Symantec Endpoint Protection 12.1: Administration

(Symantec Endpoint Protection 12.1.4)

COURSE DESCRIPTION

The *Symantec Endpoint Protection 12.1: Administration* course is designed for the network, IT security, and systems administration professional tasked with architecting, implementing, and monitoring virus and spyware protection, zero-day protection, and network threat protection solutions. This class covers how to design, deploy, install, configure, manage, and monitor Symantec Endpoint Protection 12.1 (SEP 12.1) in a Windows and Mac environment.

Students learn how to create and implement the client firewall, intrusion prevention, application and device control, and behavioral protection policies that guard the enterprise from viruses and hackers. In addition, students learn how to perform server and database management, expand the management environment and use virtualization features for virtual clients.

Delivery Method
Virtual Academy (VA)

Duration
Five days

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

- Describe Symantec Endpoint Protection products, components, dependencies, and system hierarchy.
- Install and configure Symantec Endpoint Protection management and client components.
- Deploy Symantec Endpoint Protection Windows and Mac clients.
- Manage the client user interface.
- Manage content updates for Windows and Mac clients.
- Design a Symantec Endpoint Protection environment.
- Manage Virus and Spyware Protection policies.
- Manage SONAR scans.
- Manage Firewall and Intrusion Prevention policies.
- Manage Application and Device Control policies.
- Manage virtualized clients.
- Configure replication and load balancing.

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 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

Symantec Endpoint Protection Product Solution

- Why use Symantec Endpoint Protection?
- Symantec Endpoint Protection technologies
- Symantec Endpoint Protection services
- Symantec Endpoint Protection components
- Symantec Endpoint Protection policies and concepts
- Extending Symantec Endpoint Protection

Installing the Symantec Endpoint Protection Manager

- Identifying system requirements
- Preparing servers for installation
- Installing and configuring the Symantec Endpoint Protection Manager
- Describing Symantec Endpoint Protection upgrades and version compatibility

Configuring the Symantec Endpoint Protection Environment

- Starting and navigating the SEPM
- Describing policy types and components
- Console authentication
- Licensing the SEP environment

Deploying Windows Clients

- Planning the client deployment
- Configuring client deployment package
- Deploying packages to clients
- Maintaining the client environment
- Upgrading Symantec Endpoint Protection clients

Deploying Mac Clients

- Installation planning
- Package configuration
- Web-link and email deployment
- Third-party remote deployment

Client and Policy Management
- Describing SEPM and client communications
- Administering clients
- Configuring groups
- Configuring locations
- Active Directory integration with SEP 12.1
- Client configuration modes
- Configuring domains
- General client settings and Tamper Protection

Configuring Content Updates for Windows Clients
- Introducing LiveUpdate
- Configuring the SEPM for LiveUpdate
- Configuring the LiveUpdate Settings and Content policies
- Configuring multiple group update providers (GUPs)
- Manually updating virus definitions

Configuring Content Updates for Mac Clients
- Describing content update methods
- Configuring the LiveUpdate policy
- Configuring the SEPM as a reverse proxy
- Monitoring updates

Performing Server and Database Management
- Managing SEPM servers
- Maintaining server security
- Communicating with other servers
- Managing administrators
- Managing the database
- Disaster recovery techniques

Configuring Replication and Failover and Load Balancing
- About sites and replication
- How replication works
- Symantec Endpoint Protection replication scenarios
- Configuring replication
- Failover and load balancing

Designing a Symantec Endpoint Environment
- Architecture components
- Architecture constraints
- Component placement
- Content delivery
- Determining client to SEPM ratios
- SEPM and database sizing best practices

Introducing Antivirus, Insight, and SONAR
- Virus and spyware protection needs and solutions
- Reputation and Insight
- Administrator-defined scans
- Auto-Protect
- Download Insight
- SONAR
- Included Virus and Spyware Protection policies

Managing Virus and Spyware Protection Policies for Windows
- Configuring administrator-defined scans
- Configuring protection technology settings and scans
- Configuring e-mail scans
- Configuring advanced options
- Managing scanned clients

Managing Virus and Spyware Protection Policies for Mac
- Configuring scheduled scans
- Configuring Auto-Protect
- Configuring advanced options

Managing Exception Policies
- Exceptions and exclusions
- Configuring the Exceptions policy

Introducing Network Threat Protection
- The OSI model and network threats
- Network threat tools and attack methods
- Attack and mitigation

Managing Firewall Policies
- Firewall policy overview
- Defining rule components
- Modifying firewall rules
- Configuring built-in rules
- Configuring protection and stealth settings
- Configuring Windows integration settings

Managing Intrusion Prevention Policies
- Configuring network and browser intrusion prevention
- Managing custom signatures

Managing Application and Device Control Policies
- Creating application and device control policies
- Defining application control
- Modifying policy rules
- Defining device control

Virtualization
- Introducing virtualization features
- Virtual image exception
- Network and vShield Shared Insight Cache
- Virtual client tagging
- Offline image scanner