Средство защиты информации vGate
Комментарии к версии 4.4

Данный документ содержит описание новых возможностей СЗИ vGate версии 4.4, особенностей работы и ограничений применения изделия, которые необходимо учитывать при эксплуатации ПО vGate.

Оглавление

1. Изменения и новые возможности

Ниже приводятся сведения о новых возможностях ПО vGate версии 4.4.

1.1. Версия 4.4

1. Обеспечена поддержка VMware vSphere 7.0.

2. Реализована поддержка новых политик набора "CIS for ESXi 6.7".

3. Реализован контроль операций vSAN, добавлена роль пользователя "Администратор vSAN".

4. Реализован контроль целостности файлов конфигурации ESXi-сервера.

5. В веб-интерфейсе добавлены виджеты, позволяющие построить следующие NetFlow-диаграммы:

- Разрешенный трафик между сегментами виртуальной инфраструктуры.
- Заблокированный трафик между сегментами виртуальной инфраструктуры.

6. В веб-интерфейсе реализовано отображение информации о сетевом трафике, переданном или заблокированном в соответствии с правилами фильтрации (активные сессии компонента "Сегментирование").

7. В веб-интерфейсе реализовано отображение соответствия защищаемых ESXi-серверов политикам безопасности.

8. Реализована совместимость агента аутентификации с ПО Континент и VipNet.

9. Обеспечена работа правил фильтрации компонента "Сегментирование", независящая от перемещения виртуальных машин в защищаемой инфраструктуре.

10. Выполнен перенос функций управления инфраструктурой из консоли управления vGate в веб-консоль.

11. Реализован механизм проверки только тех политик, которые назначены на ESXi-сервер.

12. Выполнен перенос функции обработки правил фильтрации сетевого трафика с сервера авторизации vGate на компоненты защиты серверов виртуализации.

13. Для правил разграничения доступа в консоли управления vGate добавлен столбец "Контроль трафика", отображающий состояние данного параметра.

14. Реализовано автоматическое удаление правил разграничения доступа пользователя при удалении его учетной записи.

15. Реализовано отображение имени виртуальной машины в событиях аудита vGate.

2. Требования к аппаратному и программному обеспечению

К компьютерам, на которые устанавливаются компоненты vGate 4.4, предъявляются следующие системные требования.

Компонент	Операционная система
Сервер авторизации	• Windows Server 2012 R2 x64 + Update KB2999226. • Windows Server 2016 x64. • Windows Server 2019 x64. Минимальная необходимая пропускная способность канала для сети резервирования — 10 Мбит/с. Для компонента "Сервер авторизации" требуется 10 ГБ на жестком диске. Дополнительно (при использовании персонального идентификатора): • Драйверы JaCarta. • Драйверы для Рутокен S, Lite и ЭЦП
Резервный сервер авторизации	• Windows Server 2012 R2 x64 + Update KB2999226. • Windows Server 2016 x64. • Windows Server 2019 x64. Для компонента "Сервер авторизации" требуется 10 ГБ на жестком диске. Минимальная необходимая пропускная способность канала для сети резервирования — 10 Мбит/с
Агент аутентификации	• Microsoft Windows 8.1 x86/x64. • Microsoft Windows 10 Enterprise. • Microsoft Windows Server 2012 R2 x64 + Update KB2999226. • Microsoft Windows Server 2016 x64. • Microsoft Windows Server 2019 x64. • Linux Альт 8 СП, ядро версии 4.4.211. Для компонента "Агент аутентификации" требуется 200 МБ на жестком диске. Дополнительно (при использовании персонального идентификатора): • Драйверы JaCarta • Драйверы для Рутокен S, Lite и ЭЦП
Консоль управления	• Microsoft Windows 8.1 x86/x64. • Microsoft Windows 10 Enterprise. • Microsoft Windows Server 2012 R2 x64 + Update KB2999226. • Microsoft Windows Server 2016 x64. • Microsoft Windows Server 2019 x64
Средство просмотра отчетов	• Microsoft Windows 8.1 x86/x64. • Microsoft Windows 10 Enterprise. • Microsoft Windows Server 2012 R2 x64 + Update KB2999226. • Microsoft Windows Server 2016 x64. • Microsoft Windows Server 2019 x64
Модули защиты ESXi	• VMware vSphere 6.5 (VMware ESXi Server 6.5). • VMware vSphere 6.7 (VMware ESXi Server 6.7). • VMware vSphere 7.0 (VMware ESXi Server 7.0). Не гарантируется работа ПО vGate с бесплатными редакциями ESXi, а также на кастомных образах vSphere (от производителей серверов HP, IBM и др.)
Компонент защиты vCenter (vCSA)	• Windows Server 2012 R2 + Update KB2999226. • Windows Server 2016 x64. • Photon OS. • VMware vSphere 6.5 (VMware vCenter Server 6.5). • VMware vSphere 6.7 (VMware vCenter Server 6.7). • VMware vCenter Server Appliance 6.5. • VMware vCenter Server Appliance 6.7. • VMware vCenter Server Appliance 7.0. Для компонента защиты vCenter требуется 200 МБ на жестком диске. Работа ПО vGate на кастомных образах vSphere (от производителей серверов HP, IBM и др.) не гарантируется

