Symantec Endpoint Protection 14.x: Manage and Administer

Course Summary

Description

The Symantec Endpoint Protection 14.x: Manage and Administer course is designed for the network, IT security, and systems administration professional in a Security Operations position tasked with the day-to-day operation of the SEPM management console. The class covers configuring sever-client communication, domains, groups, and locations and Active Directory integration. You also learn how Symantec Endpoint Protection uses LiveUpdate servers and Group Update Providers to deliver content to clients. In addition, you learn how to respond to incidents using monitoring and reporting.

Objectives

After taking this course, students will be able to:

- Describe how the Symantec Endpoint Protection Manager (SEPM) communicates with clients and make appropriate changes as necessary.
- Design and create Symantec Endpoint Protection group structures to meet the needs of your organization.
- Respond to threats using SEPM monitoring and reporting.
- Analyze the content delivery system (LiveUpdate).
- Reduce bandwidth consumption using the best method to deliver content updates to clients.
- Configure Group Update Providers.
- Create location aware content updates.
- Use Rapid Release definitions to remediate a virus outbreak.

Topics

- Introduction
- Monitoring and Managing Endpoints
- Enforcing Content Updates on Endpoints using the Best Method

Audience

This course is for IT and system administration professionals who are charged with managing and monitoring Symantec Endpoint Protection endpoints.

Prerequisites

Before taking this course, 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 operating systems.

Duration

Two days

Symantec Endpoint Protection 14.x: Manage and Administer

Course Outline

I. Introduction
- A. Course environment
- B. Lab environment

II. Monitoring and Managing Endpoints
- A. Managing Console Access and Delegating Responsibility
  1. Creating administrator accounts
  2. Managing administrators and delegating responsibility
- B. Managing Client-to-SEPM Communication
  1. Analyzing client-to-SEPM communication
  2. Restoring communication between clients and SEPM
  3. Verifying clients are online with the SEPM
- C. Managing the Client Architecture and Active Directory Integration
  1. Describing the interaction between sites, domains, and groups
  2. Managing groups, locations, and policy inheritance
  3. Assigning policies to multiple locations
  4. Importing Active Directory Organizational Units
  5. Controlling access to client user interface settings
- D. Managing Clients and Responding to Threats
  1. Identifying and verifying the protection status for all computers
  2. Monitoring for health status and anomalies
  3. Responding to incidents
- E. Monitoring the Environment and Responding to Threats
  1. Monitoring critical log data
  2. Identifying new incidents
  3. Responding to incidents
  4. Proactively respond to incidents
- F. Creating Incident and Health Reports
  1. Reporting on your environment's security status
  2. Reporting on the health of your environment

III. Enforcing Content Updates on Endpoints using the Best Method
- A. Introducing Content Updates using LiveUpdate
  1. Describing the LiveUpdate ecosystem
  2. Configuring LiveUpdate sources
  3. Troubleshooting LiveUpdate
  4. Examining the need for an internal LiveUpdate Administration server
  5. Describe the high-level steps to configure an internal LiveUpdate server
- B. Analyzing the SEPM Content Delivery System
  1. Describing content updates
  2. Configuring LiveUpdate on the SEPM and clients
  3. Monitoring a LiveUpdate session
  4. Managing content on the SEPM
  5. Monitoring content distribution for clients
- C. Managing Group Update Providers
  1. Identifying the advantages of using group update providers
  2. Adding group update providers
  3. Adding multiple and explicit group update providers
  4. Identifying and monitoring group update providers
  5. Examining group update provider health and status
- D. Configuring Location Aware Content Updates
  1. Examining location awareness
  2. Configuring location aware content updates
  3. Monitoring location aware content updates
- E. Managing Certified and Rapid Release Definitions
  1. Managing Certified SEPM definitions from Symantec
  2. Security Response
  3. Managing Certified Windows client definitions from
  4. Symantec Security Response
  5. Managing Rapid Release definitions from Symantec
  6. Security Response
  7. Managing Certified and Rapid Release definitions from Symantec Security Response for Mac and Linux clients
  8. Using static definitions in scripts to download content