imperva

Administering Imperva Security Infrastructure 13.0

April 2019

Overview

In this digital, on-demand hands-on course, students will learn:

- How to install and maintain SecureSphere system components including the Management Server, Gateway, and Agents.
- How to ensure connectivity among SecureSphere components and commonly integrated network devices.
- How to perform initial SecureSphere administration and configuration tasks that align with an organization's architecture and specific requirements or follow Imperva best practices.
- Common cross functional tasks such as object creation, policy creation, basic rule understanding, system alert interpretation, and report generation.

Who Should Attend

This course is intended for anyone who will need to configure and maintain SecureSphere, such as: database administrators, security team role(s), system administrators, Web application developers, and professional services using Imperva SecureSphere.

Prerequisites

Before taking this course, make sure you have the following skills:

- Working knowledge of Linux system administration and command line.
- Working knowledge of Linux system configuration files, such as /etc/fstab or /etc/snmp/snmpd.conf, and the ability to edit them with the vi editor.
- General understanding of application layer security concepts, application layer Web, and/or database protocols.
- Experience implementing or managing data center security or database applications is recommended.

Lesson Objectives

Video 1: Introduction

- Understand what the SecureSphere solution is and how it fulfills the requirements of the business.
- Define some sample guidelines from a corporate security strategy.
- Define a task workflow necessary for a new implementation of Imperva SecureSphere.
- Understand the high level architecture of the Imperva SecureSphere platform and how it will be
- implemented in this course.

Video 2: Getting Down to Business to Deploying SecureSphere

- Learn the process for installing Management and Gateway appliances.
- Execute the first time login procedures on your appliances.
- Define user account types used in administering SecureSphere.
- Verify connectivity and check status on your management and gateway servers.
- Define the operation mode of your gateway or gateways.
- Verify connectivity to your Management Server user interface.

Video 3: Completing the Initial Configuration

- Enable ICMP and SNMP on SecureSphere appliances to permit device monitoring.
- Mount remote file storage to collect and retain data per industry mandates.
- Configure Agent Listeners on the gateways in order to detect agent communications.

Video 4: Configuring SecureSphere in the Web UI

- Login for the first time to the SecureSphere Management Server.
- Install a SecureSphere license file.
- Navigate the SecureSphere Web user interface.
- Manage user accounts.
- Set password strength requirements.
- Download and schedule ADC updates.
- Set Protect Mode thresholds.

Video 5: Configuring Remote Authentication

- Configure remote or external authentication using Active Directory.
- Integrate LDAP into SecureSphere for security applications.
- Create a Windows Domain object to use globally through SecureSphere.

Video 6: Create Sites, Server Groups, and Services

- Create or modify a Gateway Group in the SecureSphere UI.
- Install and register SecureSphere Agents.
- Define a Site in the Site Tree.
- Understand what constitutes a Site.
- Create Server Group, Service and Application objects for a designated Site.

Video 7: Using Policies

- Review generated events from out-of-the-box policies.
- Create a system event policy.
- Identify System Events that may require specific policies or Followed Actions.
- Determine appropriate Followed Actions to use with System Event Policies.

Video 8: Responding to Events

- Create actions with email, FTP, Syslog, and other forms of communications.
- Use placeholders in an Action to enable dynamic information.

Video 9: Event Reporting

- Describe the features of SecureSphere's Report Settings.
- Demonstrate how to work with report Keywords.
- Create System Event reports.
- Schedule, archive and purge reports.
- View and configure alarms and notifications
- Report on threats using ThreatRadar event alerts.

Video 10: Basic Troubleshooting

- Use the MX Performance Graph and CLI tools to analyze and monitor gateway CPU resources.
- Troubleshoot network traffic via the Gateway's command line.
- Generate Tech info files from the CLI and Web UI.

Getting Started

Delivery Options

Digital, On-Demand
Self-paced, e-learning hosted on Imperva University. Students receive: ✓ **Four-six hours of video instruction** ✓ **Electronic Training Materials** ✓ **Sandbox access for hands-on Labs**

How to Purchase

Purchase Training Units via Purchase Order

Contact your local Imperva sales representative or contact your local Imperva partner for training unit price quote and to submit a Purchase Order for training units and receive an Imperva SRV# for use in class enrollment. If you do not have a sales contact, please call 1-866-926-4678, or complete our information form.

Purchase Classes via Credit Card

Training can be purchased using a major credit card, during the course enrollment process.

How to Enroll

IMPORTANT: Only individuals with an Imperva portal account username and password can enroll in classes.
If you do not have a Customer or Partner portal account, you may request one from our site. If you need assistance with the account request, contact support@imperva.com.

To enroll, have your portal username and password available, visit the Imperva Training website and register for your class from the Training Calendar. Select either Credit Card or Training Units as your payment option.
If you select Training Units, you may be asked to enter an Imperva SRV# (received when Purchase Order is finalized). Note: Company PO#s are not accepted for payment during class enrollment process.