Компонент	Операционная система
Компонент защиты PSC	• Platform Services Controller 6.7. • Platform Services Controller Appliance 6.7
Сервер мониторинга	VMware ESXi Server, удовлетворяющий минимальным требованиям: • процессор — 2 ядра; • память — 4 ГБ; • хранилище — 20 ГБ

Требования к аппаратному обеспечению.

- На компьютере, предназначенном для сервера авторизации, должно быть не менее одного Ethernet-интерфейса при использовании конфигурации сети с отдельным маршрутизатором и не менее двух Ethernet-интерфейсов, если маршрутизацию трафика выполняет сервер авторизации.
- Не рекомендуется использование протокола DHCP для Ethernet-интерфейсов, подключенных к защищаемому периметру и периметру сети администрирования.

3. Особенности установки

Ниже приведен список проблем, с которыми вы можете столкнуться при установке vGate. Пожалуйста, внимательно ознакомьтесь с этим списком прежде чем устанавливать компоненты vGate.

1. Не поддерживается установка сервера авторизации на компьютер, имя которого содержит символы кириллицы.

2. Не поддерживается установка агента аутентификации в папку, в пути к которой присутствуют символы кириллицы.

3. Не поддерживается установка сервера авторизации vGate и компонента защиты vCenter на контроллер домена.

4. Работа агента аутентификации vGate не поддерживается на компьютерах, в имени которых содержатся символы кириллицы.

5. Не поддерживается протокол IPv6. Для работы vGate необходимо отключить протокол IPv6 в свойствах сетевого адаптера.

6. При установке сервера авторизации vGate в имени администратора безопасности поддерживаются следующие символы: [A-Za-z0-9-_].

7. В случае если PostgreSQL уже установлен на компьютере и в его пароле присутствуют символы кириллицы, следует изменить пароль перед началом установки vGate. В противном случае установка ПО vGate завершится ошибкой.

8. Нельзя выполнить установку vGate, если открыто диалоговое окно со свойствами сетевого адаптера.

9. Если на компьютере установлено СЗИ Secret Net версии 6.0 и выше, включен режим контроля потоков и выбран уровень сессии "строго конфиденциально", то невозможно выполнить установку и удаление сервера авторизации и агента аутентификации vGate.

10. Если на компьютере установлено СЗИ Secret Net версии 6.0 и выше, включен режим контроля целостности с блокировкой ПК при нарушении контроля целостности, то невозможно выполнить установку сервера авторизации и агента аутентификации vGate.

11. Установка PostgreSQL в автоматическом режиме не поддерживается, если на компьютере не установлен Microsoft Visual C++ 2005 Redistributable Package.

12. Если производится переустановка ПО vGate вместе с базой PostgreSQL, то после удаления PostgreSQL необходимо вручную удалить каталог установки (%ProgramFiles%\PostgreSQL\9.4).

13. Если на сервере авторизации с помощью кнопки "Изменить" в меню удаления программы был изменен список защищаемых сетей, то после завершения установки нужно выполнить команду %ProgramFiles%\vGate\drvmgr.exe e.

14. Установку компонента защиты vCenter с помощью программы установки непосредственно на сервере vCenter необходимо производить из-под учетной записи локального администратора, иначе возникает ошибка "Error: Операция успешно завершена".

15. Если на компьютере установлены консоль управления или средство просмотра отчетов из пакета установки vGate Client, то при обновлении на новую версию ПО vGate необходимо снова выбрать установку этих компонентов, иначе они будут удалены.

16. В режиме интеграции vGate с Active Directory для корректной работы учетных записей Active Directory необходимо наличие контроллера домена во внешнем периметре сети администрирования инфраструктуры.

17. Если на ESXi-сервере есть работающие ВМ с включенной политикой "Очистка памяти", то для установки, обновления или удаления агента vGate на ESXi-сервере необходимо остановить все ВМ, запущенные после назначения этой политики.

18. При использовании контроллера домена для хранения учетных записей vGate необходимо выбирать контейнер, имя и полный путь к которому не содержат символов кириллицы.

19. Если в один домен входит более одного сервера авторизации и их сервисные учетные записи хранятся в разных контейнерах Active Directory, то перед обновлением сервера авторизации необходимо удалить относящиеся к нему объекты из Active Directory.

20. Если в режиме изменения параметров установки vGate программа установки не находит установочный файл сервера авторизации, необходимо указать путь к файлу установки вручную.

