Securing HPE NonStop Servers using Safeguard Training

Duration: **4 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

This course provides the knowledge and practical skills required to secure**HPE NonStop systems** using NonStop operating system utilities and **Safeguard**.

Participants explore key areas including the NonStop kernel security architecture, Safeguard installation and administration, user authentication and management, Guardian security, and techniques for securing OSS files.

The theoretical content is reinforced through hands-on laboratory exercises, giving participants an opportunity to work directly with relevant utilities and Safeguard functionality. This four-day course consists of approximately **70% instructor-led theory and 30% hands-on laboratory work** using HPE servers.

Prerequisites

Participants should have:

- Knowledge equivalent to Concepts and Facilities for HPE NonStop Systems (U4147S)
- Experience using TACL commands such as STATUS, FILEINFO, and WHO to gather information
- Familiarity with Guardian utilities including FUP, SCF, and DSAP
- Knowledge of basic OSS commands and utilities
- The ability to manage user profiles using the PASSWORD and DEFAULT programs

Who Should Attend

This course is particularly suitable for:

- Information Security Administrators
- Electronic Data Processing (EDP) Auditors
- System Operations Management personnel working within security operations

Securing HPE NonStop Servers using Safeguard Training

Duration: **4 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of the course, participants will be able to:

- Explain the $CMON interface and important TACL considerations
- Install and configure Safeguard software
- Create and manage user IDs
- Apply Access Control Lists (ACLs) to system objects
- Describe the different sources of audit events
- Work with the Safecom command utility
- Generate audit reports using the SAFEART utility
- Apply standard OSS security mechanisms and OSS ACLs to OSS objects

How You Will Benefit

Participants learn how authentication, authorization, and auditing can be used to establish an appropriate level of protection without unnecessarily restricting application performance or user productivity.

Hands-on work with Safeguard provides practical experience in protecting resources for critical production applications, helping ensure applications are accessed only by authorised clients, and protecting important data against unauthorised or accidental modification.

Training Outline

Module 1 – NonStop Kernel Security Architecture

- Guardian and OSS application environments
- Authentication, authorization, and auditing
- Objectives of NonStop kernel standard security
- Components of the NonStop kernel security architecture
- Memory address isolation and disk file protection
- The $CMON process
- Licensed program files
- Setuid settings for OSS programs
- Hands-on lab

Module 2 – Safeguard Features

- Relationship between Safeguard and the NonStop kernel
- Safeguard extensions to the NonStop kernel security system
- Safeguard process components and their functions
- Safeguard disk file components
- Global configuration options
- Safeguard warning mode
- OSS audit options
- Hands-on lab

Securing HPE NonStop Servers using Safeguard Training

Duration: **4 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Module 3 – User Authentication

- Understanding authentication
- User profile management considerations
- Safeguard configuration options for password management
- System access control
- Guardian user IDs and OSS UIDs
- Administrative and file-sharing groups
- User profile options for Guardian and OSS
- Network users and remote passwords
- Creating a user ID with Safecom
- Hands-on lab

Module 4 – User Management with Safecom

- Safecom session commands and displays
- Managing user IDs and aliases
- File-sharing groups for OSS use
- User audit attributes
- Default user protection
- Safeguard authentication service
- Hands-on lab

Module 5 – Guardian Security

- System product files and sensitive utilities
- TACL-specific security considerations
- Guardian disk file access and ownership control
- Process and ownership control
- Guardian disk file security
- OSS UGO bits, umask, and the .profile file
- OSS sticky bit, SETUID, and SETGID
- OSS file ownership, access, and control
- Hands-on 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
- Changing OSS file ownership and group association
- OSS Access Control Lists (ACLs)
- File and directory ACLs
- Hands-on lab

Module 7 – Authorization and Object Access Control

- Object types and their management
- Creating and managing object protection records with Safecom

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- Applying ACLs to objects
- Object warning mode
- ACL persistence
- Using node names within ACLs
- DISKFILE-PATTERN
- Hands-on lab

Module 8 – Safeguard Audit Configuration

- Sources of security event audit information
- Creating, managing, and activating audit pools
- Audit pool recovery modes
- OSS API and process auditing
- Configuring Safeguard for OSS auditing
- The AUDITENABLED option for OSS filesets
- Using the SAFEART utility
- Hands-on lab

Module 9 – Safeguard Administration and Installation

- Safeguard security administration capabilities
- Assigning control of Safeguard
- Safeguard security groups
- Safeguard installation options
- Undeniable Super ID
- Security Event Exit Process (SEEP)
- Learning check