kontron

Knowledge Management Centre – KMC

Information Security
2023 Knowledge Catalogue for Customers

Kontron, July 2023

Author:	Jože Kancilija
Agreed by:	Jože Kancilija
Approved by:	Aleksander Mali
Authorised by:	Jože Kancilija
Type of document:	Training documentation
Issuing date:	01 July 2023
Confidentiality level:	Internal 3
Official code:	/

If a copy of the document is used, please check its compliance with the latest document release.

Document issued by

kontron

Kontron, d. o. o.

Ljubljanska cesta 24a
4000 Kranj, Slovenia

T +386 4 207 20 00
F +386 4 207 27 12

info@kontron.si
www.kontron-slovenia.com

kontron

Table of Contents

kontron

1 Training center introduction

The emergence of new technologies that replace, complement and upgrade traditional telecommunications networks and facilitate the introduction of new services often make telecommunications providers face difficult decisions: which of the new technologies to choose; when and how to introduce it into the network; and what services to offer end users.

The mission of the S&T Iskratel Training Center is to provide professional training for S&T Iskratel customers, business partners and everyone connected via modern telecommunications.

Our vision of professional training is to provide training programs about all types of S&T Iskratel products, solutions and telecommunication technologies, which provide the participants with a clear and complete review of knowledge they need in their business environment and workplaces.

With our help participants in the training process will be able to attain their goals (successful operation of our systems and new products) in an easier, faster and more efficient way than anywhere else.

The classrooms are equipped with the most advanced terminal equipment and connections to the test bed. We organize our trainings, by previous agreement, also at our customer's premises (if the customer is able to provide the necessary equipment).

2 Check Point – Training Courses

2.1 (SSB8250AA) – Check Point Endpoint specialist (CCES) R81

Code for order: SSB8250AA

Training duration: 2 days

Description

The Check Point Endpoint Specialist (CCES) course covers the field of endpoint protection. In the course, candidates learn how to deploy endpoints in an enterprise network environment and gain a comprehensive understanding of Check Point endpoints.

Possible audience:

♦ Technical professionals who support, install deploy or administer Check Point products.

Competences:

♦ Learn basic concepts and develop skills necessary to administer Harmony Endpoint security solutions.

Prerequisites

♦ Working knowledge of Windows, UNIX, networking technology, the Internet and TCP/IP security solutions.
♦ Check Point recommends that students who wish to expand their knowledge participate in the CCSA and CCSE courses.

Contents

♦ Introduction to Harmony Endpoint
♦ Harmony Endpoint Security Management
♦ Deploying Harmony Endpoint Security
♦ Additional Endpoint Server Configurations
♦ Data Security Protection
♦ Advanced Threat Prevention
♦ Troubleshooting
♦ Practical examples:
  • Activate the Harmony Endpoint manager in the Cloud.
  • Configure Active Directory
  • Connect Active Directory to the Cloud management server.
  • Install Initial Agent on the Domain Controller.
  • Demonstrate how to deploy the Harmony Endpoint Agent on a client.
  • Configure the policy operation mode.
  • Create exception rules for specific removable media devices
  • Deploy and configure Anti-Bot and URL Filtering on an Endpoint client
  • Configure and deploy Full Disk Encryption on a client.
  • Test Anti-Bot behavioral engine.
  • Configure and deploy Media Encryption.
  • Block access to certain websites for specific user groups.
  • Configure and deploy Port Protection on an Endpoint client.
  • Perform threat emulation and extraction of malicious content.
  • Learn how to extract malicious content from a document.

Kontron

2.2   (SSB8251AA) – Check Point Security administrator (CCSA) R81.10

Code for order: SSB8251AA

Training duration: 3 days

Description

In this Check Point Certified Security Administrator (CCSA) course, you will learn how to deploy, configure and administer Checkpoint Security Gateways and Security Management Servers.

Possible audience:

♦   Technical professionals who support, install deploy or administer Check Point products.

Competences:

♦   Learn basic concepts and develop skills necessary to administer IT security fundamental tasks.

Prerequisites

♦   Working knowledge of Windows, UNIX, networking technology, the Internet and TCP/IP.

Contents

♦   Introduction to Check Point Technology
♦   Introduction to Check Point Deployment
♦   Check Point Management Operations
♦   Licensing
♦   Security Policy Management
♦   Policy Layers
♦   Application Control & URL Filtering
♦   Managing User Access
♦   Working with NAT
♦   Traffic Visibility
♦   Monitoring System States
♦   Threat Prevention
♦   Practical examples:
  • Configure the Security Management Server.
  • Use the WebUI to run the First Time Wizard.
  • Install the Smart Console.
  • Install the Alpha Gateway using the network detailed in the course topology.
  • Demonstrate how the Security Management Server and Gateway communicate.
  • Test SIC Status.
  • Create multiple administrators and apply different roles and permissions for simultaneous administration.
  • Validate existing licenses for products installed on the network.
  • Create and configure host, network and group objects.
  • Create a simplified Security Policy.
  • Demonstrate how to use Security Zones in policy.
  • Demonstrate how to share a layer between Security Polices.
  • Configure Network Address Translation for server and network objects.
  • Enable Identity Awareness.
  • Deploy user access roles for more granular control of the security Policy.

- Generate network Traffic and use traffic visibility tools to monitor the data.
- Use SmartConsole and SmartView Monitor to view status, alerts, and block suspicious traffic.

kontron

2.3 (SSB8252AA) – Check Point Security Expert (CCSE) R81.10

Code for order: SSB8252AA

Training duration: 3 days

Description

In this Check Point Certified Security Expert (CCSE) course, you will learn how to deploy, configure and administer Checkpoint Security Gateways and Security Management Servers. In this course we include a lot of practical examples.

Possible audience:
◆ Technical professionals who perform advanced deployment configurations of Check Point products.

Competences:
◆ Validate and enhance your skills and optimally manage Check Point advanced security management system.

Prerequisites
◆ CCSA training and certification with a working knowledge of Windows and/or UNIX, networking technology, the Internet and TCP/IP.

Contents
◆ Management Upgrade and Migration
◆ Management High Availability
◆ Security Gateway Upgrade
◆ Advanced Check Point Maintenance
◆ Security Gateway Operations
◆ Policy Installation
◆ Gaia and Management APIs
◆ Acceleration
◆ Site-to-Site VPN
◆ Remote Access VPN
◆ Mobile Access VPN
◆ Clustering
◆ Advanced Logs and Monitoring
◆ Practical examples:
  • Prepare for a Security Management Server Upgrade
  • Upgrade the Security Management Server
  • Deploy a Secondary Security Management Server
  • Configure a Distributed Log Server
  • Upgrade a Security Gateway from SmartConsole
  • Work with the Command Line
  • Use Scripts and SmartTasks
  • Configure Dynamic Objects
  • Monitor Traffic
  • Verify Policy Installation and Status
  • Work with Gaia and Management APIs
  • Work with Acceleration Features
  • Configure a Locally Managed Site to Site VPN
  • Configure a Site to Site VPN with an Interoperable Device

- Configure Remote Access VPN
- Configure Mobile Access VPN
- Configure a High Availability Cluster
- Work with ClusterXL
- Configure Policy Compliance
- Deploy SmartEvent

────────── (END OF DOCUMENT) ──────────

kontron