∧ՈՈLՈW | Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Puoi raggiungerci qui

Arrow ECS Srl - Via Lancia 6/a - 39100 Bolzano

Email: training.ecs.it@arrow.com
Phone: +39 0471 099 134

SOPHOS   Sophos Central Architect Course

CODE:	LENGTH:	PRICE:
SOP_CNTRL	24 Hours (3 days)	€1,125.00

Description

This course provides an in-depth study of Sophos Central, designed for experienced technical professionals who will be planning, installing, configuring and supporting deployments in production environments.

Objectives

On completion of this course, trainees will be able to:? Design an installation considering all variables? Undertake a multi-site installation appropriate for a customer environment? Explain the function of core components, how they work, and how to configure them? Track the source of infections and cleanup infected devices? Perform preliminary troubleshooting and basic support of customer environments

Audience

System Engineers that will have to install or maitain a Sophos Central Infrastracture.

Prerequisites

Prior to taking this training you should:

- Have completed and passed the Sophos Central Endpoint and Server Protection - Certified Engineer course

We recommend students have the following knowledge and experience:

- Experience with Windows networking and the ability to troubleshoot issues
- A good understanding of IT security
- Experience using the Linux command line for common tasks
- Experience configuring Active Directory Group Policies
- Experience creating and managing virtual servers or desktops

Programme

Module 1: Deployment Scenarios (60 mins)

- Identify some of the common challenges when deploying Central
- Deploy Update Caches
- Set up Message Relays
- Configure AD Sync Utility
- Identify where Update Caches and Message Relays should be used

Labs (45 mins)

- Register and activate a Sophos Central evaluation
- Install Server Protection
- Install and Configure AD Sync Utility
- Deploy an Update Cache and Message Relay

Module 2: Client Deployment Methods (65 mins)

- Identify the recommended steps for deploying Sophos Central

- Explain the installation process, and identify the different types of installer
- Automate deployment for Windows, Linux and Mac computers
- Migrate endpoints from Enterprise Console
- Locate installation log files
- Remove third-party products as part of a deployment

Labs (75 mins)

- Enable Server Lockdown
- Deploy using Active Directory Group Policy
- Use the Competitor Removal Tool
- Deploy to a Linux Server using a Script

Module 3: Endpoint Protection Policies (80 mins)

- Describe the function and operation of each of the components that make up an Endpoint Protection and Intercept X
- Configure
- Test and validate Endpoint Protection
- Configure exclusions
- Configure Data Loss Prevention

Labs (100 mins)

- Test Threat Protection Policies
- Configure and Test Exclusions
- Configure Web Control Policies
- Configure Application Control Policies
- Data Control Policies

Module 4: Server Protection Policies (30 mins)

- Configure Server Protection Policies
- Configure and Manage Server Lockdown

Labs (65 mins)

- Configure Sever Groups and Policies
- Manage Server Lockdown Sophos Central Sophos Certified Architect
- Test Linux Server Protection

Module 5: Protecting Virtual Servers (60 mins)

- Connect AWS and Azure accounts to Sophos Central
- Deploy Server Protection to AWS and Azure
- Deploy and Manage Sophos for Virtual Environments

Labs (60 mins)

- Download the installer for the Security Virtual Machine
- Install the Security Virtual Machine (SVM) on a Hyper-V Server
- Configure Threat Protection policies to apply to the Security VMs and the Guest VMs they protect
- Perform a manual installation of the Guest VM Agent and view logs
- Test and configure a script to deploy the GVM Agent
- Manage Guest VMs from the Central Console
- Test Guest VM Migration

Module 6: Logging and Reporting (45 mins)

- Explain the types of alert in Sophos Central, and be able to read an RCA
- Use the Sophos Central logs and reports to check the health of your estate
- Export data from Sophos Central into a SIEM application
- Locate client log files on Windows, Mac OS X and Linux

Labs (55 mins)

- Generate and analyze an RCA
- Configure SIEM with Splunk

Module 7: Managing Infections (45 mins)

- Identify the types of detection and their properties

- Explain how computers might become infected
- Identify and use the tools available to cleanup malware
- Explain how the quarantine works and manage quarantined items
- Cleanup malware on a Linux server

Labs (40 mins)

- Source of Infection Tool
- Release a File from SafeStore
- Disinfect a Linux Server

Module 8: Management (65 mins)

- Use the Controlled Updates policies appropriately
- Enable multi-factor authentication
- Use the Enterprise Dashboard to manage multiple sub-estates
- Identify the benefits of the Partner Dashboard
- Identify common licensing requirements

Labs (25 mins)

- Enable Manually Controlled Updates
- Enable Multi-Factor Authentication

Follow on courses

Please contact us training.ecs.it@arrow.com

Test and Certification

To become a Sophos Certified Architect, trainees must take and pass an online assessment.
The assessment tests their knowledge of both the presented and practical content. The pass mark for the assessment is 80%, and is limited to 3 attempts.

Further Information

For any other information please contact training.ecs.it@arrow.com putting your contacts. You will be called back ASAP

Session Dates

Su richiesta. Contattaci al n.ro +39 0471 099134 oppure via mail a training.ecs.it@arrow.com

Informazioni aggiuntive

Questa formazione è disponibile anche come formazione in loco. Per favore, contattaci per saperne di più.