

Symantec Endpoint Protection 11.0 MR4: Maintain and Troubleshoot

COURSE DESCRIPTION

The *Symantec Endpoint Protection 11.0 MR4: Maintain and Troubleshoot* course is designed for the network, IT security, systems administration, and support professional tasked with maintaining and troubleshooting a Symantec Endpoint Protection environment. This class covers ongoing maintenance and troubleshooting from an administrative perspective, including advanced configuration, external reporting, external logging, and product maintenance.

Students also learn how to configure Symantec Endpoint Protection Manager (SEPM) replication, failover and load balancing, and secure communications for Symantec Endpoint Protection clients.

Delivery Method

Instructor-led

Duration

Two days

Course Objectives

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

- Describe Symantec Endpoint Protection component communications.
- Configure replication partners.
- Perform advanced database management.
- Recover from a SEPM or database failure.
- Configure the SEPM for failover and load balancing.
- Perform advanced client deployment and client management.
- Secure client communications.
- Use client debug tools to analyze client logs.

Who Should Attend

This course is for customers, support engineers, consultants, and partners who need to maintain and troubleshoot Symantec Endpoint Protection.

Prerequisites

You must have attended the *Symantec Endpoint Protection 11.0 MR4: Install, Configure, and Deploy* and *Symantec Endpoint Protection 11.0: Manage and Administer* courses. You must also have working knowledge of advanced computer terminology, including TCP/IP networking terms and Internet terms, and administrator-level knowledge of Microsoft Windows 2000/XP/2003 operating systems.

Hands-On

This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

COURSE OUTLINE

Introduction:

- Course overview
- The classroom lab environment

Component Communications

- Component communications
- Monitoring the heartbeat communications sequence

Configuring Replication

- About sites and replication
- How replication works
- Symantec Endpoint Protection replication scenarios
- Configuring replication
- Replication logging

Managing Databases

- SEPM or database failure and solution examples
- Backing up and restoring the database
- Gathering critical recovery data
- Recovering from a failure
- Database maintenance
- Migrating an embedded database to an MS SQL database

Configuring Failover and Load Balancing

- About failover and load balancing
- Describing management server lists
- Configuring management server lists
- Managed load balancing
- Monitoring and troubleshooting failover and load balancing

Performing Advanced Client Deployment

- Symantec Endpoint Protection 11.0.4 clients
- Find unmanaged computers
- The Microsoft installer

- Describing the Symantec Endpoint Protection integration component

Performing Advanced Client Management

- Update paths to the SEPM
- Configuring LiveUpdate settings for the SEPM
- Configuring LiveUpdate for clients
- Managing client updates
- Client update methods overview
- Group update provider
- Using the Rx4Defs Symantec support tool

Securing Client Communications

- Secure communications
- Shared key encryption
- Content signing
- HTTPS (SSL) transport

Analyzing Symantec Endpoint Protection Debug Logs

- The Symantec Endpoint Protection Support Tool
- Enabling the Symantec Endpoint Protection debug logs
- Using the Symantec Endpoint Protection client debug logs
- Using the Symantec Endpoint Protection installation debug logs
- Using the Symantec Endpoint Protection client installation debug logs
- Additional debug logs