SECURITY code

vGate R2

Administrator guide

Principles of operation

Security Code LLC reserves the right to change the information contained herein without special notice.

Mailing address:	**P.O. Box 66, Moscow, Russian Federation, 115127 Security Code LLC**
Phone:	**+7 495 982-30-20**
Email:	**info@securitycode.ru**
Web:	**https://www.securitycode.net/**

Table of contents

List of terms and abbreviations 4

Introduction 5

About vGate 6

Protection principles and tools 6

Protection of the VMware virtual infrastructure management tools 6

Mechanisms of VM protection 7

Rules of license usage 8

vGate architecture 9

vGate components 9

Variants of component location 10

vGate installation features for different vCSA architectures of VMware vSphere 11

vGate functionality 15

Administrative function differentiation 16

Mandatory control of access to confidential resources 17

Types of security labels 17

Management of confidentiality level 18

Operations regulated by the access management function 18

Procedure for security label assigning 19

Applicability of access control function in VMware vSphere 20

Security policies 22

vGate Server security policies 22

Integrity control and trusted boot loading 22

Integrity control for VMware vSphere 22

Integrity control for Skala-R, KVM, Proxmox, OpenNebula 23

Logging events related to information security 23

Centralized management and audit 23

Automation of vGate Agents deployment 23

Hot standby function of the vGate Server 23

Management of several vGate Servers 24

Synchronization of vGate Server settings 24

Report preparation 24

Protection of KVM servers 24

Proxmox and OpenNebula support 24

Virtual infrastructure monitoring 25

vGate Functionality for VMware vSphere 25

Agentless control of vCSA operations 25

Access to virtual infrastructure without vGate Client 25

Support of VMware Auto Deploy 25

Control of the Cloud Director operations 25

Control of the VMware vSAN operations 25

Network firewall 26

Reviewing ESXi servers for compliance with security policies 26

Integrity control of ESXi server configuration files 26

Integrity control of container images 26

vGate compatibility with other products 27

Support of VMware View 27

Support of the standard Distributed vSwitch and Distributed vSwitch Cisco Nexus 1000v 27

Solutions for protection of virtual machines 27

Documentation 28

List of terms and abbreviations

AD	Active Directory is the MS Windows directory service
DNS	Domain Name System
iSCSI	Internet Small Computer System Interface is a protocol for management of data storage and transmission systems based on TCP/IP
vCenter	The tool for centralized management of ESXi servers and virtual machines
vCSA	vCenter Server Appliance is a virtual module with the installed vCenter server and services that are connected with it
PSC	Platform Services Controller is a component that supports the operation of VMware virtual infrastructure services
DB	Database
VM	Virtual machine
OS	Operating system
RAM	Random access memory
SAN	Storage area network
CPU	Central processing unit

Introduction

This guide is designed for administrators of the product vGate R2 (hereinafter — vGate). The document covers general information on the application and functionality of vGate.

Website. You can go to Security Code LLC website (https://www.securitycode.net/) or contact the company representatives by email: support@securitycode.ru.

Training courses. You can learn more about the hardware and software products of the Security Code LLC in the authorized training centers. The list of training centers and learning terms are available at https://www.securitycode.net/company/training/.

You can contact the company representatives regarding the organization of the training process by email: education@securitycode.ru.

The latest version of the operation manuals for the product "vGate R2" is available on the company's website at https://www.securitycode.net/products/vgate/.

You can request the latest version of Release Notes by email: vgateinfo@securitycode.ru.

Chapter 1
About vGate

vGate is designed to protect virtual infrastructures deployed using the VMware vSphere, KVM, OpenNebula, Proxmox and Skala-R virtualization systems.

Protection principles and tools

Protection of the VMware virtual infrastructure management tools

Virtual infrastructure management tools are as follows:

- ESXi servers designated for running virtual machines.
- vCenter (vCSA) servers designated for centralized management of the VMware virtual infrastructure.
- Skala-R Management servers designated for centralized management of the Skala-R virtual infrastructure.
- vSphere Host Client — web client designed for the ESXi server management.
- VMware Cloud Director — the platform for virtual infrastructure management based on the IaaS model.
- VMware Harbor — embedded container image registry.
- Tools designed for the infrastructure maintenance, for example, VMware Consolidated Backup, VMware Update Manager, vCenter Server Appliance.
- Third-party tools for the infrastructure monitoring and management.
- KVM servers.
- Proxmox servers.
- OpenNebula Platform.

Compromising of any of these elements may lead to the compromising of the virtual machine group or of the whole virtual infrastructure.

Virtual infrastructure management tools are located inside the perimeter that is protected by vGate. To protect them from unauthorized access, there are the following functions in vGate:

Function	Description
Actor authentication	Authentication of users and computers that attempting to get access to protected objects is based on protocols that are insensitive to the password interception attempts and that prevent interference in the data transferring.
Discretionary control of access to the virtual infrastructure management tools	Discretionary control of access to the objects which are located inside the protected perimeter, is based on the lists of access management and connection parameters (protocols, ports). Network traffic between authenticated actors and protected objects is signed, thereby the protection from Man in the Middle attacks is ensured.
Limitation of the information security administrator privileges in the virtual infrastructure management	Information security administrator privileges in the virtual infrastructure management are limited to the possibility of viewing the virtual infrastructure configuration. By default the information security administrator does not have access to VM disks and cannot gain access to the confidential data stored on them. They also do not know the virtual infrastructure administrator passwords because they must be changed by the virtual infrastructure administrators at first logon. Therefore, the information security administrator cannot perform potentially hazardous actions with virtual infrastructure
Control of the virtual infrastructure administrator actions	In vGate, there is an ability to control the virtual infrastructure administrator actions at the level of individual commands for the virtual infrastructure management
Blocking access to the protected perimeter through the web interface	An ability to access elements of the virtual infrastructure management from the external network through the browser is blocked. Access through the web interface may be allowed by the information security administrator (if needed)
Configuring password policies	Password policies allow to ensure the compliance with the industry requirements for password protection

Function	Description
Mandatory control of access to confidential resources	Mandatory access control function allows to ensure more granular access (in comparison with discretionary access control) to the confidential data.
Blocking any network traffic from VM to the virtual infrastructure management tools	Provides protection of the virtual infrastructure management tools from unauthorized access of the compromised VM
Filtering vCenter network traffic in the administration network	The vGate Agent is installed on the vCenter to ensure the incoming traffic filtering. The function provides protection from unauthorized access of the virtual infrastructure administrator to the virtual infrastructure management tools in the administration network
Providing a trusted software environment of the ESXi server	The list of executable modules which may be normally run on the ESXi server is limited to standard ESXi modules and standard vGate modules. If needed, the information security administrator may extend the list of programs that are allowed to be run on the ESXi server
Control of devices mounting to the ESXi server	Device mounting control function is used to prohibit connections of the portable devices such as USB flash drives to the server
Integrity control of the ESXi server configuration files	Reviewing compliance of checksums for selected protected server configuration files. File integrity is controlled by the vGate Agents installed on ESXi servers
Control of operations with KVM and Skala-R servers	The vGate Agent installed on KVM, Skala-R, Proxmox and OpenNebula protects servers from unauthorized access

