Symantec Endpoint Protection 12.1: Maintain and Troubleshoot

COURSE DESCRIPTION

The *Symantec Endpoint Protection 12.1: Maintain and Troubleshoot* course is designed for the IT security management professional tasked with administering, monitoring, and troubleshooting Symantec Endpoint Protection 12.1.

Students learn how to troubleshoot and upgrade to Symantec Endpoint Protection 12.1; and how to monitor and troubleshoot the SEPM, client-to-SEPM communication, content distribution, client deployments, protection technologies, and network threat protection.

The class also covers how to follow Symantec best practices for troubleshooting and remediating a virus outbreak, performing advanced monitoring using IT Analytics, and providing solutions to Symantec Endpoint Protection 12.1 case studies.

Delivery Method

This course is available in the following delivery methods:

- Instructor-led training (ILT) – 3 days
- Web-based training (WBT) – 5 hours

Course Objectives

By the end of this course, you should be able to:

- Monitor client-to-SEPM communication.
- Maintain a Symantec Endpoint Protection environment.
- Upgrade the Symantec Endpoint Protection environment.
- Monitor and troubleshoot a Symantec Endpoint Protection environment.
- Monitor and troubleshoot SEPM and client content delivery.
- Monitor and troubleshoot protection technologies.
- Use best practices when creating Application and Device Control and Firewall rules.
- Use best practices when troubleshooting and remediating a virus outbreak.
- Use IT Analytics to generate comprehensive reports from Symantec Endpoint Protection.
- Provide solutions to Symantec Endpoint Protection 12.1 case studies.

Who Should Attend

This course is for network managers, resellers, system 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 attended the *Symantec Endpoint Protection 12.1: Administration* course or have equivalent experience.

COURSE OUTLINE

Introduction

- Course overview
- The classroom lab environment

Monitoring Client-to-SEPM Communication

- Introducing client-to-SEPM communication
- Examining client-to-SEPM communication
- Monitoring communication
- Using basic troubleshooting and other monitoring tools to troubleshoot communication

Maintaining the Symantec Endpoint Protection Environment

- Identifying critical SEP 12.1 services and processes
- Checking client status
- Using the Symantec Endpoint Protection Support Tool
- Managing administrators
- Reporting and notifications

Managing and Troubleshooting the SEPM

- Managing the SEPM
- Managing and troubleshooting the database
- Configuring SEP 12.1 clients to use Secure Socket Layer (SSL) communication

Monitoring and Troubleshooting Content Distribution

- Describing LiveUpdate sources: Review
- Examining a LiveUpdate session
- Downloading full or xdelta packages
- Determining LiveUpdate status and examining logs
- SEP 12.1 LiveUpdate client management
- Managing and monitoring group update providers (GUPs)

Maintaining and Troubleshooting Clients

- Client Deployment Wizard optimizations
- Upgrading Symantec Endpoint Protection clients
- Troubleshooting client installation failures
- Performing client management
- Enabling Symantec Endpoint Protection debug logs
- Troubleshooting SEP 12.1 Mac clients

Monitoring and Troubleshooting Protection Technologies

- Managing protection technologies
- Preventing false positives
- Identifying false positives
- Introducing Windows software trace preprocessor (WPP)

Monitoring and Troubleshooting Network Threat Protection

- Application control best practices
- Application and device control use cases
- Application and device control reports and logs
- Firewall use cases

Best Practices for Troubleshooting and Remediating a Virus Outbreak

- Best practices for troubleshooting and remediating viruses
- Managing rapid release definitions

Performing Advanced Monitoring using IT Analytics

- Introducing IT Analytics
- Hardware and software requirements
- Describing how IT Analytics works
- About installing IT Analytics

Providing Solutions to Symantec Endpoint Protection 12.1 Case Studies

- Evaluating a legacy environment for upgrade
- Redesigning a Symantec Endpoint Protection 11.*x* environment