21. Установка компонента защиты vGate на vCenter Server Appliance возможна только из-под локальной учетной записи пользователя root.

22. Установка сервера авторизации vGate на компьютер может завершиться с ошибкой, если перед установкой этот компьютер был отключен от сети.

23. Возможно возникновение проблем при установке агента аутентификации vGate на компьютер с установленными виртуальными адаптерами.

24. Не корректно обновление компонентов защиты ESXi на новую версию ПО vGate, которая не поддерживается версией ПО сервера авторизации.

25. Для корректной установки ПО vGate на компьютеры с ОС Windows необходимо на время установки отключить самозащиту в Kaspersky Endpoint Security (начиная с версии 10.3).

26. Если ESXi-сервер, добавленный в список защищаемых vGate серверов по DNS-имени, удалить из инвентаризации vCenter (Remove from Inventory), а затем добавить в инвентаризацию по IP-адресу, то при развертывании компонента защиты vGate на этом сервере возможно появление ошибок.

27. Не поддерживается установка сервера авторизации vGate и сервера безопасности Secret Net Studio на один компьютер.

28. При установке сервера авторизации vGate возможно появление ошибки "Произошла ошибка при создании учетной записи службы авторизации vGate" из-за некорректной подстановки имени OU (Organizational unit).

29. При агрегации сетевых интерфейсов нельзя назначать одинаковые IP-адреса на отдельный интерфейс и на группу интерфейсов. В противном случае установка ПО vGate завершится ошибкой.

30. Установка компонентов vGate на ОС Windows может завершиться с ошибкой установки сетевого драйвера. В этом случае рекомендуется установить актуальные обновления для ОС Windows.

31. При установке резервного сервера авторизации учетные данные сервера виртуализации с основного сервера не копируются на резервный сервер. При изменении роли резервного сервера авторизации на роль основного сервера, учетные данные сервера виртуализации на новом основном сервере не сохраняются.

32. При установке компонентов vGate на серверах vCSA или PSC 6.7 с маленькой мощностью возможно появление ошибки, связанной с истечением таймаута (по умолчанию 5 минут). В этом случае нужно увеличить значение параметра "VcpOnvCenterTimeout" в реестре ОС Windows (например, до 10 минут).

33. После обновления ПО сервера авторизации vGate возможно появление ошибок вида "ERROR: [GRPC MESSAGE] Handshake failed with fatal error SSL_ERROR_SSL: error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number". После переустановки компонентов защиты ESXi-серверов ошибки продолжают появляться до перезапуска службы rhuid.

34. При переустановке ПО сервера авторизации vGate на ПО новой версии необходимо предварительно удалить компоненты защиты vGate с ESXi-серверов. В противном случае может произойти остановка службы rhuid на сервере авторизации.

35. Установка компонента защиты на ESXi-сервер завершается ошибкой, если ESXi-сервер (без vCenter) добавлен в список защищаемых объектов на сервере авторизации vGate по доменному имени.

36. Если пароль пользователя root в Photon OS состоит из 16 или более символов, установка компонента защиты на сервер vCSA завершится ошибкой.

4. Известные проблемы

Ниже приведен список проблем, известных на момент выхода vGate 4.4.

4.1. Общесистемные

1. Для корректной работы компонентов сервера авторизации vGate требуется наличие свободного TCP-порта 80.

2. Переименование сервера авторизации не поддерживается в vGate.

3. Не поддерживается использование символов кириллицы в имени домена vGate.

4. В именах учетных записей пользователей не поддерживаются следующие спецсимволы: \+()?[*@&.

5. При использовании способа аутентификации "Данные текущей сессии Windows" не поддерживается аутентификация учетных записей Windows, в имени которых содержатся символы кириллицы.

6. Не поддерживается вход в систему с использованием учетной записи пользователя домена Windows в случае, если "Имя входа пользователя" отличается от "Имени входа пользователя (пред-Windows 2000).

7. Для утилиты iSCSILocker не поддерживаются диски без серийного номера.

8. Если на vCenter активирована поддержка IPv6, то можно получить доступ посредством vSphere Client, минуя средство защиты vCenter. Модули защиты ESXi-сервера также не блокируют доступ внутри периметра по IPv6.

9. Не поддерживается полномочное управление доступом в случае использования Raw Device Mapping.

10. Для работы привилегии "Разрешено скачивать файлы виртуальных машин" необходимо, чтобы для данного пользователя было явно настроено соответствующие правило доступа.

11. Если после установки на ESXi-сервер компонента защиты vGate был изменен SNMP-порт, необходимо вручную открыть новый порт как исходящий в настройках межсетевого экрана ESXi-сервера.

12. При использовании трансляции сетевых адресов (NAT) через сетевой шлюз возможно соединение только одного агента аутентификации с сервером авторизации и защищаемыми серверами.

