Information security tool vGate

Commentary to the version 4.7

This document contains the description of the added functionality of vGate information security tool version 4.7, performance features and limitations of product applications that are needed to be considered while using the vGate software.

Contents

1. Changes and added functionality

Information on the added functionality of vGate version 4.7 is given below.

1.1. Version 4.7

1. The possibility of using vGate in heterogeneous virtual infrastructures is implemented, where vSphere, KVM, Skala-R, Proxmox and OpenNebula are used as virtualization platforms simultaneously.

2. Implemented support for KVM server management tools based on Proxmox and OpenNebula.

3. Added security policies for the vGate server: "Block concurrent sessions of virtual infrastructure administrators", "Password complexity requirements", "Session timeout in the web console", "Audit database backup". These policies allow the security administrator to configure the vGate server settings.

4. Added the "vGate network administrator" privilege, which can be granted to the security administrator. The privilege allows to view and configure the vGate firewall settings.

5. The ability to protect the configuration export file with a password is implemented.

6. Implemented support for the Jakarta personal identifier in the web console.

7. The functions of vGate server synchronization, export and import of configuration, and personal ID setting have been transferred from the vGate management console to the web console.

2. Hardware and software requirements

vGate 4.7 components have the following requirements.

Component	System requirements
vGate Server	Windows Server 2012 R2, version 6.3.9600 x64; Windows Server 2016, version 1607 x64 + Update KB4103720; Windows Server 2019, versions 1809, 2109 x64; Windows Server 2022 (21H2); Minimal required bandwidth for redundant networks — 10 Mbit/s. vGate Server requires 10 GB free disk space on a hard drive. Additionally: • JaCarta drivers (if using JaCarta security token); • Rutoken S, Lite and digital signature drivers (if using Rutoken security token)

Redundant vGate Server	Windows Server 2012 R2, version 6.3.9600 x64;
	Windows Server 2016, version 1607 x64 + Update KB4103720;
	Windows Server 2019, versions 1809, 2109 x64;
	Windows Server 2022 (21H2);
	vGate Server requires 10 GB free disk space on a hard drive.
	Minimal required bandwidth for redundant networks — 10 Mbit/s

vGate Client	• Microsoft Windows 10 1809, 2109 x64; • Windows 11; • Windows Server 2012 R2 6.3.9600 x64; • Windows Server 2016 1607 x64 + Update KB4103720; • Windows Server 2019 1809, 2109 x64; • Windows Server 2022 (21H2); • Linux Alt 8 SP with kernel version 5.10.150.std.def. The vGate Client component requires 200 MB on the hard drive. Additionally: • JaCarta drivers (if using JaCarta security token); • Rutoken S, Lite and digital signature drivers (if using Rutoken security token). vGate does not support simultaneous operation of JaCarta and Rutoken tokens while logging on via the vGate Client
Web console	• Yandex Browser 23.1.2.987 (64-bit); • Microsoft Edge 91.0.864.48 (64-bit); • Google Chrome 91.0.4472.101 (64-bit) and 91.0.4472.106 (32-bit); • Firefox 89.0 (64-bit); • Safari 12.1.2
vGate management console and report viewer tool	• Microsoft Windows 10 1809, 2109 x64; • Windows 11 (21H2); • Windows Server 2012 R2 6.3.9600 x64; • Windows Server 2016 1607 x64 + Update KB4103720; • Windows Server 2019 1809, 2109 x64; • Windows Server 2022 (21H2)
vGate Agent for 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). If you intend to use the firewall component, the server must have at least 6 GB of RAM. Operation of the vGate software on custom images of vSphere (from providers of HP and IBM servers and so on) is not guaranteed. The firewall component is not supported for VMware ESXi 7.0 Update 3i
vCenter protection component (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. vCenter protection component requires 200MB free disk space on a hard drive. vGate is not guaranteed to work with ESXi free releases and on vSphere custom images (from producers of HP servers, IBM etc.)

