

KL 005.11:

Protecting Windows Servers and Embedded Systems

Featured products

- Kaspersky Security for Windows Server
- Kaspersky Embedded Systems Security

Course objective

This course educates engineers how to deploy, configure and maintain Kaspersky Security 11 for Windows Server at midsize or large enterprises.

The training describes the actions to be taken by the administrator step by step to successfully deploy and configure the product in a corporate network. Special attention is paid to configuring Kaspersky Security 11 for Windows Server to solve specific tasks, for example, protection against crypto-ransomware, or deploying Default Deny policy, or storage protection.

Labs demonstrate today's methods of protecting an information system. The administrator manages the whole infrastructure from the workstation through the Kaspersky Security Center Administration Console and Kaspersky Security Console. Almost every section of the theoretical part of the course is accompanied by a hands-on lab where you can put your knowledge into practice and get a real feel for how the product would perform.

Duration

2–3 days.

Requirements for the students

Basic knowledge of Kaspersky Security Center and Kaspersky Endpoint Security. Understanding of contemporary threats, typical phases of the cyber kill chain and cyber security incident investigation procedures.

Contents

1. General

- 1.1. Main functions of Kaspersky Security for Windows Server
- 1.2. Kaspersky Security for Windows Server system requirements
- 1.3. Protection components of Kaspersky Security for Windows Server
- 1.4. Management and monitoring components of Kaspersky Security for Windows Server
- 1.5. Licensing
- 1.6. Main functions of Kaspersky Embedded System Security
- 1.7. System requirements of Kaspersky Embedded Systems Security
- 1.8. Protection components of Kaspersky Embedded Systems Security
- 1.9. Management and monitoring components of Kaspersky Embedded Systems Security
- 1.10. Kaspersky Embedded Systems Security licensing
- 1.11. Kaspersky Embedded Systems Security installation options

2. Deployment

- 2.1. Deployment order
- 2.2. Quick Start Wizard
- 2.3. List of installation packages
- 2.4. Adjust the KSWs installation package settings (optional)
- 2.5. Create a dedicated group for KSWs (optional)

Lab 1. Prepare the Administration Server

- 2.6. How to install Kaspersky Security for Windows Server
- 2.7. Installation results
- 2.8. Activating Kaspersky Security for Windows Server

Lab 2. Install Kaspersky Security for Windows Server and Kaspersky Embedded Systems Security

- 2.9. Installing Kaspersky Security Console

Lab 3. Install the Kaspersky Security Console

3. Configuring group tasks

- 3.1. Database Update task
- 3.2. Application Module Update task
- 3.3. On-demand scan tasks

Lab 4. Configure updates and on-demand scanning

4. File system protection

Lab 5. Configure real-time protection

Lab 6. Test protection of Windows Subsystem for Linux

- 4.1. Exploit Prevention

Lab 7. Test protection against exploits

- 4.2. Anti-Cryptor
- 4.3. How to configure Anti-Cryptor
- 4.4. How to configure the blocking period for untrusted devices

Lab 8. Configure protection for shared folders

Lab 9. Configure the Anti-Cryptor component

5. Network Threat Protection

- 5.1. How Kaspersky Security for Windows Server protects from network attacks
- 5.2. How to configure Network Threat Protection

Lab 10. Configure Network Threat Protection

6. Protection for Remote Desktop Services

- 6.1. Threat model for Remote Desktop Services sessions
- 6.2. Traffic Security: Driver Interceptor
- 6.3. Components of protection for Remote Desktop Services sessions
- 6.4. Traffic Security: Redirector
- 6.5. Traffic Security: External Proxy

Lab 11. Configure Traffic Security in Driver Interceptor mode

Lab 12. Configure Traffic Security to scan mail traffic

Lab 13. Configure Traffic Security to the External Proxy mode

7. Server control components

- 7.1. Applications Launch Control

Lab 14. Enable Applications Launch Control in Test Mode

Lab 15. Switch Application Startup Control into active mode

Lab 16. Create allow rules for installation packages and updates

- 7.2. Device Control

8. System inspection

- 8.1. File Integrity Monitor
- 8.2. Log Inspection

Lab 17. Configure the System Inspection components

9. Protection for storages

- 9.1. Storage protection capabilities
- 9.2. Real-Time File Protection for storages

Lab 18. Protect a NetApp Clustered Data ONTAP storage

- 9.3. Anti-Cryptor for NetApp

Lab 19. Configure Anti-Cryptor for NetApp

10. Additional settings

- 10.1. Protection for shared cluster resources
- 10.2. Firewall Management
- 10.3. SIEM integration
- 10.4. Managing applications
- 10.5. Collecting diagnostic information
- 10.6. Monitoring the protection status (health check)