Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition

Deployment Guide

APPLICATION VERSION: 8.0 SERVICE PACK 2

Dear User,

Thank you for choosing our product. We hope that this documentation will help you in your work and answer your questions about this software product.

This document may be amended without prior notice. For the latest version, please refer to Kaspersky Lab's website at http://www.kaspersky.com/docs.

Kaspersky Lab assumes no liability for the content, quality, relevance or accuracy of any materials used in this document the rights to which are held by third parties, or for potential damages associated with the usage of such documents.

Revision date: 2/25/2015

http://www.kaspersky.com
http://support.kaspersky.com

TABLE OF CONTENTS

SOURCES OF INFORMATION ABOUT KASPERSKY ANTI-VIRUS

This section lists the sources of information about the application. You can select the most suitable information source, depending on the level of importance and urgency of the issue.

IN THIS SECTION

SOURCES FOR INDEPENDENT RETRIEVAL OF INFORMATION

You can use the following sources to find information about Kaspersky Anti-Virus:

- Kaspersky Anti-Virus page on the Kaspersky Lab website
- Kaspersky Anti-Virus page on the Technical Support website (Knowledge Base)
- Online help
- Manuals

If you cannot find a solution for your issue on your own, we recommend contacting Kaspersky Lab Technical Support.

An Internet connection is required to use online information sources.

Kaspersky Anti-Virus page on the Kaspersky Lab website

On the Kaspersky Anti-Virus page (http://www.kaspersky.com/business-security/windows-server-antivirus-enterprise-edition), you can view general information about the application, its functions and features.

The Kaspersky Anti-Virus page contains a link to eStore. There you can purchase the application or renew your license.

Kaspersky Anti-Virus page in the Knowledge Base

Knowledge Base is a section on the Technical Support website.

The Kaspersky Anti-Virus page in the Knowledge Base (http://support.kaspersky.com/wsee8) features articles that provide useful information, recommendations, and answers to frequently asked questions about how to purchase, install, and use the application.

Knowledge Base articles can answer questions relating to not only Kaspersky Anti-Virus but also to other Kaspersky Lab applications. Knowledge Base articles can also include Technical Support news.

The deployment guide describes common ways to deploy Kaspersky Anti-Virus on a corporate network.

The installation guide describes how you can perform the following tasks:

- Prepare Kaspersky Anti-Virus for installation, install and activate the application
- Prepare Kaspersky Anti-Virus for operation
- Restore or remove Kaspersky Anti-Virus

The administrator's guide provides information about how to configure and use Kaspersky Anti-Virus.

In the Implementation Guide for Network Storage Protection you can find information about configuring and using Kaspersky Anti-Virus for network storage protection.

CONTACTING THE SALES DEPARTMENT

If you have any questions on how to purchase the application or renew your license, you can contact our Sales Department representatives in one of the following ways:

- By calling Kaspersky Lab's headquarters in Moscow (http://www.kaspersky.com/contacts)
- By sending an email to sales@kaspersky.com

The service is provided in Russian or English.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM

If your question does not require an immediate answer, you can discuss it with Kaspersky Lab experts and other users on our forum (http://forum.kaspersky.com).

On this forum you can view existing threads, leave your comments, and create new discussion threads.

CONTACTING THE TECHNICAL WRITING AND LOCALIZATION UNIT

If you have any questions about the application documentation, please contact our Technical Writing and Localization Team. You can do so by sending an email to docfeedback@kaspersky.com. In the subject line of your message, please indicate "Kaspersky Help Feedback: Kaspersky Anti-Virus 8.0 for Windows Server Enterprise Edition."

KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus protects servers running on Microsoft® Windows® operating systems and network storages against viruses and other computer security threats to which servers are exposed through file exchange. Kaspersky Anti-Virus is designed for use on local area networks of medium to large organizations. Kaspersky Anti-Virus users are corporate network administrators and specialists responsible for anti-virus protection of the corporate network.

Kaspersky Anti-Virus can be installed on servers in the following roles:

- Terminal servers
- Print servers
- Application servers
- Domain controllers
- Network storage servers
- File servers – these servers are more likely to get infected because they exchange files with user workstations.