Component	System requirements
vGate Agent for vCenter (vCSA)	• Windows Server 2012 R2 6.3.9600 x64; • Windows Server 2016 1607 x64 + Update KB4103720; • Windows Server 2019 1809 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. vGate Agent for vCenter requires 200 MB on the hard drive. Operation of the vGate software on the vSphere custom images (from providers of HP and IBM servers and so on) is not guaranteed
vGate Agent for PSC	• Platform Services Controller 6.7; • Platform Services Controller Appliance 6.7
vGate Agent for KVM	• Ubuntu 18.04.6 LTS; • Ubuntu 20.04.3 LTS; • Astra Linux Common Edition "Орел" 2.12.22; • Alt Virtualization Server 10; • Alt Server 8 SP; • R-virtualization platform 7. Additionally, the Glibc package must be installed on a KVM server
	The vGate software integration with the following KVM virtualization management tools is supported: • Proxmox 7.2; • OpenNebula 5.10.5, Proxmox 7.0 (included in Alt Virtualization Server 10); • Skala-R Management 1.80 and 1.93
Monitoring server	• VMware vSphere 6.5; • VMware vSphere 6.7; • VMware vSphere 7.0. Virtual machine requirements: • CPU cores - 2; • RAM - 4 GB; • free space - 20 GB
Analysis server	Virtual machine requirements: • CPU cores - 2 for each network interface for traffic analysis; • RAM - 4 GB; • free space - 20 GB

Hardware requirements.

- vGate Server requires at least one Ethernet-interface on the computer when deploying vGate using a router, and at least two Ethernet interfaces when using the vGate Server for traffic routing.
- We do not recommend using DHCP protocol for Ethernet-interfaces connected to the secure network perimeter or the administration network perimeter.
- vGate Server installation on a VM is available but not recommended due to security reasons.
- Deployment of the vGate Server on a VM may cause system malfunction.

3. Installation features

The list of issues you may face while installing vGate is given below. Please, read the list prior to installing vGate.

1. The vGate Server and vCenter Agent cannot be installed on a domain controller.

2. IPv6 is not supported. For vGate operation, you have to disable IPv6 in the network adapter properties.

3. While installing the vGate Server, the following characters are supported for the security administrator name: [A-Za-z0-9-_].

4. If a dialog box with the network adapter properties is opened, vGate installation is not available.

5. If Secret Net Studio is installed on a computer, flow control mode is enabled and the session level is set to any value, except “unclassified”, vGate Server and vGate Client cannot be installed or uninstalled.

6. If Secret Net Studio is installed on a computer, integrity control mode with computer blocking in case of integrity violation, vGate Server and vGate Client cannot be installed.

7. If you reinstall vGate along with PostgreSQL, you have to manually delete the installation folder (%ProgramFiles%\PostgreSQL\12) once PostgreSQL is uninstalled.

8. If the list of protected subnets is changed using the “Change” button in the program uninstallation menu on the vGate server, you have to execute the following command once the installation is completed: %ProgramFiles%\vGate\drvmgr.exe e. This command updates the driver settings.

9. Manual vGate Agent installation on vCenter must be performed by a local administrator or domain administrator using the setup program. Otherwise, an error occurs.

10. For correct operation of Active Directory accounts in the Active Directory integration mode, a domain controller in the external perimeter of the administration network is required.

11. If the domain includes more than one vGate Server and their service accounts are stored in different Active Directory containers, you have to delete all objects related to the vGate Server prior to updating the vGate Server.

12. If the vGate setup program cannot find the vGate Server installation file in the modification of installer parameters mode, you have to manually specify a path to the installation file.

13. The vGate Agent can be installed on vCenter Server Appliance only by a local root user.

14. The vGate Server installation on a computer may finish with an error if the computer was disconnected from the network before the installation.

15. Some issues may occur while installing the vGate Client on a computer with the installed virtual adapters.

16. The vGate Agent update to the new vGate version that is not supported by the vGate Server software version is executed incorrectly.

17. To correctly install vGate on computers with Windows OS, disable the Self-Defense component in Kaspersky Endpoint Security (10.3 and later).

18. If you remove an ESXi server, that is added to the vGate list of protected objects by its DNS name, from vCenter Inventory, and then add it again by its IP address, errors may occur while deploying the vGate Agent on this server.

19. The vGate Server and Secret Net Studio Security Server cannot be installed on the same computer.

20. While installing the vGate Server, you may receive the "An error occurred while creating the vGate authorization service account" error due to incorrect substitution of the OU (Organizational unit) name.

21. When aggregating network interfaces, you cannot assign the same IP address to a standalone interface and to a group of interfaces. Otherwise, vGate installation will fail.

22. Installation of vGate components on Windows may fail with the network driver installation error. In this case, we recommend installing the latest updates for Windows.