Mechanisms of VM protection

To ensure protection of virtual machines and data processed on them, the following functions are provided:

Function	Description
VM integrity control and detailed audit of changes in configuration file	Includes integrity control of VM settings before its boot loading, VM snapshots and VM BIOS image, as well as the integrity control of VM templates, blocking operations of VM deleting and VM converting to a template. The function ensures the VM program loading. VM integrity control is based on the checksum invariability. Along with the integrity control, audit of changes in protected VM VMX file is performed with an option to discard changes (if needed). Functions are realized within security policies
Approval of VM configuration changes by the information security administrator	While modifying the VM configuration with enabled integrity control, checksums change. Information security administrator may approve or discard changes in the VM configuration. If changes approved, VM checksum is recalculated
Prohibition on creating snapshots	The function is used to deal with violation of operation integrity in systems that process restricted data. Realized within security policies. The feature is available only in VMware vSphere
Prohibition on cloning VM	The function allows to limit unauthorized copying (cloning) of virtual machines that process restricted data. Realized within security policies. The feature is available only in VMware vSphere
Cleaning up the VM memory	The function guarantees the absence of residual information about processed data in VM memory. Memory cleanup may be single or double. Function is realized within security policies. The feature is available only in VMware vSphere
Cleaning up the residual information on deleted VM disks	The function guarantees the absence of residual information about processed data on hard disks after VM deletion. Residual information cleanup may be performed by writing zero values (single or double). Realized within security policies
Control of mounting devices	The function allows to restrict the unauthorized copying of VM data over the virtual device connection. Realized within security policies. The feature is available only in VMware vSphere
Restricting access to VM console	The function allows to set stricter access rules for the certain VM by blocking access to its console. This function is implemented as a user privilege. In the VMware vSphere , this feature is also implemented within security policies

Function	Description
Restricting VM files downloading	With the help of this mechanism you may limit the number of persons who may export VM files. Mechanism is realized as a user privilege
Using network firewall	Function allows to filter network traffic in the virtual machine network. The feature is available only in VMware vSphere

Rules of license usage

In vGate, the following licensing options are possible:

- vGate Standard,
- vGate Enterprise,
- vGate Enterprise Plus.

For each of these editions, license is purchased for a specified number of sockets installed on protected ESXi, KVM and Skala-R servers. vGate editions differ in functionality (see p.**15**).

To protect the Scala-R infrastructure, a vGate Enterprise or vGate Enterprise Plus license is required.

To learn about the vGate software in demonstration mode, the activation key is required. To receive an activation key for the vGate demonstration version, leave request with the specified edition and license duration at vg-ateinfo@securitycode.ru.

Note. You may send your questions and wishes connected with the vGate operation to the given mailing address. Questions related to the technical support should be sent to support@securitycode.ru.

To use vGate after expiration of the trial period you should purchase a license and register the received activation key in the vGate web console. Activation key can be unlimited and time-limited. Information on the status of the key is displayed in the vGate web console.

Chapter 2
vGate architecture

vGate components

vGate components and their functions are presented in the table below:

Component	Functions
vGate Server	• Authentication of users and computers. • Control of access to the virtual infrastructure management tools. • Security events logging. • Data storing (accounting information, audit journals and vGate configuration). • Data replication (if the redundant server is available). • Synchronization of vGate server settings. • Automatic deployment of vGate Agents on protected servers
Redundant vGate Server	• Storing the settings and the list of users. • Data replication. • Main server replacement in case of failure
vGate Client	• Identification and authentication of users. • Identification and authentication of computers. • Integrity control of the vGate Client components. • Selecting session level while working with confidential resources (with enabled session level control). • Security events logging
vGate Agent for ESXi server	• VM integrity control and trusted boot loading. • Integrity control of vGate modules and settings. • Integrity control of ESXi server configuration files. • Integrity control of container images. • Security events logging. • Protection from unauthorized access in the administration network. • Control of mounting devices. • Providing the trusted software environment.
vGate Agent for vCenter (vCSA)	• Protection from unauthorized access in the administration network. • Management of incoming traffic filtering
vGate Agent for PSC	Providing protection from unauthorized access in the administration network
vGate Agent for KVM	• Protection of KVM, Skala-R, OpenNebula and Proxmox virtualization servers. • VM integrity control and trusted boot loading. • Protection from unauthorized access in the administration network. • Security events logging
Web console	• Centralized management of vGate. • Management of user and computer accounts. • Assigning access privileges to protected objects. • Installing and configuring vGate Agents on the protected servers. • Import and export of the vGate configuration. • Configuring the hot standby function for the server. • Configuring mandatory access control. • Configuring security policies for protected objects. • Calculating VM configuration checksums. • Configuring Rutoken and JaCarta personal identifiers. • Configuring and viewing event logging journals • Configuring network traffic filtering rules. • Monitoring of security events. • Synchronization of vGate Servers
Monitoring server	Collection and correlation of virtual infrastructure events
Analysis server	Analyzing the VM network traffic within "Deep packet inspection" function

Component	Functions
Report viewer tool	Preparing reports on the status of security parameters of the virtual infrastructure, occurred events, and configuration changes
vGate deployment service	Installation of vGate Agents components on protected servers

Variants of component location

vGate components may be located as follows:

Component	Variants of location
vGate Server	Dedicated computer (installation on VM is allowed but not recommended)
Redundant vGate Server	Dedicated computer (installation on VM is allowed but not recommended)
vGate Client	Virtual infrastructure administrator workstation, information security administrator workstation (if it is located in the external perimeter of the administration network), server of the services (DNS, AD etc.)
vGate Agent for ESXi server	ESXi servers
vGate Agent for vCenter	vCenter server
vGate Agent for PSC	Platform Services Controller server
vGate Agent for KVM	KVM, Skala-R, OpenNebula and Proxmox servers
Report viewer tool	vGate Server (if the information security administrator workstation is located on the vGate Server)
vGate deployment service	vCenter server
Monitoring server	Virtual machine
Analysis server	Virtual machine

vGate Server is installed on the dedicated computer. This computer may be used as a workstation for the information security administrator.

Attention! Installation of the vGate Server on VM is allowed, but we do not recommend locating it on the server protected by the vGate.

