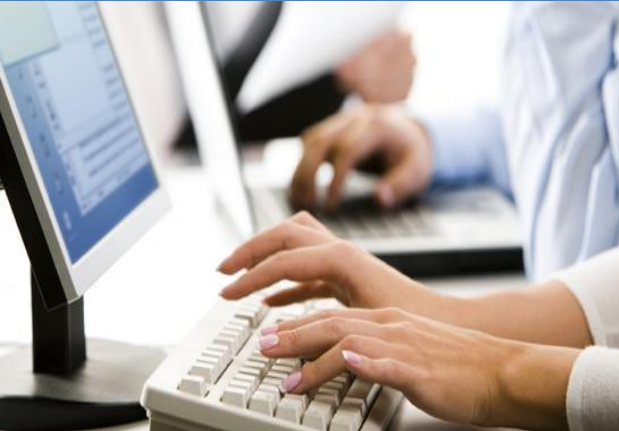


Security for Power Systems AIX

Skills and expertise to help you increase the business value from your Power Systems investment.



Purpose:

Today's leaders face multiple challenges, including the need to secure the enterprise against a barrage of new and evolving sophisticated threats. The IBM business-driven approach to enterprise security helps to identify gaps in your existing capabilities across the people, processes, applications, data, technology and physical facilities across your organization.

The goal of this course is to provide participants a detailed knowledge and hands-on experience in implementing AIX security mechanisms under AIX 6.1 and AIX 7.1. Customer using AIX 5L Version 5.3 may also attend this course.

For additional details on other AIX courses, please visit: <http://www.tlcpak.com/educ.html>

Audience:

This course is intended for persons who:

- Want to learn what the security mechanisms are built-in AIX Version 7.1 and 6.1
- Will plan, implement, or distribute a security policy in AIX

The audience for this training includes:

- AIX technical support individuals
- System administrators
- System architects

Prerequisites:

Students should have basic AIX administration experience. The AIX prerequisite may be met by attending one of the two following classes or having equivalent AIX skills:

- Power Systems for AIX II - AIX Implementation and Administration (AN120) (AU14) or (TN120)
- AIX Jumpstart for UNIX Professionals (AW18) (Q1818)



For complete details on the topics covered in each unit can be viewed at the following link.

<http://www.tlcpak.com/tn470.html>

* This course is also available for customers using AIX 6.1

Objectives:

On completion of this course participants should be able to:

- Security in an IT Environment
- Describe security threats to a computer system
- Understand AIX Base Security in detail
- List the AIX commands and components that can meet both the base system and network security threats.
- Configure, distribute, and monitor a security policy using AIX Security Expert.
- Configure the Role Based Access Control (RBAC) feature
- Implement the encrypted file systems feature
- Implement the Trusted Computing Base
- Implement the AIX install time options of Secure by Default and Trusted AIX

Course Code :TN470

Course Duration: 3 Days

Course Fee : Obtain upon request

Course Location : Customer onsite (Karachi, Lahore and Islamabad)

Discount : Discounts are available for a class of 5 and 8 students

Deliverables : Comprehensive Student Guide

Terms and Conditions: : 100% Payment in Advance



For additional information please write to us at: info@tlcpak.com or send us your nominations at www.tlcpak.com/nomination.html

Security for Power Systems AIX

Unit 1: Security in an IT Environment

Define the importance of IT Security
Describe some common threats to IT security
Define a basic model of security architecture
The ISO 7498-2 Security Architecture
Understanding Logical and physical security
List common AIX security services and threats
List AIX mechanisms for host security
List general guidelines for security policies
Firewall Technologies
Enterprise Security in a view
Integrating the physical, logical security layer
IBM Security Framework.

Unit 2: AIX Base System Security

Understand the concepts of users and groups.
Controlling root access on the system.
Define the uses of SUID, SGID and SVTX bits.
Understanding system wide security critical logs.
Users initialization process in AIX.
Assigning security privileges to a normal user.
Add/Change/Delete user and group accounts.
Setting up a long character user login ID.
Locking and unlocking a user account.
Assigning users with ADMIN rights.
AIX security files associated with Users and Groups.
AIX security checkpoint for security administrator.
Documenting Security Policy and Setup.

Unit 3: AIX network security

Potential security breaches in TCP/IP.
Check common security requirements: Availability, Integrity, Confidentiality and Monitoring.
Understanding TCP/IP start-up flow.
TCP/IP network services – Ports and Sockets
Use AIX Network Monitoring tools – iptrace, ipreport, netpmon and securetcpip.
Understanding network configuration files.
Why ssh is secure as compare to telnet.
Hardening host security.

Unit 4: Implementing Role Based Accessed Control

Introduction to AIX Role Back Access Control.
Traditional approach to AIX system administration.
Understanding available roles and authorizations.
Describe the role of Kernel Security Table.
The RBAC Framework.
Understand AIX RBAC commands.
Configuring Role Based Access Control.
Understanding Domain RBAC.

Unit 5: Implementing Trusted Computing base

Protecting your system from attacks.
Trojan Horse Practical Example.
Customization of system login prompt.
Configuring the Restricted Shell.
Configure AIX User defined authentication.
Extended File Permissions – Access Control List.
Concurrent recording of user's activity.
Use the Trusted Computing Base (TCB) facility to monitor your system and maintain system integrity.
Describe and utilize TCB components.

Unit 6: Implementing and distributing a Security Policy with AIXpert

Holistic view of AIX security framework.
Learn AIX security and regulatory and compliance.
Different levels of securities offered by AIXpert.
Illustrates how to configure security levels.
Distributing a security policy.
Undo a security policy
Check the consistency of the security policy
Disabling the remote logins.
Actions against server tampering.

Unit 7: Implementing Encrypted File Systems

Introduction and Encrypted File System usability.
Understanding CryptoLite cryptographic library.
Create and test EFS and related commands.
To backup & restore EFS.

Unit 8: AIX Install Time Security Options

BOS Install Security Options
Understand Secure by Default (SbD) Installation.
Actions to perform on a newly installed system.
Enabling and disabling SbD option.
Login control and setting up a specific herald.
AIX X11 and CDE concerns and Security Baselines.
Hardening OS, Network, and Application security.

Unit 9: Maintaining Systems Availability

System continuous availability
Understand Denial of Service (DoS) attack.
DoS Vs. DDoS – A Basic AIX Example.
Basic tools for detecting DoS attacks.
AIX host security checklist.
List common warning signs of a security breach.
AIX commands used to detect intrusion.
Real Time countermeasures.
Cleaning up the system after intrusion.