23. When you install the redundant vGate Server, the virtualization server credentials are not copied from the main server to the redundant server. When you change the redundant server role to the main server role, the virtualization server credentials are not saved on the new main server.

24. While installing vGate components on vCSA or PSC 6.7 servers with small capacity, an error related to the timeout expiration (5 minutes by default) may appear. In this case, it is necessary to increase the "VcpOnvCenterTimeout" parameter value in the Windows registry (for example, 10 minutes).

25. If, before the vGate Server installation, Windows log is cleared and the computer is not restarted, the installation may be executed incorrectly.

26. Prior to installing the vGate Agent on an ESXi server, we recommend you power off all virtual machines on this server. Otherwise, errors may occur.

27. vGate Agents can be installed or removed on a vCSA HA cluster if all ESXi servers with virtual machines in the cluster are controlled by vSphere or not controlled. This statement also applies to vSphere 6.7 virtual machines of the vCSA HA cluster with external PSC.

4. Known issues

The list of known issues for vGate 4.7 is given below.

4.1. Common

1. For correct operation of vGate Server components, free TCP port 80 is required.

2. vGate Server renaming is not supported in vGate.

3. User account names cannot contain the following symbols: \?[*@.

4. Disks without a serial number are not supported by the iSCSILocker utitlity.

5. If IPv6 is enabled on a vCenter, you may get access via the vSphere Client bypassing vCenter protection component. ESXi server protection components also do not block access over IPv6 inside the perimeter.

6. If Raw Device Mapping is used, mandatory access control is not supported.

7. For correct operation of the "File operations in data storages" privilege, the corresponding access rule for ESXi server must be configured for this user (TCP protocol, destination port 443).

8. If SNMP port is changed after the vGate Agent installation on an ESXi server, you have to manually open a new port as outgoing in the ESXi server firewall settings.

9. While using NAT through a network gateway, only one vGate Client can connect to the vGate Server and protected servers.

10. vGate integration with Secure Boot for VMware ESXi Server is not supported.

11. While managing two vGate Servers using the same vGate Client, if at least one vGate Server is switched to the emergency mode, network traffic will not be signed later on.

12. A user session in the vGate Client is unlimited.

13. For a domain controller in the vGate secure perimeter, you have to create a rule that allows incoming connections to all TCP ports.

14. In the vGate management console, the process of installing vGate Agents on Windows computers may hang.

15. When you remove the vGate Agent from vCenter with the help of the "Programs and features" menu in Windows OS, vGate Agent will not be removed from a standalone PSC (Platform Services Controller). In this case, you have to manually uninstall the vGate Agent on the PSC server.

16. To correctly finish a user session, you have to log off not only from the vGate Client, but also from vSphere Web Client and Cloud Director administrative portal in a browser. While working with virtual infrastructure through the vGate web interface (without vGate Client), you have to close the browser with deletion of cookies.

17. For correct operation of vGate, FQDN and NetBIOS name of the computer with the installed vGate Server must match. The computer name cannot be longer than 15 characters and contain unsupported characters.

4.2. Integrity control

1. After VMmotion, checksums recalculation may be required.

2. After changing VM Russian-language parameters in vSphere Client, checksum calculation is not supported.

3. If Fault Tolerance is enabled, integrity control of VM configuration files is not supported.

4. If the "Trusted boot loading of virtual machines" policy is applied to a VM controlled by an ESXi/Proxmox server, and then vGate Agent is installed on this server, VM integrity control error will appear.

5. If a VM with the installed vGate Server is located on an ESXi server from the VMware cluster, while migrating this VM to another ESXi server, integrity control will not be applied to this VM, as a file with checksums is written only to the current ESXi server.

6. If the vGate Server is installed on a VM to which with the "Trusted boot loading of virtual machines" policy applied, in case of integrity violation, the VM status will take the "Integrity confirmed" value in the vGate management console.

7. By default, the "VM BIOS integrity" parameter is selected in the "Trusted boot loading of virtual machines" policy settings. In this case, VM status may change from "Integrity confirmed" to "Integrity compromised" every time the VM is started (due to the *.nvram file integrity violation). To avoid this, you have to clear the "VM BIOS integrity" check box.

8. While importing a configuration the export of which was performed with integrity violations, checksums of all files are recalculated. These checksums will be reference ones.

4.3. vGate Server replication

1. Error messages may occur while logging on to the system via the vGate Client after passing control to a redundant vGate Server.

