KL 302.11: Kaspersky Security Center. Scaling

The course instructs how to design, deploy, and maintain protection systems based on Kaspersky products and centrally manage them via Kaspersky Security Center in distributed and large Windows networks (from 1,000 to 100,000 endpoints).

The theoretical part of the course and hands-on labs provide students with knowledge and skills needed to:

- Design and implement a security management system in a large and/or geographically distributed network, in particular, using a hierarchy of Administration Servers
- Design and organize an optimal architecture for distributing updates throughout a large and/or geographically distributed network, for example, via distribution points
- Configure Kaspersky Security Center to manage devices outside the organization's perimeter with or without connection gateways

Applications covered in the course

- Kaspersky Security Center 11
- Kaspersky Endpoint Security for Windows 11.1
- Kaspersky Security for Windows Server 10.1

Audience

The course is aimed at Microsoft Windows system administrators, security experts and administrators, technical support and presale engineers.

Duration

3 days.

Modules 1, 2, and 3 are required. Module 4 is optional. You can skip it depending on the audience and available time.

Requirements for the students

Complete course KL 002 'Kaspersky Endpoint Security and Management' to know how Kaspersky Security Center works.

Basic understanding of networking technologies: TCP/IP, DNS, email, web. Know how to configure Windows servers and workstations. Basic knowledge of information security principles.

Outline

Module 1. Managing multiple KSC servers

Chapter 1. When to use multiple Kaspersky Security Center servers
Chapter 2. Introduction to Kaspersky Security Center server hierarchy
- Lab 1. How to connect a slave Administration Server of a remote office

Chapter 3. Managing Kaspersky Security Center servers in a hierarchy
- Lab 2. How to collect information from a hierarchy
- Lab 3. How to configure management in a hierarchy
- Lab 4. How to configure updates in a hierarchy
- Lab 5. How to change the Administration Server

Module 2. Managing updates and distribution points

Chapter 1. Update management strategies
Chapter 2. Distribution points
Chapter 3. Typical configurations
- Lab 1. Configure updates from the local source depending on the network location

Module 3. Managing computers located outside the network

Chapter 1. Why use a connection gateway
Chapter 2. How to install a connection gateway
- Lab 1. Install a connection gateway in the DMZ

Chapter 3. How to set up an unconditional connection via a connection gateway
- Lab 2. Configure an unconditional connection via a connection gateway in the DMZ

Chapter 4. How to set up a conditional connection via a connection gateway
- Lab 3. Configure a conditional connection via the connection gateway in the DMZ
- Lab 4. Configure updating from the local Administration Server

Module 4. (Optional) KSC installation on a failover cluster

- Lab 1. Install Kaspersky Security Center on a failover cluster
- Lab 2. Install Kaspersky Security for Windows Server on failover cluster under high load