Hewlett Packard Enterprise

Securing HP NonStop Servers Using Safeguard U4196S

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. The course is 70 percent lecture and 30 percent hands-on labs using HP servers.

Securing HP NonStop Servers Using Safeguard	
Price	USD $3,200
Links to local schedules, pricing and registration	**US/Canada** **Mexico/Latin America** **Brazil**
HP course #	U4196S
Category	NonStop
Duration	4 days

Audience

- Information technology security administrators and auditors
- System operations management personnel in security operations

Prerequisites

- Concepts and Facilities for HP NonStop Systems (U4147S) and
- Knowledge of TACL commands and Guardian utilities and
- Knowledge of basic OSS commands and utilities and
- Ability to manage user profiles using the PASSWORD and DEFAULT programs

Course objectives

At the conclusion of this course you should be able to:

- 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
- Use the Safecom command and SAFEART utilities
- Apply OSS standard security and OSS ACLs on OSS objects

Benefits to you

- Learn how to establish a chosen level of protection selectively, without impeding application or user productivity, through authentication, authorization, and auditing
- Gain valuable hands-on experience using Safeguard software to improve server availability by reserving resources for critical production applications, ensuring that applications are accessed only by authorized clients, and protecting critical data from unauthorized or accidental modification

Next steps

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

Course outline

Module 0 - Course Overview

Module 1 - NonStop Kernel Security Architecture
- Guardian and OSS application environments
- Authentication, authorization, and auditing
- Goals of NonStop kernel standard security
- Components of NonStop kernel security architecture
- Memory address isolation and disk file protection
- $CMON process and licensed program files
- Setuid setting for OSS programs

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

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

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 and default protection for users
- Safeguard authentication service

Module 5 - Guardian Security
- System product files and sensitive utilities
- TACL specific considerations
- Guardian disk file access and ownership control
- Process and ownership control
- Guardian disk file security
- Impact of PROGID program files

Module 6 - Securing OSS Files
- OSS file system layout
- File security and 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) and ACL types

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 for non-existing diskfiles
- Node names on ACL access clause
- DISKFILE-PATTERN and SAVED-DISKFILE-PATTERN

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
- XYGATE Merged Audit (XMA) features and architecture

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)

Onsite Delivery Equipment Requirements
- Workstation with terminal emulator to access lab host system

Learn more at

hpe.com/us/training/nonstop

U4196S Ver I.00

c04707018 January 2016

Hewlett Packard Enterprise