2. If a built-in Windows domain account is used for the computer authentication, it can be denied while switching to the redundant vGate Server. In this case, we recommend you restart the computer.

3. If the main vGate Server is unavailable, the redundant vGate cannot be accessed from the external perimeter of the administration network. To access the redundant vGate Server, you have to use local access.

4. You can connect to the vGate Server twice with the same user account using the main IP address and IP address for replication. After this, user authentication errors and errors of signing the Client network traffic may occur.

5. After passing control to another vGate Server by the hot standby service, a message prompting to finish the server configuration appears in the vGate management console on the disabled vGate Server. This operation may fail. To restore vGate Server operation, follow the steps described in the operation manuals.

6. The redundant vGate Server do not display the status (version) of the vGate Agent installed on the vCenter server.

7. If vGate Agents are installed on KVM server, automatic switching to the redundant vGate server is not supported

4.4. Security policies

1. The migration of a powered-on VM between ESXi server/OpenNebula virtual storage units is not supported if the "Trusted boot loading of virtual machines" policy is applied to this VM.

2. If the "Trusted boot loading of virtual machines" policy is enabled, application of other policies that results in changing the configuration file requires VM checksums to be recalculated.

3. The "Prevent mixing various types of network traffic" policy is not supported for a Distributed Switch.

4. The "Clean up deleted virtual machine disks" policy is not supported for virtual machines that have snapshots.

5. The "Clean up deleted virtual machine disks" policy is not supported for virtual machine templates.

6. The "Clean up deleted virtual machine disks" policy does not operate automatically for Linked Clones.

7. Deleting VMware View VM clones in the vSphere Client directly connected to an ESXi server bypassing vCenter can lead to removing master replica disks if the "Clean up deleted virtual machine disks" policy is applied to the clones.

8. The following policies are not supported for virtual machines that use disks of other virtual machines: "Clean up deleted virtual machine disks", “Clean up deleted KVM disks”, “Clean up deleted Proxmox disks”. If the same disk is used by two virtual machines to one of which such a policy is assigned, when deleting the VM to which the policy is assigned, the disk will not be cleaned up. After this, when applying this policy to any other virtual machines, errors may occur while deleting virtual machines or cleaning up disks.

9. The “Clean up deleted OpenNebula disks” policy is not supported for virtual machines that use disks in the Persistent mode.

10. An outdated version of the USB driver is downloaded for the "Block USB media at ESXi servers" policy to operate on the ESXi server 6.5. After unassigning the policy, a new version of the driver (vmkusb) is not downloaded.

11. When viewing through the vCenter or ESXi Host Client, parameters, that are changed as a result of applying the following policies, take correct values only after restarting hostd: "Enable BPDU filter on the ESXi host to prevent being locked out of physical switch ports with Portfast and BPDU Guard enabled", "Set a timeout to limit how long the ESXi Shell and SSH services are allowed to run", "DCUI timeout value", "Set a timeout to limit how long the ESXi Shell and SSH services are allowed to run" and "Configure NTP time synchronization".

12. If the "Trusted boot loading of virtual machines" policy is assigned on a VM and powering on the VM with integrity violation issues is allowed, in case of changing the controlled vmx file parameters, rejection of changes is possible only when the VM is powered off. Otherwise, changes will not be rejected, even if a message about successful rejection of changes appears.

13. If IPv6 was disabled on an ESXi server as a result of the "Disable IPv6" policy operation, after unassigning this policy and restarting the server, IPv6 will still be disabled.

14. While automatically checking the "Configure NTP time synchronization" policy, the following error may appear: "Error "service is not installed (ntpd)" occurred while checking status of "Configure NTP time synchronization" policy".

15. If the "Enable lockdown mode to restrict remote access" and "Disable DCUI to prevent local administrative control" policies are included in a template, when assigning this template to an object, only the "Enable lockdown mode to restrict remote access" policy will be applied.

16. If you apply the "Enforce password history" policy to an ESXi server 6.5, the "KeyError" error occurs.

17. When assigning the "Integrity control of ESXi server configuration files" policy to an ESXi server 7.0 U2, you have to clear check boxes of the following files: /etc/vmware/hostd/config.xml and /usr/lib/vmware/hostd/bin/upgrade-config.py. Otherwise, applying of the policy will end with a count error.

