ManageEngine ADAudit Plus Training

Course Objectives

The ADAudit Plus training equips IT administrators with the skills to effectively audit Active Directory and the entire Windows infrastructure. By the end of this training, participants will be able to:

- Gain complete visibility on administrative changes in Active Directory.
- Use filter-based alerts to report on critical events.
- Answer the four vital questions: who made what change, when, and from where in the Windows infrastructure.
- Access a complete history of changes in Active Directory and Group Policy Objects.
- Organize audit data to support Security and Compliance auditing needs.

Who Should Attend

This training is ideal for:

- **IT Managers:** Responsible for overseeing IT operations and ensuring compliance.
- **IT Administrators:** Tasked with managing Active Directory and Windows infrastructure.
- **IT Auditors:** Focused on auditing IT environments for security and compliance.

This training will enhance your ability to perform auditing activities and fulfill compliance requirements.

Prerequisites

Participants should have:

- A basic understanding of Active Directory and Windows infrastructure.
- Familiarity with IT auditing concepts and practices.
- Basic experience in IT administration or IT security.

Course Objectives

By the end of this course, participants will be able to:

1. Achieve complete visibility into administrative changes in Active Directory.
2. Utilize filter-based alerts to monitor and report on critical events.
3. Answer the key auditing questions: who made what change, when, and from where within the Windows infrastructure.
4. Access and analyze the complete history of changes within Active Directory and Group Policy Objects (GPOs).

5. Organize audit data effectively to meet Security and Compliance auditing requirements.

Table of Contents (TOC)

- Other AD Object Auditing (Containers, Contacts, DNS, etc.)

Module 4: Account Lockout Analyzer

- Analyze Windows Services and Scheduled Tasks
- Analyze Network Drive Mappings, Logon Sessions, and Process Lists
- Logon Activity Analysis (Domain Controller and Local)
- OWA and ActiveSync Analysis
- Radius Server Logins Analysis

Module 5: File Server Auditing

- Auditing Windows File Servers
- Windows Failover Server Clusters Audit
- NetApp Filer Auditing
- EMC Storage Auditing
- File Integrity Monitoring

Module 6: Member Server Auditing

- Audit Logon Activity on Servers
- Track Process Activity
- Audit Policy Changes
- Monitor System Events
- Account Management on Servers
- Printer Auditing
- ADFS Auditing
- Removable Storage Auditing (USB)
- AD LDS Auditing

Module 7: Working with Alerts

- Default Alert Profiles
- Creating New Alert Profiles
- Alert Notifications
- Alert Audit Filters
- Threshold-Based Alerts

- User-Based Alerts
- Business Hour Alerts
- Customizing Alert Messages

Module 8: Advanced Configuration

- Working with Report Profiles
- Working with Event Rules
  - Creating New Rules and Rule Groups
- Global Exclude Configuration

Module 9: Administration

- Alert Me Configuration
- Adding Technicians
- Creating New Roles for Technicians
- Scheduling and Emailing Audit Reports
- Creating Custom Reports
- Archiving Events
  - Searching Archived Events
  - Generating Reports from Archived Events
  - Importing Old Archived "evt/evtx" Files
- SIEM Integration
- Configuring Mail Server

Conclusion

This course provides IT professionals with the tools and knowledge necessary to maximize the use of ADAudit Plus for effective Active Directory and Windows infrastructure auditing. By the end of the training, participants will be adept at using the software to enhance security, streamline audit processes, and meet compliance requirements.