If the vGate Server is supposed to be located in the server room (to control temperature and implement organizational measures to protect computers in a protected perimeter), the information security administrator workstation should be organized on an individual computer.

vGate installation features for different vCSA architectures of VMware vSphere

vGate may be used in virtual infrastructures controlled by vCenter Server Appliance versions 6.5, 6.7 and 7. Supported vCSA architectures and their features of the vGate software installation are listed as follows.

vCenter (vCSA) with built-in PSC deployed on its ESXi server

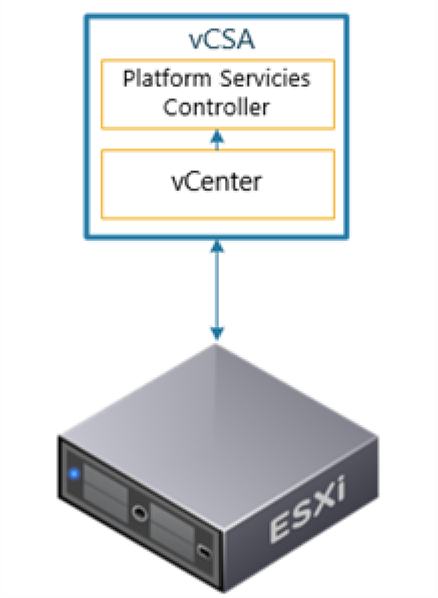


Figure 1vCenter (vCSA) with built-in PSC on its ESXi server

While installing the vGate software, credentials for accessing PhotonOS are required.

vCenter (vCSA) with external PSC deployed on its ESXi server

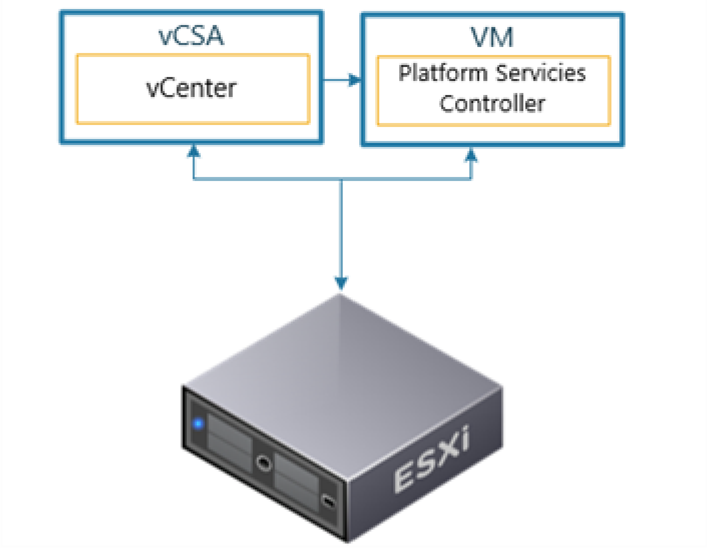


Figure 2vCenter (vCSA) with external PSC on its ESXi server

While installing the vGate software, credentials for accessing PhotonOS are required.

vCenter (vCSA) with built-in PSC deployed on the outside ESXi server

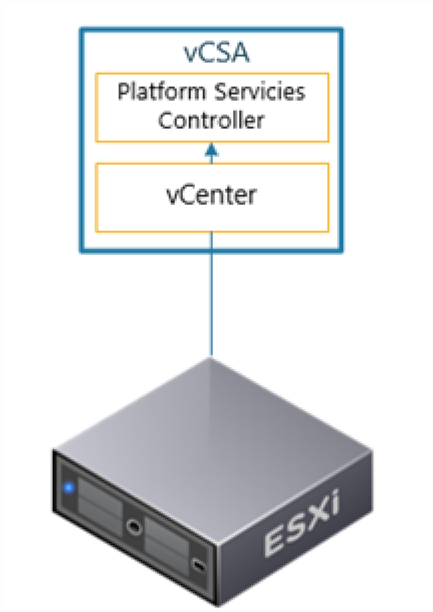


Figure 3vCenter (vCSA) with built-in PSC on the outside ESXi server

While installing the vGate software, parameters of connection to ESXi server and credentials for access to PhotonOS are required.

vCenter (vCSA) with external PSC deployed on the outside ESXi server

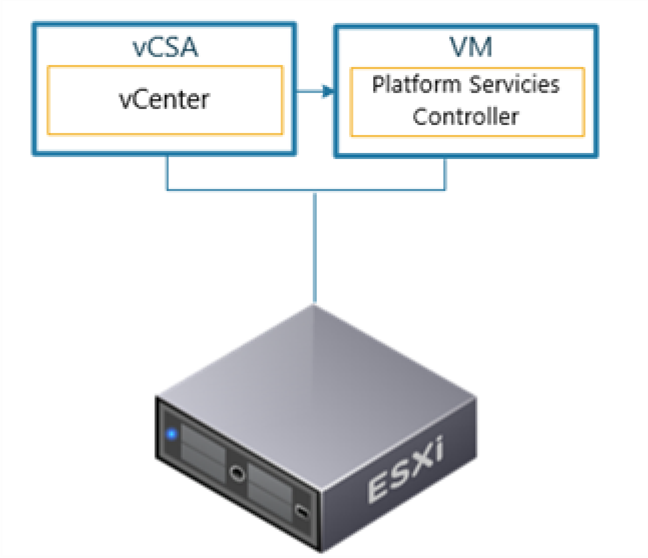


Figure 4vCenter (vCSA) with external PSC on the outside ESXi server

While installing the vGate software, parameters of connection to ESXi server and credentials for access to PhotonOS are required.

vCSA High Availability deployed on its ESXi server

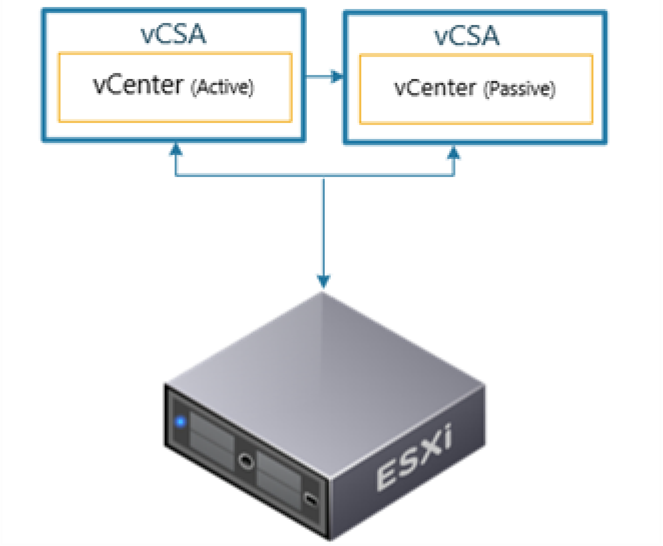


Figure 5vCSA High Availability on its ESXi server

While installing the vGate software, credentials for accessing PhotonOS are required. While installing vGate on the passive node of the vCenter server cluster, vSphere services are stopped.