18. On the computer designated to be the vGate Server, we do not recommend disabling the “User Account Control: Admin Approval Mode for the Built-in Administrator account” parameter in the Windows local security policy, as it can cause failures in the vGate operation.

19. If the High Availability function is configured for a Proxmox virtual machine to which the “Trusted boot loading of Proxmox” policy is assigned, the VM startup will not be blocked in case of integrity violation.

20. We do not recommend powering off a server right after removing a Proxmox virtual machine to which the “Clean up deleted Proxmox disks” policy is assigned from it. Cleanup time depends on the VM disks size. If the server is powered off, cleanup operation is canceled.

4.5. Audit

1. Audit events for SMB protocol include accounts related to a computer, not to a user.

2. After changing the ESXi server network configuration (adding/deleting network adapters), events related to actions in the Networking configuration section may not be registered. In this case, we recommend restarting the vGate Server.

3. Events of anonymous access to the vGate Server in the external perimeter of the administration network are not displayed in the event log.

4. SMTP authentication does not operate if an additional SMTP address (Microsoft Exchange Server) is specified as a sender address.

5. The "Failed to get certificate" error may appear in the vGate event log when using an external PSC. This error does not affect vGate and VMware vSphere.

6. The event log does not display events of applying the following policies: "Ensure proper SNMP configuration", “Integrity control of ESXi server configuration files”, “Ensure that port groups are not configured to the value of the native VLAN”, “Ensure that port groups are not configured to VLAN 4095 except for Virtual Guest Tagging (VGT)”.

7. The event log does not display events of unassigning the following policies: "Disable IPv6", "Ensure proper SNMP configuration", “Integrity control of ESXi server configuration files”, “Ensure that port groups are not configured to the value of the native VLAN”, “Ensure that port groups are not configured to VLAN 4095 except for Virtual Guest Tagging (VGT)”.

8. Error messages appear in the event log on the vGate Server and in the vGate Agent log file on the ESXi server while checking the "Disconnect unauthorized devices" policy status.

9. When assigning some security policies on an ESXi server, "Success" and "Error” messages may appear at the same time if not all server parameters is changed.

4.6. Web console

1. The "Failed to get the list of registered virtual machines" error may occur if the settings of connection to the vCenter server are invalid or not saved.

2. When creating correlation rules, the presence of such rules in the list is not checked. Therefore, the presence of the same correlation rules is possible.

3. You cannot delete events which are not marked as processed.

4. While clearing audit events in the vGate web interface, not all messages can be deleted.

5. If two port groups are created when creating a distributed virtual commutator, vGate audit receives a message about creating only one port group. If the "Create DVPortGroup" rule (bypassing vGate) is created, an audit event will be generated when creating a distributed virtual commutator. The same appears when the "Delete DVPortGroup" rule operates.

6. False activations of rules (bypassing vGate) that monitor an ESXi server operation appears if the ESXi server FQDN is used in vGate and a message from the vCenter server contains the server IP address (or vice versa).

7. Data in the "Security policies" widget may be displayed incorrectly.

8. When scaling a browser window, elements of the web interface may be displayed incorrectly.

9. If a user is logged on from the vGate Server, alerts by the "Authentication bypass vGate" correlation rule are not registered on virtualization servers.

10. If an ESXi server is controlled by NSX, for correct operation of firewall rules on the “Firewall" component, VMware Tools must be installed on virtual machines with enabled traffic control and VM IP addresses (not their names or MAC addresses) must be specified in firewall rules.

11. If the vCenter server IP address is specified when connecting to the protected virtualization server via the vGate web interface, authorization will be performed only at the second attempt.

4.7. Other features

1. If you disable PMTU Discovery in the Windows registry parameters on a computer with the installed vGate Client, some TCP connections may be unavailable.

2. The "Unspecified error" may appear in VPC of the vGate Server if VMRC is running on a computer with the installed vGate Client.

3. The vGate Client does not support work with trusted domains that are not from the same forest with the vGate Server domain. Also, if the vGate Server is included in a workgroup, work with trusted domains is not supported.

4. vGate does not support authentication of Active Directory users to which the DES algorithm is applied.

5. If a user is logged on to vGate using a domain account, the "Login attempt using VMware account has failed" warning may appear in case of successful connection to vCenter.

6. For configuration without vCenter or with several vCenter servers (if you intend to switch between ESXi servers or vCenter), GUID are used in reports for virtual machines instead of names.