Kaspersky Anti-Virus can be managed in the following ways:

- Via Kaspersky Anti-Virus Console installed on the same server with Kaspersky Anti-Virus or on a different computer
- Using commands in the command line
- Via Administration Console of Kaspersky Security Center.

The Kaspersky Security Center application can also be used for centralized administration of multiple servers running Kaspersky Anti-Virus.

It is possible to review Kaspersky Anti-Virus performance counters for the "System Monitor" application, as well as SNMP counters and traps.

Kaspersky Anti-Virus components and features

The application includes the following components:

- Real-time protection of files

  Kaspersky Anti-Virus scans objects when they are accessed. Kaspersky Anti-Virus scans the following objects:

  - files;
  - alternate file system threads (NTFS threads);
  - master boot record and boot sectors on the local hard drives and removable media.

- Script scanning

  Kaspersky Anti-Virus controls the execution of scripts created using Microsoft Windows Script Technologies (or Active Scripting), for example, VBScript or JScript®. Kaspersky Anti-Virus allows script execution only if this script has been found to be safe. Kaspersky Anti-Virus blocks the execution of a script that has been found to be dangerous. If Kaspersky Anti-Virus finds a script to be potentially dangerous, it performs the action you have specified: blocks or allows script execution.

- Network storage protection

  Kaspersky Anti-Virus installed on a server under a Microsoft Windows operating system protects network storage systems against viruses and other security threats that infiltrate the server through the exchange of files.

- On-demand scan

  Kaspersky Anti-Virus runs a single scan of the specified area for viruses and other computer security threats. Kaspersky Anti-Virus scans server files and RAM and also startup objects.

The following functions are implemented in the application:

- Updating databases and application software modules

  Kaspersky Anti-Virus downloads updates of application databases and modules from FTP or HTTP update servers of Kaspersky Lab, Kaspersky Security Center Administration Server, or other update sources.

- Quarantine

  Kaspersky Anti-Virus quarantines probably infected objects by moving such objects from their original location to the *Quarantine storage*. Objects are stored in the Quarantine storage in encrypted form for security considerations.

- Backup

  Kaspersky Anti-Virus stores encrypted copies of objects classified as *Infected* or *Probably infected* in *Backup* before disinfecting or deleting them.

- Administrator and user notifications

  You can configure the application to notify the administrator and users who access the protected server about events in Kaspersky Anti-Virus operation and the status of Anti-Virus protection on the server.

- Importing and exporting settings

  You can export Kaspersky Anti-Virus settings to an XML configuration file and import settings into Kaspersky Anti-Virus from the configuration file. All Kaspersky Anti-Virus settings or settings for individual Kaspersky Anti-Virus components can be saved in the configuration file.

HARDWARE AND SOFTWARE REQUIREMENTS

This section lists the hardware and software requirements of Kaspersky Anti-Virus.

IN THIS SECTION

REQUIREMENTS FOR THE SERVER ON WHICH KASPERSKY ANTI-VIRUS IS DEPLOYED

Before installing Kaspersky Anti-Virus, you must uninstall other anti-virus applications from the server.

Kaspersky Anti-Virus can be installed without prior removal of Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition or Kaspersky Anti-Virus 6.0 / 8.0 for Windows Servers.

Hardware requirements for the server

General requirements:

- x86-compatible uniprocessor or multiprocessor systems; x86-64-compatible uniprocessor or multiprocessor systems
- disk space requirements:
  - for installing all application components: 70 MB
  - for downloading and storing anti-virus databases of the application: 2 GB (recommended)
  - for storing objects in Quarantine and in Backup: 400 MB (recommended)
  - for storing logs: 1 GB (recommended).
  - for storing databases: 2 GB (recommended)

Minimum configuration:

- processor – 1 Intel® Core™ 1.4 GHz
- RAM: 1 GB
- drive subsystem – 4 GB of free space

Recommended configuration:

- CPU: 4 Intel Core 2.4 GHz
- RAM: 2 GB
- drive subsystem – 4 GB of free space

Software requirements for the server

You can install Kaspersky Anti-Virus on a server under a 32-bit or 64-bit Microsoft® Windows® operating system.

For installation and operation of Kaspersky Anti-Virus, Microsoft Windows Installer 3.1 must be installed on the server.

