

ArcSight ESM Advanced Administrator (ASEAA)

ID ASEAA Prix sur demande Durée 5 jours

A qui s'adresse cette formation

This course is intended for Administrators who:

- Install, maintain, and troubleshoot ESM components
- Design and implement integrations between ArcSight ESM and other ArcSight products
- Proactively investigate the health of the ESM CORRE environment

Pré-requis

To be successful in this course, you should have the following prerequisites or knowledge:

- Knowledge of ESM Concepts
- (Minimum) 6 Months ArcSight Administration Experience
- Database SQL statements experience
- Linux Administration experience
- Successful Completion of ArcSight ESM Administrator & Analyst Course or Equivalent Experience

Objectifs

On completion of this course, participants should be able to:

- Identify the ESM communication strategy used between the various devices and components within an ESM Network
- Define each ESM operation modes and components, Compact and Distributed, and the issues ESM Distributed Mode comes to solve
- Plan, install, and run ESM in Distributed Mode
- Identify functions and navigate the Command Center UI
- Install and customize the ESM console
- Install and configure ArcSight SmartConnectors
- Install and configure a Forwarding Connector
- Import Zone and Asset information with the Network Model wizard
- Customize ArcSight ESM using the properties files
- Describe and install ArcSight upgrades and patches
- Configure and manage storage groups
- Describe CORRE daily job archives
- Recognize how to Back up and restore ESM
- Describe and deploy uses of SSL technology in ArcSight

ESM

Contenu

Module 1: Introduction to ESM Components

- Describe each ESM system component

Module 2: ESM Distributed Components

- Recognize where ESM fits within the ArcSight Architecture
- Define each ESM operation modes, Compact and Distributed, and the issues ESM Distributed Mode comes to solve
- Describe the ESM Distributed Mode components
- Recognize the ArcSight Data Platform (ADP) and its components

Module 3: Installing ESM Distributed Mode

- Plan System Hardware Requirements
- Check Operating System Pre-Installation
- Install ESM Persistor Node
- Install ESM Correlator Aggregator Node
- Configure Integration of the Persistor Node
- Add Correlator Aggregator Services
- Configure Message Bus Data and Control Instances from Persistor
- Configure Repository Instances from Persistor
- Configure Distributed Cache on Correlator Aggregators
- Run Cert Admin Approveall
- Start All Cluster Wide Services from Persistor Node

Module 4: Maintaining ESM Properties Files and Upgrades

- Customize ArcSight ESM using Properties File
- Prepare System for an Upgrade
- Upgrade ESM
- Upgrade the ESM Console

Module 5: Installing the ESM Console

- Install the ESM Console
- Customize the ESM Console

- Describe Tools available in the ESM Console

Module 6: Installing SmartConnectors

- Describe how Connectors collect, normalize, and cache events
- Install and configure ArcSight SmartConnectors
- Identify Connector Command Scripts
- Describe how Connectors can be managed from an ESM Console, a Connector Appliance, or ArcSight Management Center

Module 7: Managing the Network Model

- List Network Model resources
- Describe Asset Model resources
- Add the following modelling resources:
 - Assets
 - Asset Ranges
 - Zones
 - Network and attach it to a connector
 - Import Zone and Asset information with the Network Model wizard
 - Explain the use of the Asset Import Connector

Module 8: Configuring SmartConnector Destinations

- Get SmartConnector Status
- Set SmartConnector Flow-Control
- Use SmartConnector Administrative Dashboards
- Configure SmartConnectors for Failover and Dual Destinations

Module 9: Installing the ESM Super and Syslog Connectors

- Install and configure a Forwarding Connector
- Install and configure a Syslog connector

Module 10: SmartConnectors Configurations and Advanced Features

- Configure SmartConnectors using advanced features such as turbo mode, map files, event filtering, network options and event aggregation
- Construct advanced configuration settings for optimal performance and data enrichment

Module 11: Command Center

- Log onto the ArcSight Command Center
- Identify functions and navigate the User Interface

- Use the ArcSight Command Center Help Facility
- Configure:

- Authentication
- Content
- Storage
- Appliances
- Identify stock content dashboards

Module 12: ESM Backup and Restore

- Restore the ESM Manager's configurations
- Back up and restore ESM
- Describe CORR-E Daily Job Archiving

Module 13: Certificate Management

- Describe uses of SSL technology in ArcSight ESM
- Describe SSL setup options
 - keytool/keytoolgui
 - certadmin
 - Identify the steps to deploy:
 - Self-signed Certificates
 - Approve/revoke distributed mode Certificates
 - CA (Certificate Authority)-signed Certificates

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>