13. Не поддерживается работа vGate с Secure Boot для VMware ESXi Server.

14. При управлении двумя серверами авторизации vGate с помощью одного агента аутентификации, если хотя бы один сервер авторизации будет переведен в аварийный режим, сетевой трафик перестанет подписываться.

15. Время действия сессии пользователя в агенте аутентификации vGate не ограничено.

16. Для контроллера домена в защищаемом периметре vGate требуется создать правило, разрешающее входящие соединения ко всем TCP-портам.

17. В консоли управления возможно зависание процесса установки компонентов защиты vGate на компьютерах с ОС Windows.

18. При удалении компонента защиты vCenter с помощью меню "Программы и компоненты" в ОС Windows не выполняется удаление агента vGate с отдельностоящего PSC (Platform Services Controller). В этом случае нужно удалить агент на сервере PSC вручную.

1.2. Контроль целостности

1. После VMmotion может потребоваться повторный пересчет контрольных сумм.

2. После изменения русскоязычных параметров ВМ через vSphere Client для них не поддерживается расчет контрольной суммы.

3. Если сразу после нарушения целостности контролируемых файлов гостевой ОС, находящихся на диске с включенной опцией кеширования, будет выполнена приостановка ВМ, то последующий запуск остановленной ВМ может быть разрешен.

4. Не поддерживается контроль целостности файлов конфигурации ВМ, если на ВМ включена функция Fault Tolerance.

5. Если сначала назначить политику "Доверенная загрузка виртуальных машин" на ВМ под управлением ESXi-сервера, а затем установить на этот сервер модуль защиты ESXi от vGate, то возникнет ошибка проверки целостности виртуальной машины.

6. Если ВМ с установленным сервером авторизации vGate расположена на ESXi-сервере, входящем в кластер VMware, то при миграции данной ВМ на другой ESXi-сервер для нее перестает осуществляться контроль целостности, поскольку файл с контрольными суммами пишется только на текущий ESXi-сервер.

7. Если сервер авторизации установлен на виртуальной машине, для которой назначена политика "Доверенная загрузка виртуальных машин", то при нарушении целостности в консоли управления vGate для данной виртуальной машины указывается статус "Согласована".

8. По умолчанию в настройках политики "Доверенная загрузка виртуальных машин" отмечен пункт "Целостность BIOS ВМ". В этом случае возможно изменение статуса ВМ с "Целостность ВМ согласована" на "Целостность ВМ нарушена" при каждом запуске ВМ (из-за нарушения целостности файла *.nvram). Чтобы этого не происходило, нужно удалить отметку с пункта "Целостность BIOS ВМ".

1.3. Резервирование сервера авторизации

1. При входе в систему с помощью агента аутентификации сразу после передачи управления резервному серверу авторизации могут появляться сообщения об ошибках.

2. Если для аутентификации компьютера используется встроенная учетная запись компьютера в домене Windows, то ему может быть отказано в аутентификации при переключении на резервный сервер авторизации. В этом случае рекомендуется выполнить перезагрузку данного компьютера.

3. Если основной сервер авторизации недоступен, то получить доступ к резервному серверу авторизации из внешнего периметра сети администрирования невозможно. Для входа на резервный сервер авторизации необходимо использовать локальный доступ.

4. При выходе из строя основного сервера авторизации для назначения резервного сервера основным консоль управления на резервном сервере следует запускать с помощью команды "Запуск от имени администратора" ("Run as administrator").

5. С помощью одной учетной записи пользователя можно одновременно выполнить два подключения к серверу авторизации, используя основной IP-адрес и IP-адрес для резервирования. После этого возможны ошибки при аутентификации пользователей и подписи сетевого трафика клиента.

6. После переключения управления на другой сервер авторизации службой горячего резервирования, в консоли управления vGate на отключенном сервере авторизации появляется предложение доконфигурировать сервер. Данная операция может закончиться ошибкой. Для восстановления работоспособности сервера авторизации необходимо выполнить действия, описанные в документации.

7. На резервном сервере авторизации не отображается статус (версия) установленного агента vGate на сервере vCenter.

8. При резервировании сервера авторизации не реплицируется параметр AddVMTimeout (таймаут автодобавления ВМ).

1.4. Политики безопасности

1. Не поддерживается миграция запущенной ВМ с назначенной политикой "Доверенная загрузка виртуальных машин" между виртуальными хранилищами данных (datastores) ESXi-сервера.

2. При включенной политике "Доверенная загрузка виртуальных машин" применение других политик, результатом которых будет изменение конфигурационного файла, требует пересчета контрольных сумм ВМ.

3. Политика "Запрет смешивания разных типов сетевого трафика" не поддерживается для Distributed Switch.

4. Политика "Затирание остаточных данных на СХД при удалении ВМ" не поддерживается для ВМ, имеющих снимки (snapshots).