You can install Kaspersky Anti-Virus on a server under one of the following 32-bit Microsoft Windows operating systems:

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later.

You can install Kaspersky Anti-Virus on a server under one of the following 64-bit Microsoft Windows operating systems:

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V® Server 2008 R2 SP1 or later
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter.
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2

You can install Kaspersky Anti-Virus on the following terminal servers:

- Microsoft Terminal Services based on Windows 2003 Server;
- Microsoft Remote Desktop Services based on Windows 2008 Server
- Microsoft Remote Desktop Services based on Windows 2012 Server
- Microsoft Remote Desktop Services based on Windows 2012 Server R2
- Citrix Presentation Server™ 4.0, 4,5

- Citrix® XenApp® 4.5, 5.0, 6.0, 6.5
- Citrix XenDesktop® 7.0, 7.1, 7.5.

REQUIREMENTS FOR THE PROTECTED NETWORK STORAGE

Kaspersky Anti-Virus can be used to protect the following network storages:

- NetApp with one of the following operating systems:
  - Data ONTAP 7.x and Data ONTAP 8.x in 7-mode
  - Data ONTAP 8.2.1 or higher in cluster-mode
- EMC™ Celerra™ / VNX™ with the following software:
  - operating system EMC DART 6.0.36 or higher;
  - Celerra Anti-Virus Agent (CAVA) 4.5.2.3 or higher.
- EMC Isilon™ with the operating system OneFS™ 7.0 or later.
- Hitachi NAS on one of the following platforms:
  - HNAS 4100
  - HNAS 4080
  - HNAS 4060
  - HNAS 4040
  - HNAS 3090
  - HNAS 3080.
- IBM® NAS series IBM System Storage® N series.

REQUIREMENTS FOR THE COMPUTER ON WHICH KASPERSKY ANTI-VIRUS IS DEPLOYED

Hardware requirements for the computer

Recommended RAM amount: at least 128 MB.

Free disk space: 30 MB.

Software requirements for the computer

You can install Kaspersky Anti-Virus Console on a computer running a 32-bit or 64-bit Microsoft Windows operating system.

The computer should have Microsoft Windows Installer 3.1 in order to support installation and operation of Kaspersky Anti-Virus Console.

You can install Kaspersky Anti-Virus Console on a computer running one of the following 32-bit Microsoft Windows operating systems:

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Microsoft Windows XP Professional with Service Pack 2 or later;
- Microsoft Windows Vista® Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8;
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional.

You can install Kaspersky Anti-Virus Console on a computer running one of the following 64-bit Microsoft Windows operating systems:

- Windows Server 2003 Standard / Enterprise SP2
- Windows Server 2003 R2 Standard / Enterprise SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V Server 2008 R2 SP1 or later
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter.
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2
- Microsoft Windows XP Professional Edition SP2 or later
- Microsoft Windows Vista Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8;
- Microsoft Windows 8 Enterprise / Professional
- Microsoft Windows 8.1
- Microsoft Windows 8.1 Enterprise / Professional.

PROTECTING DIRECTLY ATTACHED STORAGES (DAS)

Kaspersky Anti-Virus protects data storage devices that directly attached to the server (see figure below).

