

□

WebSphere Application Server V7 Security Information

Length:	3.0 Days
Ref:	WU611G-X
Delivery method:	ClassroomInstructor Led Online
Price:	EUR

Overview

This course covers security topics that are critical for advanced application server security configuration for WebSphere Application Server V7.

The course begins with a general discussion of the three major parts of global security: administrative security, application security, and Java 2 security. Students use security domains to configure cell-wide access. They then configure fine-grained security to the administrative console and configure application security by defining security constraints and security roles for a web application. Students also learn about the implications of application security by mapping special subjects and user groups to security roles.

This course presents the core concepts of federated repositories. Students create a federated repository using a file-based repository and add a Lightweight Directory Access Protocol (LDAP) server to the configuration. They secure the connection between the application server and the LDAP server, and learn to configure and manage a Virtual Machine Manager (VMM) security connection feature that allows the VMM to function either with or without all of its repositories available.

Secure Sockets Layer (SSL) is covered through extensive discussions about encryption technologies, digital signatures, the SSL handshake, and certificates. The course also provides additional information on SSL in the cell, including cell default trust stores, node keystores, plug-in keystores, certification expiration, and auto replacement. Lab exercises demonstrate both SSL configuration within the application server and the configuration of SSL between the application server and DB2 database. Students also configure cross cell single signon between two cells.

Students also learn how to harden the security of their application server environment by identifying areas that should be addressed in production environments. These areas include hardening the web server, configuring TAIs, protecting configuration files and private keys, using administrative roles, encrypting various links, and improving SSL configuration. Students learn how to use tracing and logs to determine authentication and authorization failures, and how to identify and resolve SSL connection problems by diagnosing log information.

Finally, students learn about the performance cost of security features in the application server, including

core JEE, messaging, and web services. A hands-on exercise on performance tuning lets students discuss techniques and trade-offs for tuning the security performance of the runtime environment.

For information about other related courses, visit the IBM Training website:
<http://www.ibm.com/training>

Public

This intermediate course is designed for application developers who want to use IBM Worklight V6 to create, manage, and deploy mobile applications to Android and iOS* mobile environments.

Prerequisites

You should have experience in Java **or** web development with Eclipse, **and** a good knowledge of the following web technologies:

- HTML5
- JavaScript
- Cascading Style Sheets (CSS) 3
- Web UI frameworks, such as Dojo **or** jQuery
- Representational State Transfer (REST) services
- Web services

A basic knowledge of a mobile web UI framework, such as Dojo Mobile, is helpful.

Objective

- Describe the conceptual differences between administrative security, application security, and Java 2 security
- Configure WebSphere Application Server to limit administrative console access to specific users
- Create and configure a security domain representing the administrative security configuration and application configuration
- Configure fine-grained administrative access to specific parts of a cell
- Define security constraints and security roles for a web application
- Map special subjects and user groups to security roles
- Configure the VMM security manager feature that allows the VMM to function either with or without all of its repositories available
- Explain the differences between symmetric and asymmetric key encryption
- Describe how digital signatures are generated and validated
- Configure secure communication between a client and a server
- Explain how certificates and certificate authorities provide secure communication
- Configure SSL for the Java Database Connectivity (JDBC) connection to the database
- Configure SSL within the cell

- Create and configure cross-cell authentication between two cells
- Harden the security configuration of the application server and its environment
- Modify the performance of security features in WebSphere Application Server
- Explain the cost of security in various areas, specifically core JEE, messaging, and web services
- Perform problem determination tasks that are related to authentication, authorization, and SSL errors
- Tune the WebSphere Application Server security runtime through custom property and administrative console configuration

Topics

- Course introduction
- WebSphere Application Server security 101 - global security
- WebSphere Application Server security 201 - global security
- Exercises overview
- Exercise: Administrative access
- Exercise: Configuring federated repositories
- More administrative access - security domains and fine-grained access
- Exercise: Working with security domains
- Exercise: Fine-grained administrative security
- Application security
- Exercise: Configuring security on the application
- Exercise: Application hardening
- Basics of SSL
- Certificates
- SSL configuration within WebSphere Application Server
- Exercise: Configuring SSL within a cell
- Establishing trusted relationships with external services
- Exercise: Configuring SSL to the database using JDBC
- Exercise: Cross-cell authentication
- Security problem determination (Optional)
- Exercise: Security problem determination (Optional)
- Security infrastructure hardening
- Exercise: Security infrastructure hardening
- WebSphere Application Server security performance (Optional)
- Exercise: Practical security performance tuning (Optional)
- Course summary