5. Политика "Затирание остаточных данных на СХД при удалении ВМ" не работает для шаблонов виртуальных машин.

6. Политика "Затирание остаточных данных на СХД при удалении ВМ" не работает автоматически для связанных клонов (при использовании технологии Linked Clones).

7. Удаление клонов виртуальных машин VMware View в vSphere Client, подключенном напрямую к ESXi-серверу в обход vCenter, может приводить к затиранию дисков базовой реплики, если на эти клоны назначена политика "Затирание остаточных данных на СХД при удалении ВМ".

8. Необходимо остановить ВМ перед назначением на нее политики "Запрет логирования ВМ".

9. На сервере ESXi 6.5 для работы политики "Запрет подключения USB" загружается устаревшая версия драйвера USB. После отмены назначения политики драйвер новой версии (vmkusb) не загружается.

10. При просмотре через vCenter или ESXi Host Client параметры, измененные в результате применения политик "Включить фильтр BPDU", "Задать ограничение допустимого времени простоя сессий ESXi и SSH", "Ограничение допустимого времени простоя сессии DCUI", "Задать ограничение допустимого времени работы служб ESXI Shell и SSH" и "Синхронизация времени", принимают нужные значения только после перезапуска hostd.

11. Если для ВМ назначена политика "Доверенная загрузка ВМ" и разрешен запуск ВМ при нарушении целостности конфигурации, то в случае изменения контролируемых параметров vmx-файла отклонение изменений возможно только если ВМ выключена. В противном случае отклонение изменений не произойдет, несмотря на появление сообщения об успешной отмене изменений.

12. Если на ESXi-сервере протокол IPv6 был отключен в результате работы политики "Отключить протокол IPv6", то после отмены назначения данной политики и перезагрузки сервера протокол IPv6 будет по-прежнему отключен.

13. На ВМ с установленной ОС периодически нарушается целостность файла конфигурации BIOS *.nvram (политика "Доверенная загрузка ВМ").

14. При автоматической проверке политики "Синхронизация времени" возможно появление ошибки "При проверке статуса политики "Синхронизация времени" произошла ошибка "service is not installed" (ntpd)".

15. Если в шаблоне политик есть политики "Включить Lockdown mode" и "Отключение DCUI", то при назначении этого шаблона на объект будет применена только политика "Включить Lockdown mode".

16. При назначении политики "Контроль целостности файлов конфигураций ESXi" на ESXi-сервер версии 7.0 U1 необходимо снять отметку с файлов /bin/vmkiscsi-tool, /etc/init.d/ddecomd и /usr/libexec/jumpstart/plugins/libconfigure-locker.so, иначе применение политики завершится ошибкой подсчета.

1.5. Аудит

1. Для протокола SMB в событиях аудита присутствуют учетные записи, относящиеся к компьютеру, а не к пользователю.

2. После изменения сетевой конфигурации ESXi-сервера (добавление/удаление сетевых адаптеров) могут не регистрироваться события, связанные с производимыми в разделе конфигурации Networking действиями. В этом случае рекомендуется перезагрузить сервер авторизации.

3. В журнале событий не отображаются события анонимного доступа к серверу авторизации по сети внешнего периметра администрирования.

4. Не работает SMTP-авторизация, если в качестве адреса отправителя указан дополнительный SMTP-адрес (Microsoft Exchange Server).

5. В журнале событий могут появляться сообщения аудита с кодом события "0" и без указания категории. Такие сообщения могут быть проигнорированы.

6. При использовании внешнего PSC в событиях аудита vGate может возникать ошибка "Не удалось получить сертификат". Данная ошибка не влияет на работоспособность ПО vGate и VMware vSphere.

7. В журнале аудита не отображаются события о применении следующих политик: "Создание политики сложности паролей", "Настроить централизованное хранилище для сбора дампов памяти ESXi-сервера с помощью ESXi Dump Collector", "Запрет SSH", "Запрет ESXi Shell", "Проверка настроек SNMP-агента", "Удалить ключи SSH из файла authorized_keys", "Проверка описаний и уровней поддерживаемости VIB-пакетов", "Запрет логирования ВМ".

8. В журнале аудита не отображаются события об отмене следующих политик: "Синхронизация времени", "Разделение сетей консоли управления и виртуальных машин", "Использование протокола CHAP для iSCSI-устройств", "Избегать использования несохраняющихся (nonpersistent) дисков", "Отсылка событий сервера виртуализации на syslog-сервер", "Ограничение доступа к VMSafe Network API", "Отключение протокола IPv6", "Настройка безопасности для виртуальных коммутаторов", "Установка и поддержка целостности файловой системы", "Создание политики сложности паролей", "Настроить централизованное хранилище для сбора дампов памяти ESXi-сервера с помощью ESXi Dump Collector", "Запрет SSH", "Запрет ESXi Shell", "Проверка настроек SNMP-агента", "Удалить ключи SSH из файла authorized_keys", "Проверка описаний и уровней поддерживаемости VIB-пакетов".

