, а так же с помощью winbox к оборудованию Mikrotik.

Для подключения к хосту достаточно просто нажать мышкой на его имя. После этого будет запущен либо rdp клиент, либо ssh (putty), либо winbox, в зависимости от типа хоста. Подключение пробрасывается через облако сервиса, поэтому прямой доступ не нужен. По сути, подключаться можно откуда угодно.

Вы можете вручную вводить каждый раз учетные данные для каждого подключения. Если не хочется это делать, то их можно задать для хоста, либо сразу для группы хостов. Тогда подключение будет выполняться автоматически, что весьма удобно.

Один этот функционал, к тому же бесплатный, интересен сам по себе. Не нужно заморачиваться с пробросом портов или использованием каких-то отдельных систем для удаленного доступа. Если есть опасения за сохранность логинов и паролей, их можно не сохранять, а вводить каждый раз вручную.

Мониторинг Web сайта с помощью Veliam

Еще одна небольшая, но полезная возможность — мониторинг web сайта. Его достаточно по адресу добавить в систему. Мониторинг будет проверять доступность сайта. Если не доступен — оповещение. Просто, быстро и удобно. Альтернатива платным или более сложным системам.

Общее впечатление о системе

Я рассмотрел практически весь функционал. Как вы видите, он пока небольшой. Но при этом все работает нормально. А самое главное — очень легко настраивается. Я думаю на этом будет сделан акцент и дальше будет поддерживаться эта простота. Я без проблем во всем разобрался за один вечер, изредка заглядывая в документацию. Она, как и сам продукт, простая и лаконичная, но при этом содержит все необходимое для настройки.

Настроить Veliam сможет практически любой продвинутый пользователь компьютера. К примеру, если вы владелец небольшого бизнеса и у вас вовсе нет сисадмина, можете сами настроить простейший мониторинг и удаленный доступ. Я сталкивался с владельцами небольшого бизнеса, которые сами занимались настройкой и обслуживанием своих простых информационных систем. У меня они заказывали консультацию, либо разовую настройку каких-то систем.

Особенно понравился удаленный доступ. Причем реализован он очень просто на базе стандартных программ — rdp, ssh, winbox клиентов. Создается локальный шлюз для проброса портов на целевые хосты через облако системы.

Из минусов отмечу клиентское ПО. Оно, по сути, обертка для доступа к серверу по http. Я так понял, что он написан, как многие современные приложения, на Electron. Но тут уже выбирать особо не приходится. Если у таких гигантов как Microsoft (Skype) и Slack не находится ресурсов для написания нативных приложений, откуда они возьмутся у небольшого стартапа Veliam. Приходится привыкать к подобным приложениям. Суть моей претензии в том, что они просто не очень отзывчивые и кушают оперативу, ведь под капотом у них движок от Хрома.

> Как позже мне сказали разработчики, клиент написан с помощью Lazarus, а не Electron. Так что я ошибся, но ведет он себя по факту схоже с приложениями на Electron.

Могу порекомендовать к использованию систему, кому ее функционала достаточно. На текущий момент она полностью бесплатная, потому что только начала свое развитие. В будущем появятся платные тарифные планы и останется какой-то бесплатный функционал с ограничениями, как это обычно бывает. Если останется так же как сейчас, ограничение на 50 хостов, то это будет отлично. Для небольшой инфраструктуры этого будет достаточно.

Заключение

В целом, считаю, что продукт закрывает потребности некоторых пользователей и будет полезен. Найдет свою аудиторию. Возникают вопросы по

безопасности, так как работа завязана на онлайн службы. Этот вопрос актуален для всех услуг, работающих по модели SaaS (Software-as-a-Service), а их с каждым днем все больше и больше. Так что в этом плане ничего уникального. Для тех, кто не готов мириться с тем, что его данные будут доступны третьей стороне, будет использовать свои сервисы, в том числе мониторинг.

Я в свое время использовал отличный мониторинг, работающий по схожей модели — newrelic. Там вообще не было своей серверной части. Все данные с агентов сразу уходили в облако. Мониторинг очень крутой, дорогой и популярный. Со временем, они убрали бесплатный тариф, чем меня огорчили. Аналогов с сопоставимым функционалом больше не встречал.

В общем, попробуйте, посмотрите. Возможно в вашей инфраструктуре найдется место для системы управления и мониторинга Veliam.