vCSA High Availability deployed on the outside ESXi server

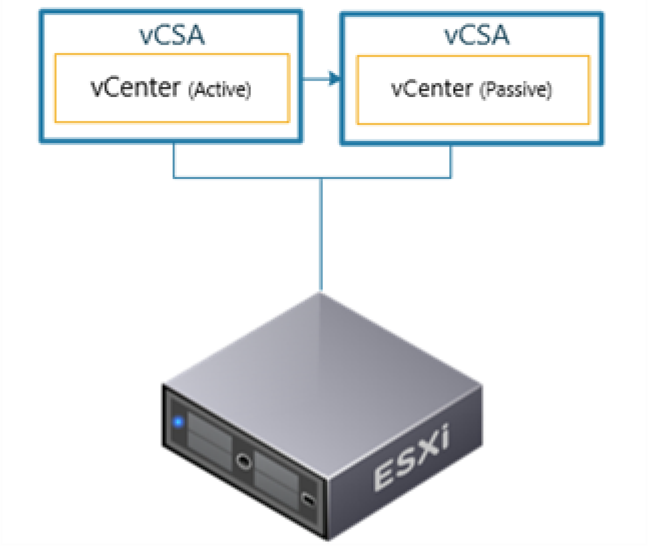


Figure 6vCSA High Availability on the outside ESXi server

While installing the vGate software, parameters of connection to the ESXi server and credentials for access to PhotonOS are required. After installing vGate on the passive node of the vCenter server cluster, vSphere services are stopped.

vCSA High Availability is deployed on several ESXi servers

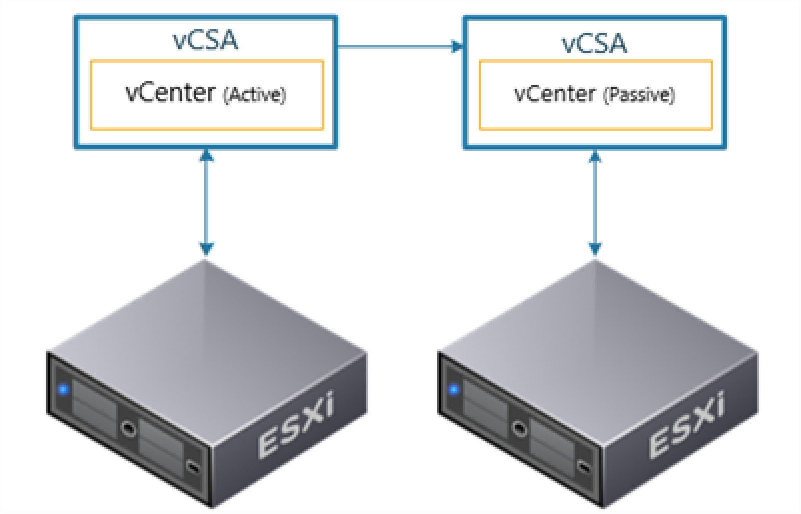


Figure 7vCSA High Availability on several ESXi servers

While installing the vGate software, credentials for accessing PhotonOS are required. While installing vGate on the passive node of the vCenter server cluster, vSphere services are stopped.

vCSA High Availability deployed on several outside ESXi servers

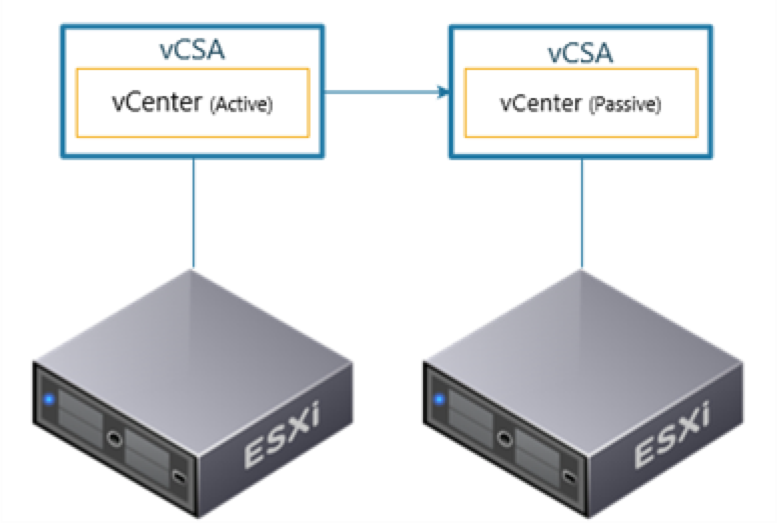


Figure 8vCSA High Availability deployed on several outside ESXi servers

While installing the vGate software, parameters of connection to all ESXi servers and credentials for accessing PhotonOS are required. While installing vGate on the passive node of the vCenter server cluster, vSphere services are stopped.

Chapter 3
vGate functionality

vGate is delivered in three editions: Standard, Enterprise and Enterprise Plus (see p.8). vGate Enterprise and Enterprise Plus are extended editions of vGate Standard. They include additional functions for ensuring the virtual infrastructure security. The list of the vGate software functionality is presented in the comparison table.

Function	vGate Standard	vGate Enterprise	vGate Enterprise Plus
Administrative function differentiation, authentication of administrators and computers	+	+	+
Mandatory access control to confidential resources	+	+	+
Security policies	+	+	+
VM integrity control and trusted boot loading	+	+	+
Integrity control of ESXi server configuration files	+	+	+
Logging information security events	+	+	+
Centralized management and audit	+	+	+
Sending messages about audit events over SMTP and Syslog protocols	+	+	+
Automation of vGate Agents deployment	+	+	+
Agentless control of vCSA operations	+	+	+
Virtual infrastructure administrator access to protected servers without vGate Client (for VMware vSphere only)	+	+	+
Backup of the vGate configuration and event log	+	+	+
Protection of KVM servers	+	+	+
Protection of Skala-R servers	+	+	+
Support of Proxmox and OpenNebula	+	+	+
Management of several vGate Servers at the same time	-	+	+
Synchronization of vGate Server settings	-	+	+
vGate Server hot standby	-	+	+
Support of VMware Auto Deploy	-	+	+
Support of VMware vCenter Linked Mode	-	+	+
Support of VMware vCenter High Availability	-	+	+
Control of the VMware Cloud Director operations	-	+	+
Control of the VMware vSAN operations	-	+	+
Preparing reports on information security events and status	-	-	+
Virtual infrastructure monitoring	-	-	+
Network firewall (for VMware vSphere only)	-	-	+
Reviewing ESXi servers for compliance with security policies	-	-	+
Integrity control of container images (for VMware vSphere only)	-	-	+

Administrative function differentiation

In vGate there is the principle of role differentiation — differentiation of rights to manage the virtual infrastructure and information security.

While installing the vGate Server (see the document [2]), an account of the chief information security administrator is created.

Attention! There is only one chief information security administrator role, and it cannot be passed to another information security administrator. The chief information security administrator has the number of privileges in comparison with other information security administrators. Only this account has rights to add access control rules for an external adapter of the vGate Server or redundant vGate Server, and to edit an account of the chief information security administrator. However the chief information security administrator does not have an access to the virtual infrastructure due to security concerns.

Initially the chief information security administrator allocates rights between vGate users using two main roles: virtual infrastructure administrator and information security administrator.

These roles have the following privileges.