7. We do not recommend deploying the Secret Net Studio Security server in the secure perimeter. Some issues may occur when logging on to computers with the installed Secret Net Studio agents that are located outside the secure perimeter.

8. If Secret Net Studio is installed on a computer, flow control mode is enabled and the session level is set to any value, except “unclassified”, work with the management console is blocked.

9. During VMmotion of a powered-on VM, the "Device busy" error may appear when accessing the *.nvram file.

10. The “Security standards and regulations compliance (in brief)” or “Security standards and regulations compliance (detailed)” report displays that an ESXi server complies with a set of policies, even if the server or virtual machines running on it were not restarted (policies only take effect after a restart).

11. By default, Kaspersky Internet Security installed on a computer with the vGate Client will proxy network packets from the vSphere Client. In this case, the network traffic goes from the vGate Agent computer account, not from vGate user account. To avoid it, you have to configure the list of trusted applications and specify controlled ports in Kaspersky Internet Security.

12. vGate does not protect the creation of Port Profiles for Cisco Nexus 1000v switch as it is done using the Cisco VM. You cannot create Port Profiles for Cisco Nexus 1000v switch with the help of the VMware vSphere Client.

13. Some issues may occur while running the vSphere Client in the Secret Net Studio confidential session. In this case, you have to configure the redirection mechanism according to the Secret Net documentation.

14. If the VMware Workstation software is installed on the vGate Server computer or vGate Client computer, network bridges are not available for virtual machines on these computers.

15. Packets fragmentation is not supported on a path between the vGate Server and vGate Client.

16. If you use a domain account to log in to the rhuid service in vSphere, virtual infrastructure administration is available only using access through the vCenter server. In this case, ESXi server administration bypassing vCenter is not supported.

17. While using the vSphere Web Client for virtual infrastructure administration, the "Failed to get certificate from ‘IP:PORT’. Reason: Agent is not installed on ‘IP’. Make sure the vGate agent is installed on the server" audit event may appear.

18. While adding a set of access rules based on the "View Connection Server access to vCenter" template, you cannot add an access rule for vCenter (port 443) that is applied to all users. This port is used in the template by default. If necessary, create similar vCenter access rules applied to certain users.

19. VM creation event is not displayed in the vGate event log while viewing events related to the VM (the "Related events" button).

20. CDROM/Floppy connection is not available on a computer with the installed vSphere Web Client, if the Web Client is managed using Remote Console Plugin.

21. In the vSphere Host Client, notifications about blocking access by the “vSphere access control” component are not displayed. If a privilege to edit a port group is blocked, the port group will be deleted.

22. If the Export OVF Template operation is prohibited in vGate with the help of security labels, only error message appears on a computer with the installed vGate Client, messages about the operation rejection do not appear. The Export OVF Template operation cannot be performed if a user has no access rules for the ESXi server. However, the vGate event log will contain a message about successful operation (if it is allowed by security labels).

23. VMs and vApp import in the vSphere Web Client (Flash) is not supported for all vCenter versions.

24. For the simultaneous operation of vGate and VMware vCenter Server Appliance 6.5 (vCSA), you have to deploy a vCSA server on a VM that is running on an ESXi server. This ESXi server must be added to VCSA as a virtualization server.

25. While installing (removing) the vGate Agent on a vCSA server, web-server services are restarted, therefore, the vSphere Web Client will be temporarily unavailable.

26. If Windows Firewall is enabled on a computer with the installed vGate Server, for correct operation of vCenter Server Appliance, you have to open port 30443 in the Windows Firewall settings.

27. Operations blocked by vGate are not displayed in the vSphere HTML5 Web Client while connecting to Windows vCenter.

28. vGate may operate incorrectly with NIC Teaming.

29. For correct vGate operation, full domain names of VCSA servers must be specified using lowercase characters in the settings of connection to the virtualization server in the web console.

30. vGate does not support simultaneous operation of JaCarta and Rutoken tokens.

31. If the Secret Net Studio software with the enabled data wipe mechanism is installed on the vGate Server, we do not recommend using the db-util utility.

32. When you create a VM using a scheduled task, the storage security labels are not inherited.

33. Installing the vGate Agent on a VCSA server fails if in DNS both invalid and valid IP addresses are specified for the VCSA server.

34. If you change your password using the vGate management console, compliance with the "Differ from the previous password by" policy is not checked.

