# VMware vSphere:
# Manage and Design for Security

## Overview

This course shows you how to follow best practices for secure design, deployment, and operation of a VMware vSphere™ environment. Through lecture, discussion, and hands-on practice, you will gain the knowledge and skills necessary to meet the security and compliance goals of your organization.

## Course Objectives

After completing this course, you should be able to:

- Identify vulnerabilities in the current design of a vSphere environment and recommend corrective actions
- Harden vSphere components as described in *vSphere Hardening Guide*
- Recommend configuration and change management policies, processes, and systems

## Target Audience

System administrators, systems engineers, and consultants responsible for securing a vSphere installation

## Prerequisites

This is an advanced course. Prerequisites include the completion of one of the following:

- VMware vSphere 4: Install, Configure, Manage
- VMware vSphere: Fast Track
- VMware vSphere 4: What's New
- Equivalent knowledge and administration experience with VMware ESX™/ESXi and VMware vCenter™ Server

Experience working at the command prompt is helpful.

## Pricing and Scope

- Three (3) days of instructor-led classroom training
- 60% lecture and 40% lab exercise
- Individual enrollment is available at convenient locations worldwide at http://www.vmware.com/education.
- Contact your VMware representative for pricing information.
- Onsite training is available for companies that want the benefits of instructor-led classes without travel.
- Contact VMware Education to discuss facility requirements for onsite training at education@vmware.com.

## Course Outline

### Module 1: Course Introduction
- Introductions and course logistics
- Online resources for security and compliance

### Module 2: Security in a Virtual Environment
- Review of information security and risk management concepts
- How virtualization affects security and compliance
- Top vulnerabilities in a virtual environment
- Basic guidelines for securing a virtual environment
- Security tools and technologies

### Module 3: Secure Virtual Networking
- vNetwork security architecture
- Network segmentation and traffic isolation
- Secure virtual network configuration
- Traffic isolation with private VLANs

### Module 4: Protecting the Management Environment
- vCenter Server authentication, authorization, and accountingWorking with SSL certificates
- Hardening the vCenter Server system

### Module 5: Protecting VMware ESX/ESXi Host Systems
- ESX and ESXi security architecture
- Controlling access to storage
- Hardening ESX and ESXi hosts.

### Module 6: Hardening Virtual Machines
- Virtual machine security architecture
- Configuring security parameters

### Module 7: Configuration and Change Management
- Configuration and change management goals and guidelines
- Maintaining the proper configuration of vSphere components
- Monitoring logs for security-related events
- Configuration and change management tools and technologies

**vm**ware®