Role	Privileges
Information security administrator	• Discretionary control of access to the virtual infrastructure management tools. • Configuring mandatory access control to the confidential resources. • Managing security policies of the virtual infrastructure management tools and objects in the protected perimeter. • Audit of security events. • Configuring vGate. • Managing user accounts (creating, deleting, editing) except the chief information security administrator account. • Configuring and managing the redundant vGate Server (if available). • Viewing the settings of virtual infrastructure management elements with the help of VMware vSphere, Skala-R, Proxmox and OpenNebula management tools. • Virtual infrastructure monitoring. • Configuring network traffic filtering rules
Virtual infrastructure administrator	• Managing virtual infrastructure with the help of VMware vSphere, Skala-R, Proxmox and OpenNebula management tools. • Choosing the session confidentiality level while working with confidential resources (to use this function, vGate configuration is needed, it is disabled by default). • Configuring the virtual infrastructure administrator account for viewing virtual infrastructure management elements with the help of VMware vSphere, Skala-R, Proxmox and OpenNebula management tools

Note. In regard to the roles described above, the following terminology is used in vGate:

- "Administrator" — the user who performs functions of the information security administrator.
- "Users" — virtual infrastructure administrators.

Authentication of the virtual infrastructure administrators, information security administrators and computers is performed using the vGate Client.

Mandatory control of access to confidential resources

In vGate, the mandatory control of access to confidential resources is used.

While performing the number of standard operations with the virtual infrastructure objects, security labels of the virtual infrastructure administrator accounts and resources are compared.

Security labels are assigned to the following resources:

- ESXi server,
- vCenter server,
- KVM server,
- Skala-R server,
- Skala-R data storage,
- vSphere data storage,
- vSphere virtual machine,
- KVM virtual machine,
- vSphere network adapter,
- vSphere virtual network,
- distributed virtual switch,
- user,
- object group,
- Cloud Director organization.

Types of security labels

In vGate, there are following types of security labels.

Label	Description
Hierarchical label	Contains only one confidentiality level
Non-hierarchical label	Contains one or several equal confidentiality categories
Compound label	Contains one confidentiality level and one or several confidentiality categories

Confidentiality level characterizes access level with regard to resource or clearance level with regard to the user.

By default, the following confidentiality levels are used (in ascending order):

- non-confidential;
- restricted.

Information security administrator can create custom confidentiality levels.

The confidentiality category defines if the resource belongs to a group or the user has access to a group (for example, a department in a company). The security label may contain several confidentiality categories at the same time. Such a label on the resource points out that this resource is used by the several different groups at the same time (for example, VM may be used by an accounting department and a personnel department at once); on the user it tells that this user has clearance to resources of such groups (for example, the user may manage VM an accounting department and a personnel department at the same time).

The list of five confidentiality categories represented with colors ("Blue", "Green", "Yellow" etc.) is configured in the system by default. The information security administrators may modify the list of available categories as they see fit.

Management of confidentiality level

When mandatory access control based on hierarchical or compound labels is configured, the user may perform operations with resources, that have the confidentiality level lower or equal to their confidentiality level.

When the session level control is enabled (this function is controlled by the information security administrator and disabled by default), the user may manage their confidentiality level. For this, the user may choose the session level lower or equal to their confidentiality level. In this case, the user gets access to resources with a confidentiality level that is equal to the chosen session level.

Operations regulated by the access management function

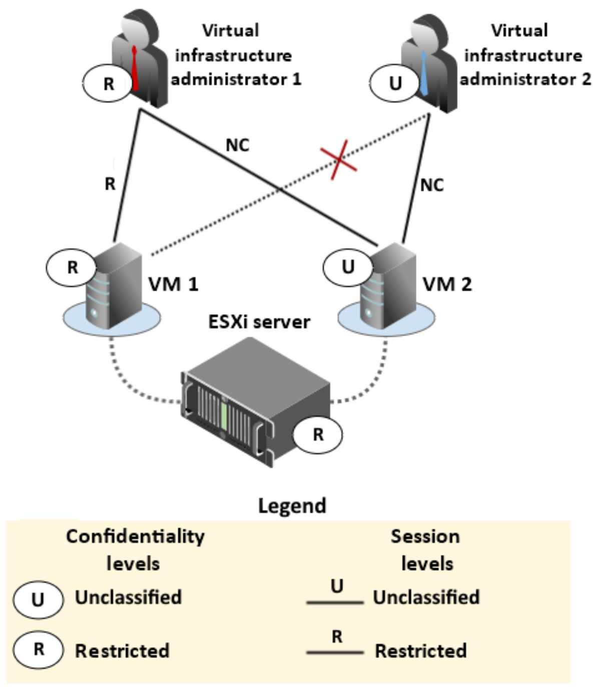
Mandatory access control is used to manage privileges for such operations as a VM running, VM parameters editing, network parameters editing etc. The complete list of operations with confidential resources which are regulated by mandatory access control and conditions of their performance are presented in the annex to the document [2].

It is to be noted that access of the virtual infrastructure administrator to the ESXi, Skala-R or KVM server is determined by access control rules.

Examples of access granting procedure for running VM are considered below.

Example 1. Management of VM running while using the confidentiality levels

On the ESXi server with "restricted" confidentiality level for which an additional parameter "Allowed to run VM with the lower level" is set, VM 1 with "restricted" confidentiality level and VM 2 with "non-confidential" level may be run. Let us consider which virtual machines may be run by the virtual infrastructure administrator 1 with "restricted" confidentiality level and virtual infrastructure administrator 2 with "non-confidential" level.

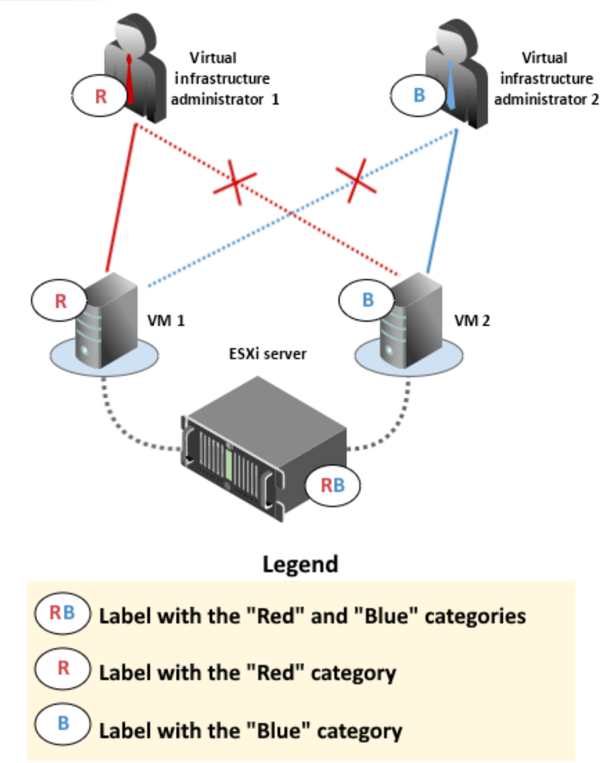


While the session level control is enabled, the virtual infrastructure administrator 1 may run both virtual machines (VM 1 and VM 2) by choosing the session confidentiality level equal to the VM confidentiality level. The virtual infrastructure administrator 2 may run only VM 2; running of VM 1 is blocked for him.