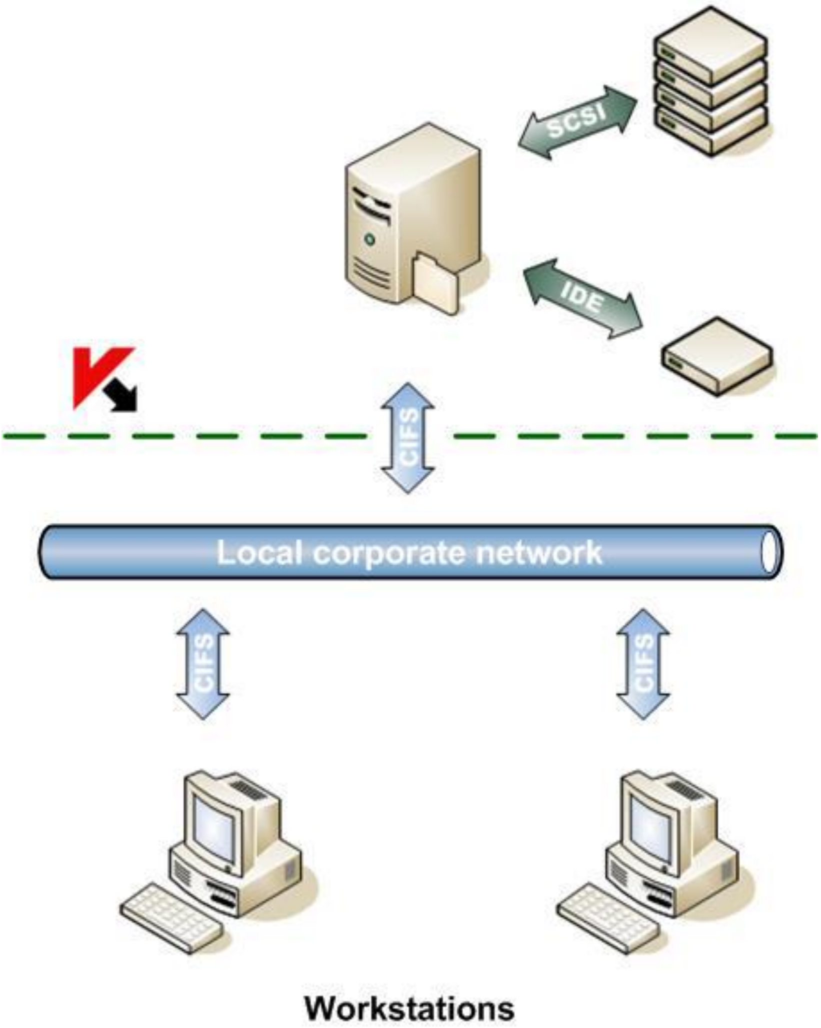

Figure 1: Directly Attached Storages protection scheme

Kaspersky Anti-Virus controls file operations on files in DAS. Kaspersky Anti-Virus recognizes DAS as local file resources on the server.

PROTECTIN CLUSTERS

Kaspersky Anti-Virus supports installation on server clusters running in **Active** / **Active** and **Active** / **Passive** modes (see figure below).