9. Во время проверки статуса политики "Отключение ненужных устройств" в журнале аудита на сервере авторизации и в лог-файле агента vGate на ESXi-сервере появляются сообщения об ошибках.

10. При назначении некоторых политик безопасности на ESXi-сервер могут одновременно приходить сообщения аудита "Успех" и "Ошибка", если были изменены не все параметры данного сервера.

1.6. Веб-консоль

1. Возможно появление ошибки "Не удалось получить список зарегистрированных виртуальных машин", если были указаны некорректные или не были сохранены параметры подключения к серверу vCenter.

2. На Панели мониторинга в веб-интерфейсе vGate возможно отображение виджетов, которые ранее были отключены.

3. При создании правил корреляции не проверяется наличие подобных правил в списке. Поэтому возможно появление нескольких однотипных правил корреляции.

4. После неудачного подключения к серверу vCenter на сервере мониторинга не возобновляются попытки подключения. Чтобы выполнить повторное подключение к серверу vCenter нужно перезапустить службу vgate-event-collector.

5. При переходе со страницы аудита на Панель мониторинга возможна смена кодировки и некорректное отображение информации.

6. Невозможно удалить инциденты, предварительно не выполнив для них действие "Пометить как обработанный".

7. В веб-интерфейсе vGate в разделе "Аудит" осуществляется неправильный переход при вводе номера страницы вручную.

8. В веб-интерфейсе vGate в разделе "Аудит" при фильтрации событий по дате в окне настройки фильтра не сохраняется указанное значение даты.

9. При выполнении очистки событий аудита в веб-интерфейсе vGate возможно удаление не всех сообщений.

10. В некоторых версиях браузера после изменения правила, отслеживающего события в обход vGate, список выбранных событий в правиле отображается неверно.

11. Если при создании распределенного виртуального коммутатора создаются 2 портгруппы, в аудит vGate приходит сообщение о создании только одной портгруппы. Поэтому если создано правило (обход vGate) "Создание распределенной виртуальной портгруппы (DVPortGroup)", то при создании распределенного виртуального коммутатора будет генерироваться событие аудита. Аналогичная ситуация возникает при работе правила "Удаление распределенной виртуальной портгруппы (DVPortGroup)".

12. Происходит ложное срабатывание правил (обход vGate), отслеживающих выполнение операций с ESXi-сервером, если в vGate используется полное доменное имя ESXi-сервера (FQDN), а в сообщении от сервера vCenter указан IP-адрес сервера (или наоборот).

13. Возможно ошибочное появление уведомления "Ошибка обработки RPC-запроса на сервере мониторинга. Подробнее см. лог-файл на сервере мониторинга".

14. В веб-интерфейсе vGate невозможно выполнить отключение от сервера мониторинга.

15. Возможно некорректное отображение данных на графике в виджете "Политики безопасности".

16. При масштабировании окна браузера возможно некорректное отображение элементов веб-интерфейса.

17. При открытии информации о виджете "Инциденты" отображаются все существующие инциденты.

18. Для корректной работы межсетевого экрана vGate на ESXi-сервере версии 6.0 необходимо наличие установленных VMware Tools на виртуальных машинах.

19. При аутентификации пользователя с сервера авторизации vGate на серверах виртуализации не создаются инциденты по правилу корреляции "Аутентификация в обход vGate".

20. Если ESXi-сервер находится под управлением NSX, для корректной работы правил фильтрации в функции "Сегментирование" необходимо установить VMware Tools на ВМ, трафик которых контролируется, и указать в правилах фильтрации IP-адреса ВМ, а не их имена или MAC-адреса.

1.7. Прочие особенности

1. Если на компьютере, на котором установлен агент аутентификации vGate, в параметрах реестра ОС Windows отключить PMTU Discovery, то могут не работать некоторые соединения по протоколу TCP.

2. Если на компьютере, на котором установлен агент аутентификации vGate, запущенно VMRC, возможно появление ошибки "Unspecified error" в VCP на сервере авторизации.

3. Агент аутентификации vGate не поддерживает работу с доверенными доменами не из одного леса с доменом сервера авторизации. Также не поддерживается работа с доверенными доменами, если сервер авторизации входит в рабочую группу.

4. В vGate не поддерживается аутентификация пользователей Active Directory, для которых используется алгоритм шифрования данных DES.

5. Если авторизация в vGate выполнена с использованием учетной записи доменного пользователя, то при успешном подключении к vCenter с помощью vSphere Client в журнале аудита может появляться предупреждение "Попытка входа под учетной записью VMware завершилась неудачно".