Example 2. Management of VM running while using the confidentiality category

Note. Access control by confidentiality categories is disabled by default. This function may be configured and enabled by the information security administrator in the vGate web console.

On the ESXi server that is common for the "Red" and "Blue" categories, VM 1 with the "Red" category and VM 2 with the "Blue" category may be run.


Virtual infrastructure administrator 1
R
Virtual infrastructure administrator 2
B
R
VM 1
B
VM 2
ESXi server
RB
Legend
RB Label with the "Red" and "Blue" categories
R Label with the "Red" category
B Label with the "Blue" category

Virtual infrastructure administrator 1 can run the VM 1 only, virtual infrastructure administrator 2 can run the VM 2 only.

Procedure for security label assigning

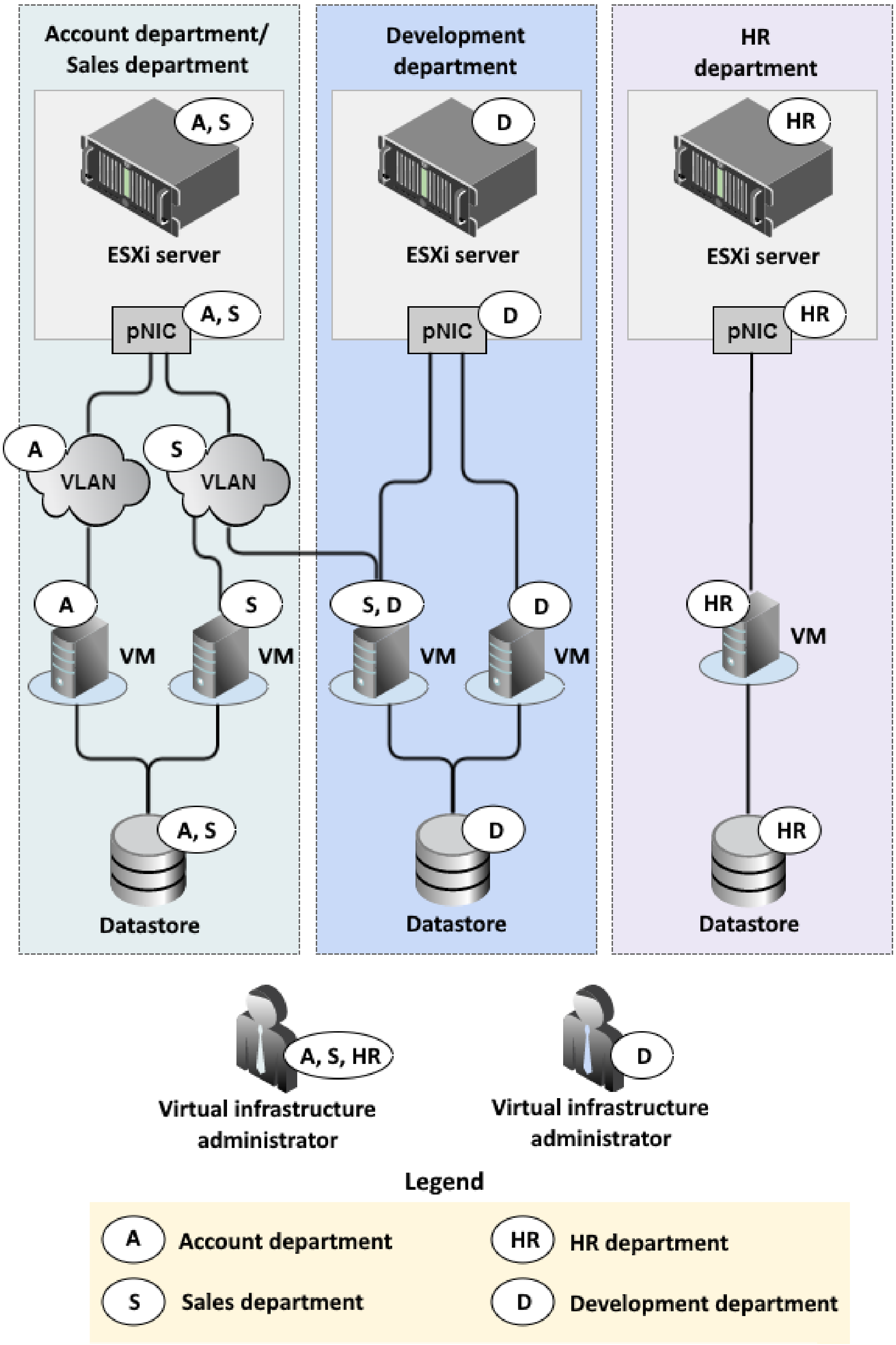
Security labels are assigned by the information security administrator using the vGate web console while configuring the information security tool (see the "Configuring mandatory control of access to confidential resources" section in the document [2]).

Security labels are assigned automatically to the newly created virtual machines (see the "The list of main operations with confidential resources and conditions for performing them" section in the annex of the document [2]).

Applicability of access control function in VMware vSphere

1. Control of the virtual infrastructure administrator access to the resources of different departments

Non-hierarchical labels are used to control access to the resources of different departments. An example of non-hierarchical labels configuration for such a case is presented in the figure below.

