

Securing NonStop Servers using Safeguard

U4196S



Delivery Type: Classroom

Duration: 4 days

Overview

This course provides information and knowledge needed to secure HP NonStop systems using NonStop operating system utilities and Safeguard. Topics covered include kernel security architecture, Safeguard administration and installation, user authentication and management, Guardian security, and securing OSS files. Hands-on labs reinforce concepts discussed and provide the opportunity to use the utilities and Safeguard. The four-day course is 70 percent lecture and 30 percent hands-on labs using HP servers.

Target Audience

This course is suitable for Information security administrators, Electronic Data Processing (EDP) auditors and System operations management personnel in security operations.

Pre-Requisites

- ✓ Concepts and Facilities for HP NonStop Systems (U4147S) **and**
- ✓ Knowledge of TACL commands (such as STATUS, FILEINFO, and WHO) for information gathering **and**
- ✓ Knowledge of Guardian utilities (such as FUP, SCF, and DSAP)
- ✓ Knowledge of basic OSS commands and utilities
- ✓ Ability to manage user profiles using the PASSWORD and DEFAULT programs

Objectives

- ✓ Be familiar with the \$CMON interface and TACL considerations
- ✓ Install and configure Safeguard software
- ✓ Create and manage user IDs
- ✓ Apply Access Control Lists (ACLs) on system objects
- ✓ Describe sources of audit events
- ✓ Use the Safecom command utility
- ✓ Use the SAFEART utility to generate audit reports
- ✓ Apply OSS standard security and OSS ACLs on OSS objects

Content

Module 1 - NonStop Kernel Security

Architecture

- ✓ Guardian and OSS application environments
- ✓ Authentication, authorization, and audit
- ✓ Goals of NonStop kernel standard security
- ✓ Components of NonStop kernel security architecture
- ✓ Memory address isolation and disk file protection
- ✓ \$CMON process
- ✓ Licensed program files
- ✓ Setuid setting for OSS programs
- ✓ Lab

Module 2 - Safeguard Features

- ✓ Relation of Safeguard to the NonStop kernel
- ✓ Safeguard extensions to NonStop kernel security system
- ✓ Safeguard process components and their functions
- ✓ Safeguard disk file components and global configuration options
- ✓ Safeguard warning mode and OSS audit options
- ✓ Lab

Module 3 - User Authentication

- ✓ Authentication defined
- ✓ User profile management considerations
- ✓ Safeguard configuration options for password management and system access control
- ✓ Guardian user IDs and OSS UID
- ✓ Administrative and file sharing groups
- ✓ User profile options for Guardian and OSS
- ✓ Network users and remote passwords
- ✓ Create a user ID using Safecom
- ✓ Lab

Module 4 - User Management with Safecom

- ✓ Safecom session commands and displays
- ✓ User IDs and aliases management
- ✓ File sharing group(s) for OSS usage
- ✓ User audit attributes
- ✓ Default protection for users
- ✓ Safeguard authentication service
- ✓ Lab

Module 5 - Guardian Security

- ✓ System product files and sensitive utilities

- ✓ ACL specific considerations
- ✓ Guardian disk file access and ownership control
- ✓ Process and ownership controlHP Education services are governed by the HP Education Services Terms and Conditions 3
- ✓ Guardian disk file security
- ✓ OSS UGO bits, umask, and .profile file
- ✓ OSS sticky bit, SETUID, SETGID
- ✓ OSS file ownership access and control
- ✓ Lab

Module 6 - Securing OSS Files

- ✓ OSS file system layout
- ✓ File security
- ✓ Permission modes
- ✓ File and directory permissions
- ✓ User and group IDs
- ✓ Setting the sticky bit
- ✓ OSS file change ownership and group association
- ✓ OSS Access Control Lists (ACLs)
- ✓ File and directory ACLs
- ✓ Lab

Module 7 - Authorization and Object Access Control

- ✓ Object types and their management
- ✓ Safecom to create and manage protection records on objects
- ✓ Apply ACLs on objects
- ✓ Object warning mode
- ✓ ACL persistence
- ✓ Node names on ACLs
- ✓ DISKFILE-PATTERN
- ✓ Lab

Module 8 - Safeguard Audit Configuration

- ✓ Sources of security event audit information
- ✓ Create, manage, and activate audit pools
- ✓ Audit pool recovery modes
- ✓ OSS API and process audit
- ✓ Safeguard configuration for OSS audit
- ✓ AUDITENABLED option for OSS filesets
- ✓ SAFEART utility
- ✓ Lab

Module 9 - Safeguard Administration and Installation

- ✓ Safeguard security administration features
- ✓ Assign control of Safeguard

- ✓ Safeguard security groups
- ✓ Safeguard installation options
- ✓ Undeniable super ID
- ✓ Security Event Exit Process (SEEP)
- ✓ Learning check

Follow on Courses

- ✓ Consider attending the other advanced learning courses in the HP NonStop Operations Management curriculum.