MaxPatrol VM версия 2.8

Обзор новых возможностей

Дата редакции документа: 10.06.2025

Содержание

1. Новые возможности

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

1.1. Лицензионный контроль количества активов

Теперь при превышении лимита количества активов, установленного для вашей лицензии, MaxPatrol VM отображает предупреждение.

1.2. Стандартная роль с правами только на просмотр данных

Для обеспечения информационной безопасности администраторам MaxPatrol VM важно иметь возможность гибко настраивать права доступа в зависимости от полномочий и обязанностей сотрудников организации.

Теперь в приложении MaxPatrol 10 доступна новая стандартная роль **Наблюдатель** с правами только на просмотр данных.

Подробное описание стандартных ролей для приложений MaxPatrol VM вы можете найти в разделе «Предоставление прав доступа» Руководства администратора.

1.3. Совместимость с FreeIPA

Добавлена совместимость со службами каталогов FreeIPA и ALD Pro. Вы можете подключиться к этим службам по LDAP-протоколу, чтобы выполнять синхронизацию и аутентификацию пользователей и настраивать соответствие ролей MaxPatrol VM и групп пользователей FreeIPA и ALD Pro.

1.4. Персональные токены доступа

Теперь в PT MC вы можете создавать бессрочные персональные токены доступа для выполнения запросов к API, требующих авторизации. Использование токена сделает авторизацию более удобной. Подробное описание токенов и работы с ними в PT MC приведено в разделе «Управление токенами доступа» Руководства администратора PT MC.

1.5. Новая роль «Оператор» в приложении Management and Configuration

Для более гибкого доступа к функциям Management and Configuration в приложение добавлена новая стандартная роль **Оператор**, которая позволяет просматривать всю информацию в приложении.

1.6. Настройка парольной политики и блокировки пользователей

Теперь в веб-интерфейсе PT MC в разделе **Параметры приложений** вы можете задать параметры парольной политики, такие как сложность пароля и срок его действия, а также параметры блокировки пользователей, включая количество попыток ввода пароля и время неактивности пользователя до блокировки.

Подробное описание настройки приведено в разделе «Настройка парольной политики, автоматической блокировки и продолжительности сессии пользователя» Руководства администратора PT MC.

Кроме того, в PT MC в карточке заблокированного пользователя теперь отображается причина его блокировки.

2. Экспертиза: поддержка систем

В этом разделе перечислены системы, поддержка которых реализована в новой версии MaxPatrol VM, системы, для которых реализован поиск новых уязвимостей, а также новые системные стандарты.

Обнаружение уязвимостей

В новой версии MaxPatrol VM реализовано обнаружение уязвимостей в следующих системах:

- Apache Cassandra;
- Atlassian Bamboo;
- Atlassian Bitbucket;
- HashiCorp Consul;
- IBM AIX;
- Jenkins;
- Kubernetes;
- macOS;
- OpenNebula;
- pgAdmin;
- PowerDNS Recursor;
- PowerDNS Authoritative Server;
- Teleport;
- VMware Workstation;
- zVirt;
- ОС «ОСнова».

Обнаружение систем

MaxPatrol VM при сканировании в режиме Audit теперь может обнаруживать следующие системы:

- HashiCorp Vault;
- Secret Net Studio;
- Veritas InfoScale;
- Zabbix Agent 2;
- ОС «ОСнова».

Сбор данных о конфигурации активов

Реализован сбор данных о конфигурации следующих систем:

- Apache HTTP Server;
- Elasticsearch;
- Eltex ESR;
- Eltex MES (под управлением ISS);
- Eltex MES 5448;
- Juniper Networks Junos OS;
- Kaspersky Security Center;
- Microsoft Internet Information Services (IIS);
- Microsoft Office;
- Microsoft SharePoint;
- nginx;
- Proxmox VE.

3. Технические особенности

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

Существует ряд особенностей версии 2.8:

— Версия 2.8 поддерживает обновление с версий 2.0, 2.1, 2.5, 2.6, 2.7.

— Версия 2.8 поддерживает интеграцию с PT NAD версий 12.0, 12.1, 12.2.

— 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.

4. Улучшения

В этом разделе описаны улучшения MaxPatrol VM новой версии.

Подробное журналирование действий

Теперь журнал действий показывает не только сам факт изменений в системе, но и что было изменено. В списке действий отображаются смена паролей и ролей пользователей, а также изменение набора привилегий, входящих в состав роли.

Увеличение допустимого объема PDF-отчетов

Увеличен допустимый объем для отчетов, выпускаемых в формате PDF. Теперь можно создавать отчеты объемом до 5000 страниц.

Повышение скорости выгрузки данных для XLSX-отчетов

Оптимизирован механизм выпуска отчета по шаблонам в формате XLSX. Теперь отчеты формируются на 30% быстрее.

Деактивация PT MC в веб-интерфейсе

Если ключ инсталляции уже использовался для активации PT MC на другом устройстве, при восстановлении данных из резервной копии вам потребуется деактивировать PT MC. Теперь вы можете это сделать в веб-интерфейсе PT MC на странице **Лицензии**.

Подробнее см. в разделе «Деактивация PT MC» Руководства администратора.

Активные ссылки в журнале действий пользователя

Записи в журнале действий пользователя теперь могут содержать активные ссылки на страницу с расширенной информацией о выбранном действии (например, на отчет). Ссылки стали доступны в панели **Подробности**. Расширенная информация о выбранном действии пользователя открывается в новой вкладке.

FQDN в качестве цели сбора данных для модуля HostDiscovery

Улучшена работа модуля HostDiscovery: теперь можно собирать полные доменные имена (FQDN) из целей сканирования. Это снижает вероятность дублирования активов при их сканировании в разных режимах.

Ротация результатов сканирования, импорта и ручного ввода активов

Для освобождения дискового пространства в MaxPatrol VM реализован механизм ротации. Результаты сканирования, импорта и ручного ввода активов автоматически удаляются по достижении указанного срока хранения. Ротация позволяет актуализировать состояние активов на основе данных, полученных из событий.

Подробности см. в разделе «Ротация результатов сканирования, импорта и ручного ввода активов».

Новые возможности утилиты deployer

Расширены возможности утилиты deployer, поставляемой с ролью Deployer. Теперь с помощью утилиты вы можете:

— установить значение любого из параметров экземпляра роли;

— сбросить значение параметров экземпляра роли до значений по умолчанию;

— получить список всех доступных параметров экземпляра роли с описанием и типами;

— удалять неиспользуемые пакеты ролей компонентов MaxPatrol VM.

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.