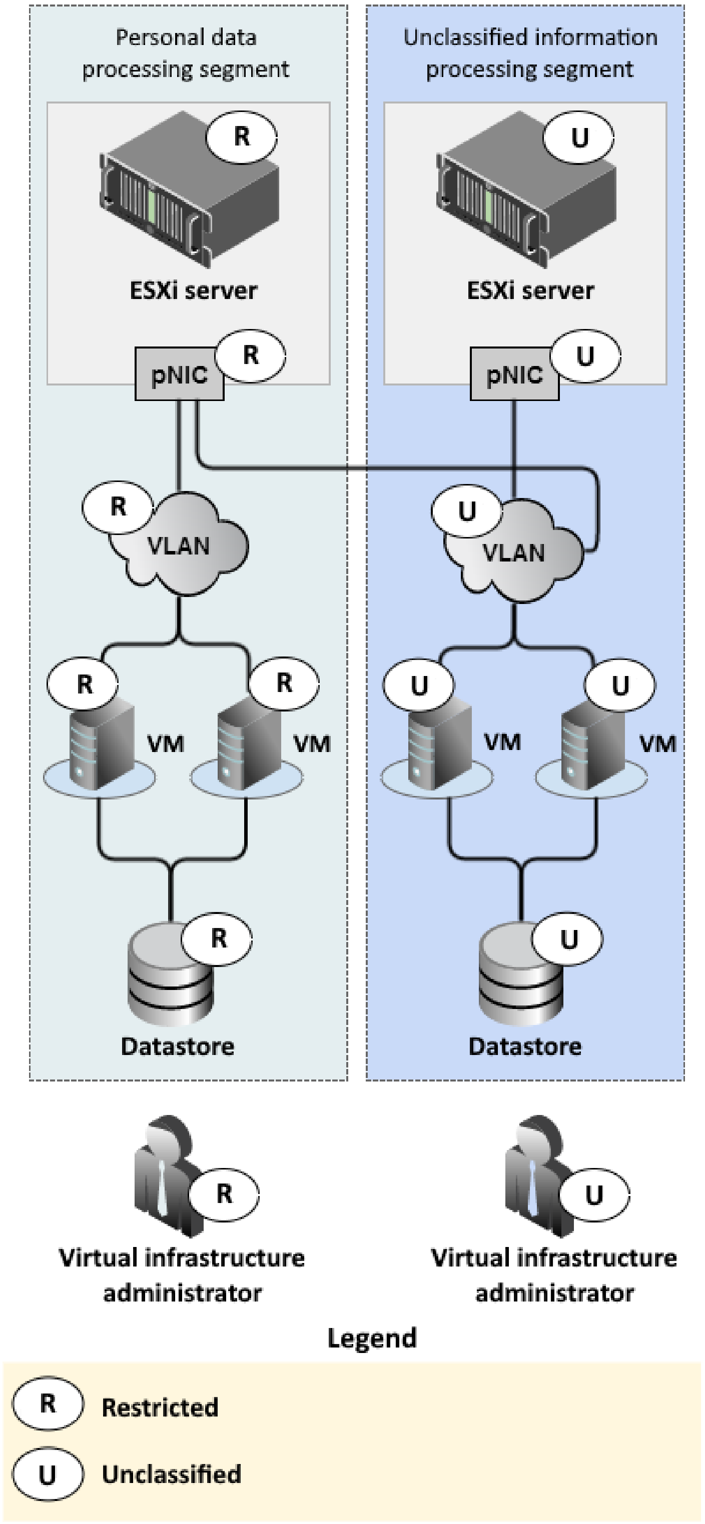


In the example, the personnel department and the development department each have their ESXi-server, and the accounting department and the sales department have common ESXi-server.

Note. In the example, standard confidentiality categories are adapted to users' objectives.

2. Control of the virtual infrastructure administrator access to non-confidential data and personal data

To control access of the virtual infrastructure administrator to personal data and non-confidential resources, hierarchical labels are used. An example of configuring hierarchical labels for this case is presented in the figure below.


Personal data processing segment
Unclassified information processing segment
R
ESXi server
pNIC
R
R
VLAN
R
VM
R
VM
R
Datastore
U
ESXi server
pNIC
U
U
VLAN
U
VM
U
VM
U
Datastore
R
Virtual infrastructure administrator
U
Virtual infrastructure administrator
Legend
R Restricted
U Unclassified

3. **Control of the virtual infrastructure administrator access to non-confidential data processed in different departments**

Sometimes it is needed to control access not only to resources of different departments but also to data with different levels within one department.

In this case, compound labels are used.

Security policies

In vGate, security policies control the settings of protected objects that are crucial for the virtual infrastructure security.

Security policies can be assigned to the following objects:

- ESXi server;
- vGate Server;
- virtual machine;
- virtual machine template;
- network adapter;
- distributed virtual switch;
- Embedded Harbor Registry.

For ease of use, security policies are grouped in policy sets (templates). Using the templates, the virtual infrastructure protection mechanisms may be quickly configured according to the requirements of industry standards (for example, PCI DSS and СТО БР ИББС), the law on personal data, FSTEC of Russia requirements for particular class of automated systems and manufacturer's guidelines (such as vSphere 6.7 Security Configuration Guide and VMware ESXi 6.7 Benchmark).

Templates may be used in any combination, depending on the specifics of the company. Moreover, the information security administrator may selectively apply policies from the template, i. e. enable necessary policies and disable unused.

Policy set based on templates is applied directly to the objects or object groups.

It should be noted that from the set of policies assigned to the object, only policies that designed for this object work: for ESXi server - ESXi server policies, for VM - VM policies, etc.

Every policy in the set may be in one of the following states:

- enabled (policy is working);
- disabled (policy is not working).

vGate Server security policies

vGate supports assigning security policies to the vGate Server.

The following functions are implemented:

- limiting the number of simultaneous sessions of virtual infrastructure administrators from different workstations;
- ensuring that the password meets the specified requirements;
- termination of an inactive administrator session in the vGate web console after the specified time;
- saving all audit events to the selected directory on the vGate Server when the values of the specified parameters are exceeded.

Integrity control and trusted boot loading

Integrity control for VMware vSphere

To ensure the integrity control of the software environment and the trusted boot loading of virtual machines in vGate, components with following protection functions are installed on each ESXi server:

- integrity control of VM settings before boot loading;
- integrity control of VM shapshots;
- integrity control of VM BIOS image;
- OS trusted boot loading is performed using the integrity control of the virtual disk's boot sector;

- integrity control of VM template;
- integrity control of VM template BIOS image;
- integrity control of VM template disk images;
- integrity control of ESXi server configuration files;

Integrity control for Skala-R, KVM, Proxmox, OpenNebula

To ensure the integrity control of the software environment and the trusted boot loading of virtual machines, vGate components performing integrity control of the main configuration file are installed on each Skala-R, KVM, Proxmox and OpenNebula server.

Logging events related to information security

In vGate, security events are logged for all protected computers, including computers related to the virtual infrastructure management tools.

Events are centrally stored on the vGate server in security events log. Logged events are described by the set of parameters (see the "Event parameters" section in the document [2]).

vGate allows to select and view events from the security events log.

Centralized management and audit

The vGate web console is used for centralized management and audit.

The following functions are available in the vGate web console:

- centralized management of vGate settings;
- monitoring the virtual infrastructure events;
- management of the firewall settings (for VMware vSphere only);
- configuring and viewing event logs and reports;
- user account management;
- configuring security policies, checking protected ESXi servers for compliance with policies;
- export and import of vGate configuration;
- configuring the hot standby function for the server;
- synchronization of vGate Servers;
- configuration of JaCarta and Rutoken personal identifier.

Note. The chief information security administrator cannot download virtual machine files or create scheduled tasks due to security concerns.

All settings are centrally stored on the vGate Server.

Automation of vGate Agents deployment

vGate contains the built-in component for the automation of vGate Agent deployment on all protected virtualization servers (ESXi, KVM, Skala-R, OpenNebula and Proxmox servers).

The "vGate deployment service" component is automatically installed when installing the vGate Agent on the vCenter server.

Attention! vGate Standard allows to protect only one vCenter server. If several vCenter servers are operated in a company, and these servers are linked using the VMware vCenter Linked Mode, the vGate Agent must be installed on each of them. This function is available in vGate Enterprise and Enterprise Plus only (see the "Functionality" section in the document [1]).

Hot standby function of the vGate Server

This function is available only in vGate Enterprise and Enterprise Plus.

The hot standby function is used to ensure the fault tolerance of the vGate Servers. In case of the main vGate Server failure (hardware, system or vGate service failure), the redundant server automatically takes all the management functions. After getting control, the redundant server takes all functions of the vGate management and authorization of the virtual infrastructure administrators.