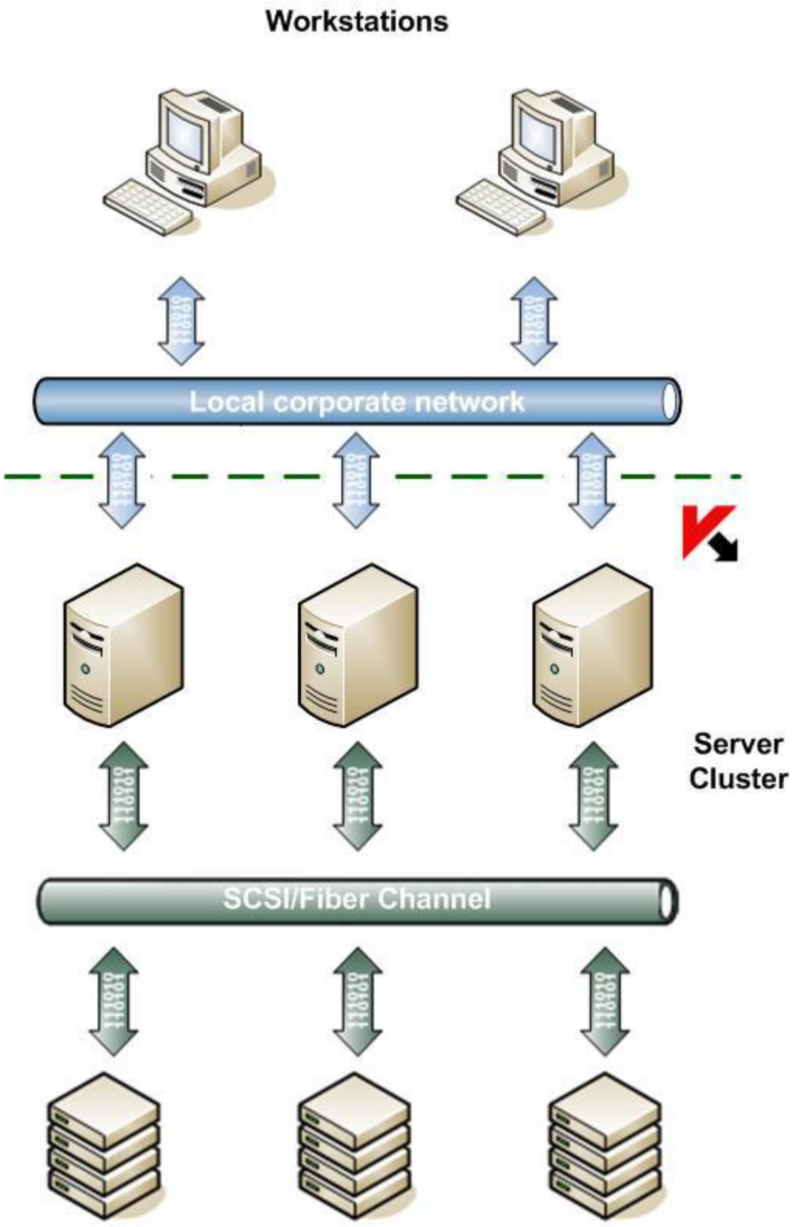

Figure 2: Server cluster protection scheme

Kaspersky Anti-Virus ensures correct server operation during migration of cluster resources (**failover** / **failback**).

Total cluster protection is achieved if Kaspersky Anti-Virus is installed on every node. Kaspersky Anti-Virus protects local drives in the server file system and shared cluster drives currently owned by the protected node. File resources owned by an unprotected node in the cluster are not protected.

You can find more detailed information in the *Installation Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*.

PROTECTING TERMINAL SERVERS

Kaspersky Anti-Virus protects terminal servers (see figure below).

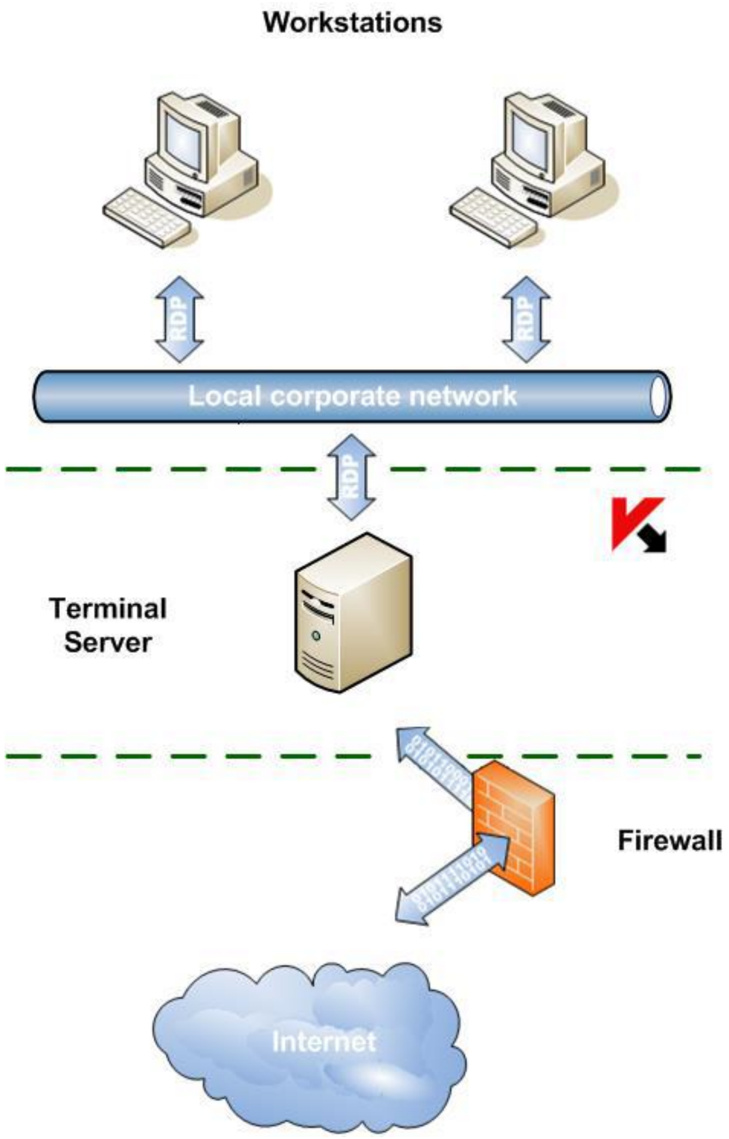

Figure 3: Terminal server protection scheme

Kaspersky Anti-Virus:

- protects terminal users working in desktop publishing and application publishing mode
- notifies terminal users by means of terminal servers
- audits actions on files and scripts by terminal users

You can find more detailed information in the *Administrator's Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition*.

NETWORK STORAGE PROTECTION

Kaspersky Anti-Virus installed on a server under a Microsoft Windows operating system protects network storage systems against viruses and other security threats that infiltrate the server through the exchange of files.

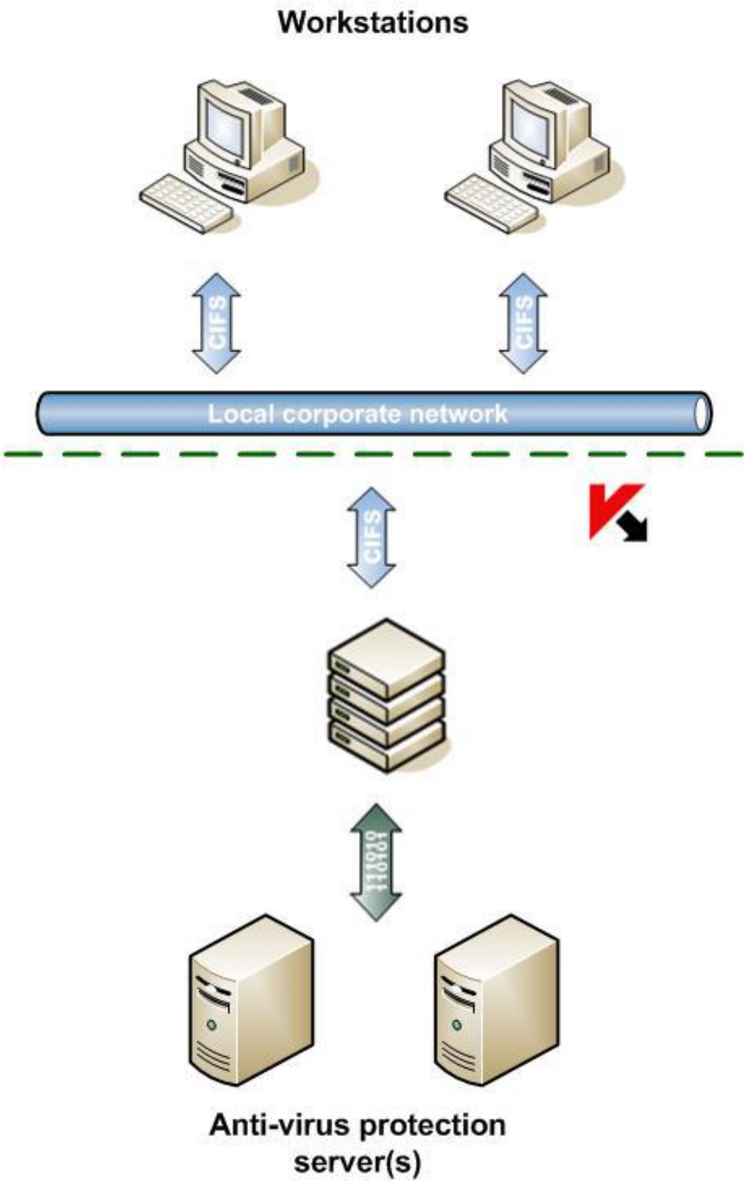

Figure 4: Network storage protection scheme

Kaspersky Anti-Virus scans files located in network share folders in the network storage system when an attempt is made to read or modify the files from a workstation. The network storage system allows reading or modifying a file if Kaspersky Anti-Virus has identified that file as safe. If Kaspersky Anti-Virus has identified a file as infected or probably infected, the network storage system blocks that file from being read or modified. Kaspersky Anti-Virus lets you configure actions that the application takes on infected and probably infected files. By default Kaspersky Anti-Virus disinfects infected files, and if disinfection is not possible it deletes them (if the action is available in the network storage system); probably infected files are placed in quarantine. Before disinfecting or deleting a file, Kaspersky Anti-Virus places a copy of the file in backup storage..

