

ArcSight Certified Integrator/Administrator (ACIA) Certification Workshop Student Course Description



Upon successful completion of this workshop, the participant will be able to:

- Describe the ArcSight ESM Roles and Components which include ArcSight Connectors, the ArcSight Manager, the ArcSight Database and the various ArcSight Interfaces.
- Maintain the ArcSight ESM Oracle 10g database including understanding the Oracle tablespaces created during installation, implementing Oracle partitioning and ArcSight Partition Management.
- Install all of the components of the ArcSight ESM v4.0 within a Windows 2003/Linux Virtual Machine or other system, including the embedded Oracle 10g Database, the ArcSight Manager, the ArcSight Console and ArcSight SmartConnectors.
- Create ArcSight users including the proper administration of Access Control Lists (ACL's) for resources as well as understanding and deploying a password policy.
- ArcSight ESM notifications within your system implementation to receive system alarms and to inform or escalate security related events for proper remediation.
- Describe the measures taken to download, install and administer ArcSight ESM software patches including the ArcSight SmartConnectors, the ArcSight Manager and the Oracle 10g Database along with deploying new ArcSight ESM license files for your enterprise.
- Install and update as well as migrate SSL certificates as they pertain to the administration and use of the ArcSight ESM system.
- Install and configure ArcSight SmartConnectors for specific environments including filtering and batching events and providing failover and multiple destination configurations.
- Understand and use the Customer Support Center and appropriately use the send logs utility to send logs to ArcSight Customer Support.
- Troubleshoot the TNSListener service for ArcSight ESM to ensure proper database communications.
- Learn the properties and use of the various Manager log files as well as gain a basic understanding of the Logfu for Manager and Connector utility.
- Protect the ArcSight Manager and Oracle Database by learning the various ports required for communications between components.

- **Introductions**

(Instructor Led Presentation)

- **Lesson 1**

- **Overview of ArcSight ESM**

(Instructor Led Presentation)

- ArcSight Roles
 - ArcSight ESM Components
 - SmartConnectors
 - Supported Data Sources
 - FlexAgents
 - ArcSight Manager
 - ArcSight Database
 - User Interfaces
 - Console
 - Web
 - Discovery Modules
 - Resources
 - ArcSight Communications
 - Invoking SSL (CA)
 - Communication Ports Used
 - System Hardware/Software Recommendations

- **Lesson 2**

- **Managing the ArcSight Database**

(Instructor Led Presentation)

- Database Structure
 - Oracle Tablespace
 - ArcSight Tablespace
 - ArcSight Recommended Volume Layout
 - ArcSight Recommended RAID Configurations
 - Retention Area Configurations
 - Understanding Oracle Partitions
 - Understanding ArcSight Partitions
 - Retention Area Configurations
 - Online Retention Period Considerations
 - Archive Retention Period Considerations
 - Reserve Period Considerations

- **Lesson 3**

- **Installing ArcSight ESM**

(Instructor Led and Hands On Activity)

- Software Versioning
 - ArcSight Installation Overview
 - Installing ArcSight ESM V4.0
 - Installing the Embedded Oracle Database
 - Installing the ArcSight Database
 - Installing the ArcSight Manager
 - Installing the ArcSight Console
 - Installing the ArcSight Web

▪ **Lesson 4**

Administering ArcSight ESM

(Instructor Led and Hands On Activity)

- Administration of Users
 - Creating Users
 - Understanding User Types
 - Administration of ACL's
 - Group Inheritance
 - Resource Control
 - Configuring ArcSight Password Policy
- Administration of Notifications
 - Understanding Notifications
 - Using the Notification Templates
 - Configuring Notifications within ArcSight
- ArcSight Partition Management
 - Partition Lifecycle
 - Configuring Partition Management and the Archiver Agent
 - Using the Partition Manager within ArcSight
- ArcSight Packages
 - User Created, Custom Packages
 - ArcSight System Content
- Administering ArcSight's ESM SSL Certificates
- Using ArcSight Variables
 - Understanding variables
 - Most commonly used variables

▪ **Lesson 5**

ArcSight Connectors

(Instructor Led and Hands On Activity)

- Understanding ArcSight SmartConnectors
 - Overview of SmartConnectors
 - Installing ArcSight SmartConnectors
 - Customizing ArcSight SmartConnectors
 - Upgrading ArcSight SmartConnectors
 - Advanced Configurations of ArcSight SmartConnectors
 - Configuring Connectivity Failover
 - Multi Manager Configuration
- Understanding ArcSight FlexConnectors
 - What is a FlexConnector
 - Types of FlexConnectors
 - Installing a FlexConnector
 - The Configuration File
 - The Categorization File

▪ **Lesson 6**

Troubleshooting and Performance Tuning ArcSight

(Instructor Led Presentation with Hands On Activity)

- Troubleshooting ArcSight
 - Troubleshooting Tools
 - Troubleshooting the Event Flow
 - Troubleshooting the TNSListener
 - ArcSight Manager Logs
 - Using Logfu
 - Manager Logfu
 - Connector Logfu
- Using Customer Support Center (**Exercise**)
 - The Send Log utility
- Optimizing and Protecting ArcSight ESM
 - Query Optimization
 - Protecting Your Installation