



ET 712: Syslog and Audit Log Consolidation Management (SYSLOG)

Course Outline

Day 1

1. Introduction to Audit Log

- Overview SCOM Report
- Operation Report
- Audit Collection Report
- CCA Report

2. Implement Audit Collection Service

- Design ACS Infrastructure
- Install Audit Collection Service
- Display ACS Report
- Maintenance ACS Database

3. Deploying CCA Server Component

- Design and Sizing H/W for CCA
- Install CCA Component
- Checking and Upgrade CCA Version
- Uninstalling CCA Component
- Customizing CCA

Day 2

4. Collect Microsoft Log using CCA Agent

- Overview Log Consolidation using Agent
- Install CCA Agent
- Configuring CCA Agent to sending log to server
- Trouble shooting CCA Agent

5. Collect Microsoft Log using Argo Agentless

- Overview Agentless Process
- Deploy Windows Agentless Component
- Configure Windows Agentless
- Advanced Log Collection using Argo Agentless

6. Integrated Unix Sub System

- Overview SFU and SUA
- Install SFU on Windows 2003
- Configure Open SSH on windows
- Collect log file from Unix using SCP and SFTP

Day 3

7. Implement Syslog Server

- Overview Syslog Process
- Install Syslog Component
- Collect Syslog Data

8. CCA Report

- Introduction to CCA Report
- Deploying CCA Report
- Customizing CCA Report

9. Advanced CCA Implementation

- Distributed Component
- Backup and Restore Configuration