You can find more detailed information in the *Implementation Guide for Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition for Network Storage Protection*.

CONTACTING TECHNICAL SUPPORT

This section describes the ways to receive technical support and the conditions on which it is available.

IN THIS SECTION

ABOUT TECHNICAL SUPPORT

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application, we recommend that you contact Kaspersky Lab Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Technical support is available only to users who have purchased a commercial license for the application. Technical support is not available to users who have a trial license.

Before contacting Technical Support, we recommend that you read through the support rules (http://support.kaspersky.com/support/rules).

You can contact Technical Support in one of the following ways:

- By calling Kaspersky Lab Technical Support.
- By sending a request to Technical Support through the Kaspersky CompanyAccount web service.

TECHNICAL SUPPORT VIA KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) is a web service for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount web service is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. You can use Kaspersky CompanyAccount to track the status of your online requests and store a history of them as well.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account gives you centralized management of online requests from these employees to Kaspersky Lab, as well as control over the rights of these employees in your Kaspersky CompanyAccount.

The Kaspersky CompanyAccount web service is available in the following languages:

- English
- Spanish
- Italian

- German
- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website (http://support.kaspersky.com/faq/companyaccount_help).

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call Kaspersky Lab Technical Support representatives (http://support.kaspersky.com/support/contacts).

Before contacting Technical Support, you are advised to read the technical support rules (http://support.kaspersky.ru/support/rules). These rules contain information about the working hours of Kaspersky Lab Technical Support and about the information that you must provide so that Kaspersky Lab Technical Support specialists can help you.

USING TRACE FILES AND AVZ SCRIPTS

After you report a problem to Kaspersky Lab Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Anti-Virus and to send it to Kaspersky Lab Technical Support. Kaspersky Lab Technical Support specialists may also ask you to create a *trace file*. The trace file allows following the process of how application commands are performed, step by step, in order to determine the stage of application operation at which an error occurs.

After analyzing the data you send, Kaspersky Lab Technical Support specialists can create an AVZ script and send it to you. With AVZ scripts, it is possible to analyze active processes for threats, scan the computer for threats, disinfect or delete infected files, and create system scan reports.

GLOSSARY

A

Administration server

A component of Kaspersky Security Center that performs centralized storage of information about Kaspersky Lab applications installed on the corporate network and ways of managing them.

Anti-virus databases

Databases that contain information about computer security threats known to Kaspersky Lab as of the anti-virus database release date. Anti-virus database signatures help to detect malicious code in scanned objects. Anti-virus databases are created by Kaspersky Lab specialists and updated hourly.

Application settings

Settings of the application that are common for tasks of all the types and responsible for the operation of the application itself, for example: application performance settings, settings of reports, Backup settings.

Archive

A file that contains inside itself one or several other files, which, in their turn, may also be archives.

B

Backup

A dedicated storage area intended for storing backup copies of files that have been created before their first disinfection or deletion.

D

Disinfection of objects

A method of processing infected objects that results in a complete or partial recovery of data. Not every infected object can be disinfected.

F

False alarm

A situation when a non-infected object is identified by a Kaspersky Lab application as infected because its code is similar to that of a virus.

H

Heuristic Analyzer

A module of Kaspersky Anti-Virus that performs heuristic analysis.

Heuristic analysis

A technology intended for detection of threats that cannot be detected using the current version of the databases of Kaspersky Lab applications. It allows finding files that may contain some unknown virus or a new modification of a known virus.

The Probably-infected status is assigned to files in which the heuristic analysis has detected malicious code.

I

INFECTED FILE

A file that contains malicious code (i.e., when scanning the file, code of a known application that poses a threat has been detected). Kaspersky Lab specialists recommend that you abstain from handling such files since this may lead to an infection of your computer.

