

Symantec Endpoint Protection 11.0 MR4: Manage and Administer

COURSE DESCRIPTION

The *Symantec Endpoint Protection 11.0 MR4: Manage and Administer* course is designed for the network, IT security, and systems administration professional tasked with architecting, implementing, and monitoring a client firewall and intrusion prevention system (IPS). This class also covers how to monitor Symantec Endpoint Protection and implement disaster recovery procedures.

In addition, students learn how to configure application and device control, add additional protection, perform server and database management, and expand the management environment.

Delivery Method

Web-based training (WBT)

Duration

Four hours

Course Objectives

By the completion of this course, you will be able to:

- Monitor and maintain the Symantec Endpoint Protection environment.
- Configure firewall and intrusion prevention policies.
- Customize network threat protection.
- Manage the Intrusion Prevention System.
- Add additional protection components.
- Perform server and database management.

Who Should Attend

This course is for network managers, resellers, systems administrators, client security administrators, systems professionals, and consultants who are charged with the installation, configuration, and day-to-day management of Symantec Endpoint Protection in a variety of network environments, and who are responsible for troubleshooting and tuning the performance of this product in the enterprise environment.

Prerequisites

You must have working knowledge of advanced computer terminology, including TCP/IP networking terms and Internet terms, and an administrator-level knowledge of Microsoft Windows 2000/XP/2003 operating systems.

COURSE OUTLINE

Introduction

Course overview

Introduction to Network Threat Protection and Application and Device Control

- Network threat protection basics
- The firewall
- Intrusion prevention
- Application and device control

Configuring Firewall Policies

- Configuring firewall policy elements
- Configuring firewall rules
- Configuring Smart Traffic filtering
- Configuring traffic and stealth settings

Managing Intrusion Prevention System (IPS) Policies

- Configuring IPS
- Managing custom signatures

Configuring Application and Device Control Policies

- Introducing application and device control
- Creating application and device control policies
- Customizing application and device control policies

Customizing Network Threat Protection and Application and Device Control

- Managing locations
- Managing policy components
- Configuring application learning
- Configuring system lockdown

Configuring Additional Protection

- Configuring tamper protection
- Configuring centralized exceptions

Monitoring and Reporting

- Viewing summary data
- Viewing and managing logs
- Configuring and viewing notifications
- Creating and viewing reports

Performing Server and Database Management

- Managing Symantec Endpoint Protection servers
- Managing server security
- Communicating with other servers
- Managing administrators
- Managing the database
- Disaster recovery techniques

Installing Additional Management Components

- Installing additional LiveUpdate servers
- Installing and configuring the central quarantine
- Expanding the management environment