

Oracle ADF and WebLogic Log Analysis

Native tools, monitoring and troubleshooting

FA-0652 · 3 days

DevOps, Cloud & Infrastructure

Read and correlate Oracle ADF and WebLogic logs, use native and selected third-party tools, and practise monitoring, WLST-assisted tasks and retention decisions in a prepared lab.

Introduction

This three-day course is for administrators and developers who support Oracle ADF, WebLogic and related Fusion Middleware environments. It develops a structured approach to finding relevant log entries, correlating events and using evidence to investigate failures.

Native tools and a selected third-party log-analysis tool are used in a prepared lab. Tool availability, interfaces and log formats depend on the installed Oracle components and versions; the course does not imply that every Oracle product has identical diagnostics.

Participants progress from log structure and native viewing to monitoring, troubleshooting, limited scripting and retention practices. Exercises use illustrative or sanitised logs and authorised lab access. Log interpretation supports investigation, but does not by itself prove a root cause or guarantee performance improvements.

Learning outcomes

The course teaches participants to:

- Distinguish relevant ADF, WebLogic and related middleware log types, levels and timestamps.
- Locate, filter and correlate entries using available native tools.
- Evaluate and configure a selected third-party viewer or collector for the training log formats.
- Monitor new entries and recognise limitations, noise and incomplete evidence.
- Investigate a prepared failure scenario and document evidence and follow-up checks.

- Use supported WLST operations and simple scripts for selected logging tasks.
- Review rotation, retention, access and sensitive-data handling without deleting evidence needed for investigation.

Prerequisites

- Basic understanding of Oracle ADF and WebLogic architecture.
- Familiarity with log files and their significance in system monitoring.
- Basic scripting knowledge (Shell scripting, Python, etc.) is beneficial.

Access to a prepared Oracle ADF/WebLogic lab or representative sanitised logs, with the selected native and third-party tools available. Required licences and authorised access are arranged before training.

Training outline

1. Day 1 – Logs and Native Oracle Tools

Morning: log structure and ADF logging

- Introduction to Logs: Importance and Types
- Oracle ADF logging mechanisms and Oracle Diagnostic Logging (ODL), where applicable

Afternoon: WebLogic logs and native viewing

- WebLogic server, domain and HTTP access logs: format, levels and correlation
- Practical exercise: filter and inspect logs using available Fusion Middleware Control, WebLogic console tools, JDeveloper log analysis or supported command-line tools

2. Day 2 – Third-Party Tools and Monitoring

Morning: tool selection and configuration

- Third-party log-analysis tools: format support, collection, access and suitability
- Configure one approved tool for the prepared Oracle lab; avoid assuming compatibility across all versions

Afternoon: monitoring and log-analysis practice

- Monitoring new log entries, filtering noise and correlating events

- Practical Exercise: Setting Up and Using Third-Party Tools for Log Analysis

3. Day 3 – Troubleshooting, Automation and Retention

Morning: evidence-led troubleshooting and WLST

- Troubleshooting using Logs
- WebLogic Scripting Tool: inspect logging configuration and demonstrate selected supported tasks

Afternoon: management practices and a selected automation exercise

- Log rotation, retention, access control, sensitive-data handling and preservation of investigation evidence
- Practical exercise: a bounded logging script and review of retention settings in the lab