35. The "Deny use of the VM console" policy does not operate when you open the VM console in a browser.

36. Mandatory control of access to a VM console is not supported if it is opened via the web client.

37. Automatic adding of virtual machines function continues to operate in the vGate emergency operation mode.

38. If the DNS server is not available, you may have issues while loading vCenter access rules in the vGate test operation mode.

39. Removal of ESXi servers (VM, vApp, datastores, network devices) along with the directory from the vCenter Inventory is blocked. The directory can only be deleted if it is empty.

40. After the vGate Server software removal, the "IpEnableRoute" registry key remains set to 1.

41. The "The wait operation timed out" error may appear while logging on to the vGate Client as a user from a group in Active Directory parent domain if a child domain is not available.

42. If you delete one of the Active Directory groups from vGate, all user sessions added to the vGate accounts along with the Active Directory groups will be terminated.

43. If there are problems in the domain infrastructure (for example, child domains are disabled), authorization in the vGate Client and update of the list of accounts in authorization console may be performed with delays up to 3 minutes.

44. If there are problems in the domain infrastructure (for example, domain controllers are disabled), vGate Server installation in the Active Directory integration mode may be unavailable.

45. Once you installed the VMware vSphere additional software or added Identity Sources on the vGate monitoring server, you have to execute the following command to reconnect to the vCenter server: sudo vgate-config vcenter.

46. The "Local error" error may appear when logging on to the vGate Client as a user from the Active Directory security group.

47. Unavailability of the DNS server may lead to a loss of connection (GRPC) with vGate Agents on protected servers which are added by their names (FQDN), even if there are logs in the host file.

48. Backup error may appear when using the envget utility. In this case, we recommend you manually run the utility from the Temp folder of the current administrator.

49. The "User session is not found" error may appear when logging on through the vGate web interface (without the vGate Client) during the active session.

50. File operations in datastores (download/upload) may be unavailable in the vSphere Web Client may be unavailable when logging on through the vGate web interface (without the vGate Client). In this case, you have to use the ESXi Embedded Host Client.

51. If an ESXi server is powered off and then powered on, the configured correlation rule that monitors actions bypassing vGate may be falsely triggered.

52. Once the vGate Agent is installed on vCSA, Life Cycle Manager stops operating and the Certificate Management page is not displayed in VMware vSphere 7. To access them, switch vGate to the emergency operation mode.

53. Live Migration of a virtual machine between two ESXi servers does not operate if the vGate Agent is installed at least on one of the servers. For correct operation, you have to combine the servers into a cluster.

54. Exporting reports to DOC is not supported in the vGate management console.

55. When migrating a VM to another ESXi server, allowing outgoing firewall rules may operate incorrectly.

56. When changing priorities of custom confidentiality levels, confidentiality levels of active administrator sessions may be displayed and controlled incorrectly.

57. If you get the “Error while getting the list of container images: Remote service returns an error. (200 Empty message body)” error, restart the rhuid.exe service. The error may appear while getting the list of container images of the embedded Harbor Registry.

58. While changing a virtual machine configuration (related to adding or changing the network adapter), applying of firewall rules to this virtual machine may take some time.

59. Once you revert a virtual machine to a snapshot, it may be necessary to reconfigure the firewall settings for this virtual machine in the vGate web console.

60. For correct operation of the vGate software, vGate and PostgreSQL installation folders must be added to the Windows Defender exclusions.

61. If a user is logged on through the web interface (without the vGate Client), connection via VMRC is not supported.

62. vGate for Skala-R 4.6 configuration cannot be imported into vGate 4.7.

63. If the vGate configuration includes user names that contain the “/” character, once this configuration is imported, vGate web console may operate incorrectly.

64. If a user connects to a protected server through the web interface (without the vGate Client) for the first time, the user has to log on to vGate twice. To avoid this, we recommend that you specify FQDN of the protected ESXi/vCSA server when logging in.

65. If the OpenNebula management server is not added to the list of protected servers, OpenNebula virtual machines will not be displayed on the “Virtual machines” page in the vGate web console.

66. If you configure a connection to vCenter and KVM servers, then add vCenter, ESXi and KVM servers to the list of protected servers, and after that delete the connection to the vCenter server, you will not be able to assign security policies and security labels to KVM servers.

SECURITY CODE LLC

Mailing address:	P.O. Box 66, Moscow, Russian Federation, 115127
Phone:	(495) 982-30-20
Email:	info@securitycode.ru
Web:	https://www.securitycode.net/