6. Для конфигураций без vCenter или с несколькими vCenter (если используется переключение между ESXi-серверами или vCenter) в отчетах для ВМ вместо имен фиксируются идентификаторы (guid).

7. Не рекомендуется размещение сервера безопасности Secret Net в защищаемом периметре. Возможно возникновение проблем при входе пользователей на компьютеры с агентами Secret Net, расположенные вне защищаемого периметра.

8. Если на компьютере установлено СЗИ Secret Net, включен режим контроля потоков и выбран уровень сессии "строго конфиденциально", то работа с консолью управления блокируется.

9. Во время VMmotion включенной виртуальной машины может возникнуть ошибка "Device busy" при доступе к файлу *.nvram.

10. Отчет вида "Соответствие стандартам безопасности (кратко)" или "Соответствие стандартам безопасности (подробно)" покажет, что ESXi-сервер соответствует набору политик, даже если не были выполнены необходимые перезагрузки самого сервера или запущенных на нем ВМ (после которых политики начинают реально действовать).

11. Не поддерживается редактирование правила с атрибутом –z (disable_proxy), созданного с помощью команды clacl –W. Чтобы изменить такое правило, следует удалить старое правило и создать новое правило с нужным значением атрибута –z.

12. При переустановке ПО сервера авторизации vGate с сохранением существующей базы конфигурации будет очищен список добавленных доверенных доменов.

13. Команда для выключения виртуальной машины (esxcli vms vm kill или esxcli vm process kill) vSphere CLI недоступна.

14. Kaspersky Internet Security, установленный на компьютере с ПО vGate Client, по умолчанию будет проксировать сетевые пакеты от vSphere Client. При этом сетевой трафик будет идти от имени учетной записи компьютера с агентом vGate, а не от имени vGate-пользователя. Этого можно избежать, если настроить список доверенных программ или задать контролируемые порты в Kaspersky Internet Security.

15. vGate не защищает создание групп портов (Port Profiles) для Cisco Nexus 1000v switch, так как оно происходит через виртуальную машину Cisco. Средствами VMware vSphere Client невозможно создать группу портов для Cisco Nexus 1000v switch.

16. Для успешной установки ПО сервера авторизации vGate на компьютер, на который незадолго до этого было установлено ПО Secret Net 7, необходимо выполнить перезагрузку этого компьютера.

17. Vmdktool не работает для виртуальных машин, в пути к конфигурационным файлам (*.vmx) и vmdk-файлам которых присутствуют символы кириллицы.

18. Возможно возникновение проблем при запуске vSphere Client в конфиденциальной сессии Secret Net. В этом случае рекомендуется настроить механизм перенаправления согласно документации Secret Net.

19. Если на компьютере сервера авторизации vGate или на компьютере vGate Client установлено ПО VMware Workstation, то для виртуальных машин на данных компьютерах не работают адаптеры сетевых мостов (network bridge).

20. Не поддерживается фрагментация пакетов на пути между сервером авторизации и агентом аутентификации vGate.

21. Если для авторизации службы vGate VI Management Service в vSphere используется доменная учетная запись, администрирование виртуальной инфраструктуры возможно только при наличии доступа к ней через vCenter. Администрирование ESXi-сервера в обход vCenter в этом случае не поддерживается.

22. При использовании vSphere Web Client для администрирования виртуальной инфраструктуры возможно появление события аудита следующего вида: "Не удалось получить сертификат с 'IP:PORT'. Причина: Агент на 'IP' не установлен. Возможно, компоненты vGate не установлены на сервер".

23. При добавлении набора правил разграничения доступа на основе шаблона "Доступ View Connection сервера к vCenter" запрещено добавлять на vCenter правило доступа к порту 443, действующее для любого пользователя.

24. Событие создания ВМ не отображается в списке событий журнала аудита vGate при просмотре событий, связанных с данной ВМ (кнопка "Связанные события").

25. Не работает подключение CDROM/Floppy к компьютеру с vSphere Web Client, если управление Web Client выполняется при помощи плагина Remote Console Plugin.

26. В vSphere Host Client не отображаются уведомления о блокировании доступа компонентом "Контроль доступа vSphere". Если блокируется доступ к редактированию группы портов (port group), то группа портов удаляется.

27. Если в vGate с помощью меток безопасности настроен запрет операции Export OVF Template, то на компьютере, на котором установлен агент аутентификации vGate, нет всплывающих сообщений об отклонении операции, только сообщение об ошибке. Если для пользователя нет правил доступа к серверу ESXi, то операция Export OVF Template не может быть выполнена, но в журнале vGate появится сообщение об успешной операции (если метки безопасности разрешают данное действие).

28. Не поддерживается выполнение операций импорта виртуальных машин и vApp в vSphere Web Client (Flash) для всех версий vCenter.