Therefore, system operation cannot be blocked for a long time. As long as the relevant information about the system configuration, user accounts, etc. is stored on the redundant vGate Server, the vGate Server replacement will be almost unnoticed for the virtual infrastructure administrators who work in the protected virtual environment.

After the main vGate Server recovery or replacement, system management functions may be returned to that server or left to the former redundant server.

Note. The function of automatic switching to the redundant vGate Server should be enabled in the vGate R2 web console (see the document [2]). This function is disabled by default.

Management of several vGate Servers

This function is available only in vGate Enterprise and Enterprise Plus.

The vGate Client can connect to several vGate Servers. Management of each vGate Server is performed using the vGate web console.

Note. vGate Servers should belong to the same domain or trusted domains.

Synchronization of vGate Server settings

This function is available only in vGate Enterprise and Enterprise Plus.

vGate supports the simultaneous operation of the vGate Client and several vGate Servers. The vGate administrator may enable synchronization of security labels, user accounts, security policies and object groups between these vGate Servers. If one of the vGate Servers is unavailable, the information security administrator may connect to any other vGate Server from the forest.

Report preparation

This function is available only in vGate Enterprise Plus.

In vGate, it is possible to prepare reports that allow to get relevant information on current license, status of security settings, virtual infrastructure objects compliance with security policies, as well as on configuration changes and occurred information security events over a certain period of time.

vGate allows to choose an optimal report design for each company (select color scheme, add company name and logo on a report form).

The report can be exported in PDF format in the vGate web console.

Protection of KVM servers

vGate allows to protect KVM virtualization servers.

The following functions are available:

- storing account data for connection to KVM servers;
- adding KVM servers to the list of servers protected by vGate;
- installing vGate Agents on KVM servers;
- control of the VM loading;
- integrity control of VM when loading;
- cleaning up the residual information after VM deletion;
- assigning security labels and security policies to the virtual machines;
- adding KVM servers to the groups (includes automatic adding)
- export and import of the KVM servers configuration;
- synchronization of vGate settings on KVM servers between vGate Servers.

Proxmox and OpenNebula support

vGate supports Proxmox and OpenNebula management tools for KVM servers.

Virtual infrastructure monitoring

This function is available only in vGate Enterprise Plus.

In the vGate web-console, data collection and analysis is performed on the virtual infrastructure objects: vGate Server, protected servers, computers in the external perimeter of the administration network, on which the vGate Client is installed.

The ability to create and configure correlation rules is implemented. The rules allow to track certain events that occur in the virtual infrastructure under specified conditions.

The data on operation of the correlation rules and on audit events is presented in a graphical form on the monitoring panel in the vGate web console.

vGate Functionality for VMware vSphere

Some vGate functions are only available for VMware vSphere.

Agentless control of vCSA operations

Control of vCSA operations is available without installing the vGate Agent.

Note. Agentless control of operations is supported for VMware vCenter Server Appliance 7.0 update 1 and later.

Access to virtual infrastructure without vGate Client

vGate provides access to protected servers from the virtual infrastructure administrator workstation over the vGate web interface (without the vGate Client).

Prior configuration of access rules in the vGate management console is needed to provide access to the virtual infrastructure through the web interface.

Note. Access to the vCenter (vCSA) server with external PSC without the vGate Client is not supported.

Support of VMware Auto Deploy

This function is available only in vGate Enterprise and Enterprise Plus.

VMware vSphere includes the "Auto Deploy" function designated for the ESXi server automatic deployment. VibModifcator.exe utility is a part of the vGate software, it allows to create an archive of vGate Agent installation files and add it to the ESXi server image used by VMware Auto Deploy.

Control of the Cloud Director operations

The vGate software supports the control of VMware Cloud Director operations. Within this function the following actions for Cloud Director organization management are available in the vGate management console:

- view organization properties;
- assign labels;
- add organization to the group and remove organization from it;
- view related events;
- update the list of organizations;

Control of Cloud Director server operations is available only in vGate Enterprise and Enterprise Plus.

Control of the VMware vSAN operations

The vGate software supports control of VMware vSAN operations. vSAN administrator role has been added in the vGate web console for providing access to vSAN.

Control of VMware vSAN server operations is available only in vGate Enterprise and Enterprise Plus.

Network firewall

This function is available only in vGate Enterprise Plus.

Network firewalling allows to filter the network traffic in the virtual machine network, including virtual machines located on different virtualization servers. vGate network administrator role has been added in the vGate web console for providing access to the firewall.

Network traffic filtering is performed according to the rules configured in the vGate web console. Filtering rules may be created for the certain virtual machine or for several grouped virtual machines.

Stateful packet inspection (SPI) and Deep packet inspection (DPI) are also available within this function.

Reviewing ESXi servers for compliance with security policies

This function is available only in vGate Enterprise Plus.

vGate allows to review protected ESXi servers for compliance with security policies. Scanning may be run in the vGate web console.

Integrity control of ESXi server configuration files

vGate allows to perform integrity control for protected ESXi servers with assigned "Integrity control of ESXi server configuration files" policy. The policy is aimed to prohibit operations with the specified ESXi server configuration files.

Integrity control of ESXi server configuration files is available only in vGate Enterprise Plus.

Integrity control of container images

vGate allows to perform the integrity control of container images stored in the embedded Harbor Registry. The integrity control is performed only for container images to which the "Integrity control of container images" policy is assigned. The policy is aimed to prohibit an unauthorized running of containers images, the integrity of which has been compromised. Integrity control of images is performed by monitoring the invariability of their checksums.

This component is available in vGate Enterprise Plus only.

Chapter 4
vGate compatibility with other products

Support of VMware View

vGate supports operation with VMware View 5.1, VMware Horizon View 6.1, 6.2, 7.0, 7.1, 7.6, 7.8, 7.10. and 8.3. To ensure the View Connection Server access to the protected perimeter and virtual infrastructure administrator access to the View Connection Server, the primary setup should be performed (see the "Setting up the View Connection Server" section in the document [2]).

Support of the standard Distributed vSwitch and Distributed vSwitch Cisco Nexus 1000v

vGate supports operation with the standard distributed virtual switch Distributed vSwitch (DVX), and with the Distributed vSwitch Cisco Nexus 1000v by VMware. Network switch should be installed before the vGate software.

This function is available only for VMware vSphere.

Solutions for protection of virtual machines

vGate ensures protection of the virtual infrastructure administration environment and integrity control of files of virtual machines that are executed on protected servers. To additionally protect virtual machines, we recommend to use the supportive information security tools (for example, Secret Net Studio). vGate is compatible with information security tool Secret Net Studio version 8.9.

Documentation

1.	vGate R2. Administrator guide. Principles of operation
2.	vGate R2. Administrator guide. Installation, configuration and operation
3.	vGate R2. Administrator guide. Quick start
4.	vGate R2. User guide. Work in a protected environment