O

OLE OBJECT

A file that has been merged or integrated into another one. Kaspersky Lab applications allow scanning OLE objects for viruses. For example, if you embed a Microsoft Office Excel® spreadsheet into a Microsoft Office Word document, the former will be scanned as OLE object.

P

POSSIBLY INFECTED FILE

A file that contains either modified code of a known virus, or code that is similar to one but still unknown to Kaspersky Lab. Possibly files can be detected by means of the heuristic analyzer.

POTENTIALLY INFECTABLE FILE

A file with a specific structure or format that may be used by criminals to convert this file into a container for storing and spreading malicious code. As a rule, they include executable files, for example, those with com, exe, dll, and other similar extensions. The risk of malicious code penetration into such files is rather high.

Q

QUARANTINE

The folder to which Kaspersky Anti-Virus moves possibly infected objects that have been detected. Files are stored in Quarantine in encrypted form in order to avoid any impact on the computer.

S

SIGNATURE ANALYSIS

The technology of threat detection, which uses databases of Kaspersky Anti-Virus that contain descriptions of known threats and methods of neutralizing them. Protection with signature analysis ensures the minimum admissible security level. According to recommendations of Kaspersky Lab specialists, this analysis method is always enabled.

STARTUP OBJECTS

A set of applications that are required for start and proper operation of the operating system and software installed on the computer. Every time the operating system boots, it runs those objects. There are viruses aimed at infecting such objects, which may result, for example, in blocked booting of the operating system.

T

TASK

Functions performed by a Kaspersky Lab application are implemented as tasks, for example: Real-time protection of files, Full Scan, Update application databases.

TASK SETTINGS

Settings of the application that are specific for each task type.

U

UPDATE

A procedure that consists in replacing / adding new files (databases or application modules) retrieved from Kaspersky Lab update servers.

V

VULNERABILITY

A flaw in the operating system or in an application that may be exploited by malicious programs in order to intrude into the operating system or application and corrupt its integrity. A large number of vulnerabilities in the operating system makes its operation unreliable, because viruses that have intruded into the operating system may provoke failures in the system's operation or errors in the operation of installed applications.

KASPERSKY LAB

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world’s top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today Kaspersky Lab is an international group of companies headquartered in Moscow and comprising five regional divisions, which manage the company's operations in Russia, Western and Eastern Europe, the Middle East, Africa, Northern and Southern America, Japan, China, and other countries of the Asia-Pacific region. The company employs more than 2,000 skilled professionals.

PRODUCTS. Kaspersky Lab products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and tablet computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab’s centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab products are certified by major testing laboratories, compatible with the applications of most software vendors, and optimized for work on most hardware platforms.

Kaspersky Lab virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly*; and the *Anti-Spam database every five minutes*.

TECHNOLOGIES. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Openwave Messaging (Ireland), D-Link (Taiwan), M86 Security (USA), GFI Software (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), Netasq+Arkoon (France), NETGEAR (USA), Parallels (USA), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company’s innovative technologies are patented.

ACHIEVEMENTS. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a reputed Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company’s products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab website:	http://www.kaspersky.com
Virus Encyclopedia	http://www.securelist.com/en/
Virus Lab:	newvirus@kaspersky.com (only for sending probably infected files in archives)
Kaspersky Lab web forum:	http://www.kaspersky.com

INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in a file named legal_notices.txt and stored in the application installation folder.

TRADEMARK NOTICES

Registered trademarks and service marks are the property of their respective owners.

Citrix, Citrix Presentation Server, XenApp, and XenDesktop are registered trademarks of Citrix Systems, Inc. and/or subsidiaries in the United States and/or elsewhere.

Core and Intel are trademarks of Intel Corporation registered in the United States and/or elsewhere.

Celerra, EMC, Isilon, OneFS, and VNX are either registered trademarks or trademarks of EMC Corporation in the United States and/or elsewhere.

IBM and System Storage are trademarks of International Business Machines Corporation registered all over the world.

Microsoft, Windows, Windows Server, and Windows Vista are trademarks of Microsoft Corporation registered in the United States and/or elsewhere.

Data ONTAP and NetApp are either registered trademarks or trademarks of NetApp, Inc. in the United States and/or elsewhere.

INDEX