29. Для совместной работы ПО vGate и VMware vCenter Server Appliance версии 6.5 (VCSA) необходимо, чтобы сервер VCSA был развернут на ВМ, запущенной на ESXi-сервере. Данный ESXi-сервер должен быть добавлен в VCSA как сервер виртуализации.

30. При установке (удалении) компонента защиты vCenter на сервере VCSA выполняется перезагрузка служб web-сервера, поэтому vSphere Web Client будет временно недоступен.

31. Если на компьютере с ПО сервера авторизации vGate включен Windows Firewall, то для корректной работы vCenter Server Appliance в настройках Windows Firewall необходимо открыть порт 30443.

32. Доступ к серверу vCenter по анонимным правилам с опцией "Контроль трафика" будет запрещен VCP.

33. В vSphere HTML5 Web Client при подключении к Windows vCenter не отображаются запреты операций со стороны vGate.

34. Возможна некорректная работа ПО vGate совместно с NIC Teaming.

35. Для корректной работы ПО vGate полные доменные имена серверов VCSA должны быть заданы с использованием символов в нижнем регистре.

36. Не поддерживается совместная работа персональных идентификаторов JaCarta и Рутокен.

37. Если на сервере авторизации vGate установлено ПО Secret Net Studio с включенным механизмом затирания данных, не рекомендуется использовать утилиту db-util.

38. При создании ВМ в рамках назначенного задания не происходит наследования меток безопасности хранилища.

39. Установка компонента защиты на сервер VCSA завершается ошибкой, если в DNS для VCSA указаны некорректные (помимо правильных) IP-адреса.

40. При смене пароля через консоль управления не проверяется соответствие политике "Разница при смене пароля".

41. Политика "Запрет доступа к консоли ВМ" не срабатывает при открытии консоли ВМ в браузере.

42. Не поддерживается мандатное управление доступом к консоли ВМ, если она открыта через web-клиент.

43. В аварийном режиме vGate функция автодобавления виртуальных машин продолжает работу.

44. Если DNS-сервер не доступен, могут возникнуть проблемы при загрузке правил доступа к серверу vCenter в тестовом режиме vGate.

45. Удаление ESXi-серверов (ВМ, vApp, хранилищ, сетевых устройств) вместе с каталогом из инвентаризации vCenter (Remove from Inventory) блокируется. Возможно удаление только пустого каталога.

46. После удаления ПО сервера авторизации vGate не возвращается значение ключа реестра IpEnableRoute".

47. Возможно появление ошибки "The wait operation timed out" при авторизации в агенте аутентификации vGate пользователем из группы Active Directory родительского домена при недоступном дочернем домене.

48. После удаления группы Active Directory из списка учетных записей vGate в агенте аутентификации завершается сессия пользователя Active Directory из этой группы, но такой пользователь может войти в систему снова еще на 1-2 минуты.

49. При удалении любой одной из групп Active Directory из vGate будет завершена сессия всех пользователей, добавленных в учетные записи vGate вместе с группами Active Directory.

50. При проблемах в доменной инфраструктуре (например, если выключены дочерние домены) авторизация в агенте аутентификации vGate и обновления списка учетных записей в консоли авторизации могут производится с задержками до 3 минут.

51. При проблемах в доменной инфраструктуре (например, если выключены контроллеры домена) установка сервера авторизации vGate в режиме интеграции с Active Directory может быть невозможна.

52. После установки дополнительных продуктов VMware vSphere или после добавления трастовых доменов (Identity Sources) на сервере мониторинга нужно выполнить команду для переподключения к серверу vCenter (sudo vgate-config vcenter).

53. Возможно появление ошибки "Local error" при авторизации в агенте аутентификации vGate пользователем из группы безопасности Active Directory.

54. При недоступности DNS-сервера возможна потеря связи (GRPC) с компонентами защиты vGate на защищаемых серверах, добавленных по имени (FQDN), даже при наличии записей в файле hosts.

55. Если на компьютерах, на которых установлено ПО сервера авторизации, используется компонент vGate Service Pack 1, то перед удалением/внесением изменений в параметры установки компонентов ПО vGate необходимо удалить компонент vGate Service Pack 1 с этих компьютеров. Если сначала было удалено ПО vGate, то удаление Service Pack 1 можно выполнить, запустив на исполнение файл vGateServicePack1.msi, или с помощью средства Windows "Программы и компоненты" (нажав кнопку "Изменить").

56. После установки компонента защиты на vCSA в VMware vSphere 7 перестает работать vCenter Server Life-cycle Manager и не отображается страница Certificate Management. Для доступа к ним необходимо перевести vGate в аварийный режим работы.

ООО "КОД БЕЗОПАСНОСТИ"

Почтовый адрес:	115127, Москва, а/я 66
Телефон:	(495) 982-30-20
E-mail:	info@securitycode.ru
Web:	https://www.securitycode.ru