Symantec Endpoint Protection 14: Maintain and Troubleshoot

Course Summary

Description

The Symantec Endpoint Protection 14.x: Maintain and Troubleshoot course is designed for the IT security management professional tasked with troubleshooting Symantec Endpoint Protection 14.x. Students learn how to troubleshoot installations, monitor and troubleshoot the SEPM, client-to-SEPM communication, content distribution, client deployments, and protection technologies. The class also covers how to follow Symantec best practices for remediating a virus outbreak, automating functionality with REST APIs, and integrating Symantec Endpoint Protection with 3rd party applications.

Objectives

By the end of this course, students will be able to:

- Monitor, maintain, and troubleshoot a Symantec Endpoint Protection environment.
- Upgrade the Symantec Endpoint Protection environment.
- Use best practices when troubleshooting and remediating a virus outbreak.
- Automate functionality with Rest APIs and integrate Symantec Endpoint Protection with 3rd party applications.

Topics

- Introduction
- Troubleshooting Techniques and Tools
- Troubleshooting the Console
- Installation and Migration Issues
- Client Communication Issues
- Content Distribution Issues
- Extending the SEP infrastructure
- Responding to a Security Incident
- Performance Issues

Audience

This course is for IT and system administration professionals who are charged with planning and installing a Symantec Endpoint Protection environment.

Prerequisites

You must have attended Symantec Endpoint Protection 14: Configure and Protect or have relevant experience maintaining a SEP environment, including basic troubleshooting.

Duration

Three days

ProTech "Charting the Course ...

protechtraining.com

... to Your Success!"

Symantec Endpoint Protection 14: Maintain and Troubleshoot

Course Outline

I. Introduction
- A. Course overview
- B. The classroom lab environment

II. Troubleshooting Techniques and Tools
- A. Use a systematic approach for problem solving.
- B. Describe Symantec and third-party troubleshooting tools and how they are used.
- C. Know which SEPM and SEP client logs to research when troubleshooting specific issues.
- D. Use the Symantec Knowledge Base and interact with Symantec Technical Support.

III. Troubleshooting the Console
- A. Describe the components that make up the Symantec Endpoint Protection Manager.
- B. Describe SEPM services and their roles.
- C. Troubleshoot problems related to the SEPM services that prevent you from logging onto the console.
- D. Describe the database configuration and connection methods.
- E. Configure email to enable an administrator to reset passwords and know where to check administrator permissions.

IV. Installation and Migration Issues
- A. Troubleshoot and resolve a failed Symantec Endpoint Protection Manager installation.
- B. Troubleshoot and resolve a failed Symantec Endpoint Protection for Windows client install.
- C. Troubleshoot and resolve a failed Symantec Endpoint Protection for Mac client install.
- D. Troubleshoot and resolve a failed Symantec Endpoint Protection for Linux client install.

V. Client Communication Issues
- A. Identify the interactions between the client and the SEPM.
- B. Identify heartbeat process.
- C. Locate and configure debug logs for client communication issues.
- D. Describe communications issues from the client perspective.
- E. Identify Linux and Mac communication issues.

VI. Content Distribution Issues
- A. Troubleshoot and resolve LiveUpdate issues on the SEPM and client.
- B. Troubleshoot and resolve issues between a client and management server.
- C. Troubleshoot and resolve issues from clients who retrieve updates from a Group Update Provider.

VII. Extending the SEP infrastructure
- A. Describe how data is transferred during replication and know which replication logs are affected.
- B. Automate functionality with Rest APIs.
- C. Integrate Symantec Endpoint Protection with third party applications.

VIII. Responding to a Security Incident
- A. Identify and examine useful SEPM reports for incident response.
- B. Learn the best approach for handling a virus outbreak.
- C. Identify and submit false positives to Symantec.

IX. Performance Issues
- A. Assess SEP performance using sizing and scalability recommendations.
- B. Optimize performance for the SEPM.
- C. Optimize performance for the SEP client.
- D. Utilities and other resources.
- E. Case studies