КОД БЕЗОПАСНОСТИ

Что нового в vGate R2 4.2

Обзор основных изменений обновленной версии продукта

Октябрь 2019

vGate

Сертифицированное средство защиты среды виртуализации

Решение для контроля действий администратора и защиты от специфических угроз виртуализации. В обзоре представлены возможности vGate версии 4.2 (далее – vGate 4.2) по сравнению с версией 4.1.

Поддержка платформы виртуализации VMware vSphere 6.7

Новая версия vGate поддерживает VMware vSphere версии 6.7. Это дает возможность применять продукт в самых современных виртуальных инфраструктурах. В поддержку включены сложные конфигурации с Platform Services Controller, который выделен в отдельный сервер и способствует распределению нагрузки. Это обеспечивает удобство работы vGate 4.2 в крупномасштабных инфраструктурах со сложной архитектурой. Поддержка vSphere 6.7 охватывает все последние вышедшие на момент релиза апдейты платформы.

Расширенный список политик безопасности

В vGate 4.2 добавлен новый набор политик безопасности – VMware vSphere 6.7 Security Configuration Guide.

Обновленный межсетевой экран

В модуле vNetwork выполнены доработки для vSphere, теперь появилась возможность автоматизированного добавления виртуальных машин (далее – ВМ) в сегменты виртуальной инфраструктуры по имени, что упрощает процесс применения правил фильтрации на новые ВМ в больших динамично изменяющихся инфраструктурах.

Обновленный мониторинг виртуальной инфраструктуры

Модуль vMonitor пополнился важной функцией мониторинга виртуальной инфраструктуры. Теперь стало возможным контролировать аутентификацию пользователей в vSphere в обход vGate.

Обновленный мастер установки агентов защиты

В новой версии продукта возможные настройки показываются адаптивно, в зависимости от компонентов инфраструктуры. При этом происходит валидация введенных данных, проверка настроек, а также другие операции, направленные на минимизацию ошибок при внедрении vGate.

Разграничение прав доступа администраторов к серверам управления vCenter

В vGate 4.2 vCenter стал объектом мандатного доступа. Теперь есть возможность администраторам виртуализации предоставить доступ только определенным серверам управления инфраструктурой.

Поддержка групп Active Directory

В продукте реализована работа с группами пользователей Microsoft Active Directory, назначение на них меток и правил доступа. Это расширяет возможности автоматизации процессов для администраторов безопасности. В отличие от предыдущей версии, в vGate 4.2 можно назначить метки и правила доступа группам пользователей AD – соответственно, все пользователи группы унаследуют права доступа и привилегии из нее автоматически.

Агент аутентификации для ОС Альт 8 СП

Впервые в истории развития продукта добавлен агент аутентификации для Linux. Первой поддерживаемой операционной системой стала Альт 8 СП.

Контроль операций Cross vCenter Clone

По аналогии с операцией Cross vCenter vMotion теперь контролируются и операции клонирования виртуальной машины между серверами управления. Таким образом можно, к примеру, разрешить клонирование виртуальной машины в рамках одного контура управления, но запретить в случае необходимости переезда на другой сервер vCenter.

Новый механизм взаимодействия агентов на ESXi с сервером vGate

Производительность работы агента ESXi увеличена по сравнению с предыдущими версиями. Это поможет при совершении в виртуальной инфраструктуре массовых действий, таких как старт/стоп большого пула виртуальных машин, перезапуск хостов после обновления и прочих действий, оказывающих влияние на скорость работы.

Поддержка Скала-Р версии 1.20

Список поддерживаемых платформ виртуализации vGate расширен. Теперь vGate можно использовать вместе с российской гиперконвергентной ИТ-инфраструктурой Скала-Р – универсальное решение для построения масштабируемых виртуализованных центров обработки данных.

Расширенные возможности веб-интерфейса

В веб-интерфейс управления добавлены настройки отправки событий и инцидентов по syslog и e-mail.

Расширенный список поддерживаемых идентификаторов

Начиная с версии 4.2 в vGate реализована поддержка электронного идентификатора JaCarta-2.

Импорт и экспорт конфигурации

Все новые функциональные возможности добавлены в импорт/экспорт конфигурации.

Функциональные различия редакций:

Функциональные возможности	Standard	Enterprise	Enterprise Plus
Количество серверов авторизации vGate	1	Неограниченно	Неограниченно
Разграничение доступа (vAccess):			
Выделенные роли администраторов	●	●	●
Мандатное и дискреционное разграничение доступа	●	●	●
Разбиение виртуальной инфраструктуры на сегменты	●	●	●
Управление перемещением виртуальных машин и обрабатываемых на них данных	●	●	●
Контроль целостности и доверенная загрузка ВМ	●	●	●
Регистрация событий безопасности (аудит)	●	●	●
Автоматизация меток и политик, группировка объектов	●	●	●
vCompliance:			
Шаблон безопасности КИИ	●	●	●
Шаблон ГОСТ Р 57580.1-2017	●	●	●
Шаблон ГОСТ Р 56938-2016	●	●	●
Шаблон безопасности CIS Benchmarks	●	●	●
Шаблон безопасности VMware vSphere 6.7 Security Configuration Guide[new]	●	●	●
Шаблон безопасности ГИС	●	●	●

Шаблон безопасности ИСПДн	●	●	●
Шаблон безопасности РД АС	●	●	●
Шаблон безопасности СТО БР ИББС	●	●	●
Шаблон безопасности PCI DSS	●	●	●
vNetwork			
Межсетевое экранирование на уровне гипервизора	–	–	●
vMonitor			
Корреляция событий безопасности виртуализации	–	–	●
vReport			
Создание отчетов безопасности	–	–	●
Отказоустойчивость:			
Создание резервной копии конфигурации vGate (BackUp сервера авторизации)	●	●	●
Архивирование журналов аудита	●	●	●
Горячее резервирование серверов vGate (кластер)	–	●	●
Подключение агента авторизации к нескольким серверам авторизации vGate	–	●	●
Создание фермы серверов авторизации (синхронизация настроек между серверами vGate)	–	●	●
Совместимость с компонентами виртуализации:			
Совместимость с VMware vCenter SRM	●	●	●
Совместимость с VMware View (Horizon)	●	●	●
Совместимость с VMware vCloud Director	●	●	●
Поддержка серверов управления vCenter Linked Mode	–	●	●
Поддержка VMware Auto-Deploy	–	●	●
Поддержка vCenter High Availability	–	●	●
Контроль управления серверами Hyper-V через System Center Virtual Machine Manager	–	●	●

Почтовый адрес: 115127, Россия, Москва, а/я 66.
Адрес офиса в Москве:
1-й Нагатинский проезд, д. 10, стр.1.
Тел.: +7 (495) 982 30 20 (многоканальный).
Факс: +7 (495) 744 29 31.

Адрес офиса в Санкт-Петербурге:
Пискаревский пр-т, д. 2, корп. 3, лит. А, БЦ «Бенуа».
Тел.: +7 (812) 313 80 28.
E-mail: info@securitycode.ru

Запрос дополнительной информации о продуктах: info@securitycode.ru
По вопросам стоимости и покупки продуктов: buy@securitycode.ru
По вопросам партнерства и сотрудничества: info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте www.securitycode.ru
Также с помощью онлайн-калькулятора можно рассчитать стоимость решения.

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность инфор¬мационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.