

Oracle Solaris 11 Security Administration

Course Summary

Description

Students will learn about the security features in Solaris 11. Students will learn how to implement these features and technologies to reduce the risk of intrusion and to secure their system applications and data

Objectives

- Describe Features in Solaris 11 to Secure the OS
- Understand Minimization
- Secure Users and Processes through Role Based Access Accounts (RBAC)
- Secure and Harden System Services
- Install Security Updates
- Restrict System and Root Access
- Configure Security Settings in the OS
- Manage Encryption and Certificates
- Configure Auditing to Audit Significant Events
- Secure Files and Filesystems
- Secure Systems and Attached Devices
- Manage Authentication Services
- Implement Network Security
- Secure the Network with Packet Filtering
- Securing the Solaris OE using Containers
- Implement Labeled Security Using Trusted Extensions
- Build and Install a Golden Image using the Automated Installer (AI)

Topics

- Security Planning
- Oracle Solaris 11 Security Technologies
- RBAC Roles, Rights, Profiles and Privileges
- Control System Services
- Solaris Cryptographic Services
- Auditing in Oracle Solaris 11
- Secure Files and File Systems
- Secure Systems and Attached Devices
- Manage Authentication Services
- Administer System Security
- Implement Basic Network Security
- The Solaris Security Compliance Utility
- Secure the Network with Packet Filtering
- Control System Services
- Implement Security in Oracle Solaris Zones
- Implement Labeled Security Using Trusted Extensions
- Building a Secure System

Prerequisites

Students should have the following skills

- Completed the Advanced Solaris 11 System Administration course
- Understand how to install Solaris software packages and OS updates with IPS
- Understand how to administer user accounts
- Understand how to configure the network in Solaris 11
- Understand how to create ZFS storage pools and file systems
- Understand Solaris file permissions
- Understand how to configure and manage Solaris Zones

Duration

Five Days

Oracle Solaris 11 Security Administration

Course Outline

- I. Security Planning**
 - A. Evaluating Security Principles
 - B. Develop a Security Policy
 - C. Review Steps to Configure a Secure System
 - D. Perform a Security Audit
- II. Oracle Solaris 11 Security Technologies**
 - A. Introducing the Oracle Solaris 11 operating system
 - B. Oracle Solaris 11 Security
- III. RBAC Roles, Rights, Profiles and Privileges**
 - A. Planning for RBAC
 - B. Using RBAC
 - C. Configure and Manage Privileges
 - D. Secure Root by Implementing Roles
 - E. Install and Implement ARMOR (Authorization Roles Managed on RBAC)
- IV. Control System Services**
 - A. Securing Services Through SMF
 - B. Managing Services
 - C. Secure Kernel Functions
- V. Solaris Cryptographic Services**
 - A. Cryptographic Services
 - B. The Cryptographic Framework
 - C. Key Management Framework
- VI. Auditing in Oracle Solaris 11**
 - A. Describe Auditing Tools
 - B. The Basic Audit Reporting Tool (BART)
 - C. Configure Auditing
 - D. Administering the Audit Service
 - E. Managing the Audit Records
- VII. Secure Files and File Systems**
 - A. Delegate and Manage ZFS Security
 - B. Controlling Access to Files
 - C. Implement ZFS Encryption
- VIII. Secure Systems and Attached Devices**
 - A. Controlling Access to Systems
 - B. Controlling Access to Devices
 - C. Using PAM to Authenticate Users
- IX. Manage Authentication Services**
 - A. Implement PAM to Authenticate Users
 - B. Implementing Kerberos Authentication Mechanism
 - C. Securing Remotely Accessed File Systems
- X. Administer System Security**
 - A. Controlling Access to Systems
 - B. Controlling Access to Devices
 - C. Using PAM to Authenticate Users
- XI. Implement Basic Network Security**
 - A. Network Security
 - B. Configure the Secure Shell
 - C. Configure Host Based Authentication with SSH
 - D. Configure TCP Wrappers
 - E. Understand the Kerberos Protocol
 - F. Using IPsec and IKE
 - G. Securing Remotely Accessed File Systems
- XII. The Solaris Security Compliance Utility**
 - A. Configure Security Compliance Checking and Reporting
- XIII. Secure the Network with Packet Filtering**
 - A. IP Filter Implementation
 - B. Configuring the IP Rules Set
 - C. Configuring IP Filter
- XIV. Control System Services**
 - A. Securing Services through SMF
 - B. Managing Services

Oracle Solaris 11 Security Administration

Course Outline (Cont.)

XV. Implement Security in Oracle Solaris Zones

- A. Securing the OS using Zones
- B. Security in Zones
- C. Integrating Security Features into Zones
- D. Managing Resources in Zones
- E. Managing Network Security in Zones
- F. Delegate Administrative privileges

XVI. Implement Labeled Security Using Trusted Extensions

- A. Describing Labeled Security
- B. Configure Labeled Zones and Filesystems
- C. Managing Trusted Extensions

XVII. Building a Secure System

- A. Building a custom distribution with the Distribution Constructor
- B. Configure a Secure Hands-off Installation using the Solaris Automated Installer (AI)