MaxPatrol VM версия 2.7

Обзор новых возможностей

Дата редакции документа: 15.05.2025

Содержание

1. Новые возможности

В этом разделе перечислены новые возможности MaxPatrol VM и дано их краткое описание.

1.1. Подтверждение добавления нового приложения

Начиная с версии 2.7 вы можете включить необходимость подтверждать добавление новых приложений. В этом случае при получении запроса на добавление нового приложения в PT MC вы увидите соответствующее сообщение в центре уведомлений. В разделе **Площадки** новое приложение будет отмечено значком ⚠. Подтвердить или отклонить добавление приложения может только пользователь с привилегией «Добавление и удаление приложений». Подтверждение добавления приложений, установленных неавторизованными пользователями, по умолчанию выключено.

Подробности см. в разделе «Управление приложениями» Руководства администратора PT MC.

1.2. AI-поиск по активам и уязвимостям

Добавлена бета-версия AI-поиска по системным PDQL-запросам с помощью фраз на русском и английском языках. Доступны PDQL-запросы для поиска активов и уязвимостей, а также для проверки соответствия стандартам. Чтобы включить эту возможность, нужно изменить конфигурацию роли Core.

Подробности см. в разделе «Фильтрация активов с помощью AI-поиска по запросам» Руководства оператора.

1.3. Дифференциальный отчет за 7 дней

Добавлена возможность создания дифференциального отчета по уязвимостям повышенного уровня опасности (то есть критического или высокого). Отчет помогает отследить изменения, происходившие с уязвимостями за последние 7 дней, например: какие новые уязвимости были обнаружены, какие были устранены, а какие — сохранены без изменений. Данные выгружаются в формате XLSX.

1.4. Визуализация метрик PostgreSQL

Теперь вы можете отслеживать метрики СУБД PostgreSQL на новом дашборде. Дашборд доступен в веб-интерфейсе Grafana и содержит готовый набор виджетов, отражающих основные показатели работы PostgreSQL.

1.5. Визуализация метрик состояния серверов

Добавлен дашборд для мониторинга состояния серверов. Дашборд доступен в веб-интерфейсе Grafana и содержит готовый набор виджетов, отражающих основные метрики серверов, на которых установлен MaxPatrol VM.

2. Технические особенности

Информация, представленная в этом разделе, поможет избежать возможных ошибок при обновлении и последующей работе с продуктом.

Существует ряд особенностей версии 2.7:

— Версия 2.7 поддерживает обновление с версий 2.0, 2.1, 2.5, 2.6.

— Версия 2.7 поддерживает интеграцию с PT NAD версий 10.1, 10.2, 10.3, 11.0, 12.0, 12.1.

— Начиная с версии 2.7 компоненты MaxPatrol VM можно установить на Debian 10.3 и выше, Debian 11 и 12 (на базе ядра Linux версии 5.10 и выше).

— Если требуется обновить MaxPatrol VM вместе с обновлением ОС, сначала нужно выполнить подготовку к обновлению MaxPatrol VM, затем обновить ОС и после этого — обновить компоненты MaxPatrol VM.

— Начиная с версии 2.7 компоненты MaxPatrol VM могут быть развернуты в системе виртуализации zVirt версии 4.2.

— Прежде чем приступать к обновлению MaxPatrol VM, рекомендуется остановить все задачи на сбор данных, а также убедиться, что на период обновления не запланирован запуск задач по расписанию. Это позволит избежать накопления очередей во время обновления, а также ошибок при выполнении задач после обновления.

3. Улучшения

В этом разделе описаны улучшения MaxPatrol VM новой версии.

Проверка пользовательских сертификатов на соответствие требованиям

Теперь во время установки пользовательские корневые сертификаты автоматически проверяются на соответствие требованиям безопасности. Выявленные несоответствия отображаются в терминале.

Настройка прокси-сервера для онлайн-активации

Теперь вы можете указать данные прокси-сервера в параметрах конфигурации роли Management and Configuration. Таким образом можно выполнить онлайн-активацию, когда сервер PT MC подключен через веб-прокси.

Стандартизация копирования данных из таблиц

Усовершенствован процесс копирования табличных данных из PT MC (например, из таблиц **Пользователи** и **LDAP-подключения**). Стало доступно копирование из любых таблиц PT MC. Статусы копирования теперь имеют текстовые пояснения. При успешном копировании отображается значок ✓.

Активные ссылки при экспорте отчетов

Теперь при выгрузке данных в XLSX-формате ссылки в отчетах остаются активными.

Отображение очереди выпуска отчетов

Теперь вы можете просматривать очередь выпускаемых отчетов и отменять их выпуск по кнопке **Очередь** на странице **Система** → **Отчеты**.

Повышение скорости обработки PDQL-запросов

Для высоконагруженных систем добавлена возможность повысить скорость обработки PDQL-запросов в несколько десятков раз. При этом размер базы данных сервиса TRM увеличивается на 10—30%. Чтобы включить эту возможность, нужно изменить конфигурацию роли Core.

Подробности см. в разделе «Оптимизация выполнения PDQL-запросов для высоконагруженных систем» Руководства администратора.

positive
technologies

Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют около 3000 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.