



Securing HPE NonStop Servers using Safeguard U4196S

| | |
|---|--------------------------|
| HPE course number | U4196S |
| Course length | 4 days |
| Delivery mode | ILT, VILT |
| View schedule, local pricing, and register | View now |
| View related courses | View now |

This course provides information and knowledge needed to secure HPE NonStop systems using HPE 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 course is 70% lecture and 30% hands-on labs using HPE servers.

Why HPE Education Services?

- IDC MarketScape leader 5 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

Audience

- Information security administrators
- Electronic Data Processing (EDP) auditors
- System operations management personnel in security operations

Prerequisites

- Concepts and Facilities for HPE NonStop Systems (U4147S)
- Knowledge of TACL commands (such as STATUS, FILEINFO, and WHO) for information gathering
- 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

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
- 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

Detailed course outline

| | | |
|--|---|--|
| Module 1: NonStop Kernel Security Architecture | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• \$CMON process• Licensed program files• Setuid setting for OSS programs• Lab |
| Module 2: Safeguard Features | <ul style="list-style-type: none">• Relation of Safeguard to the NonStop kernel• Safeguard extensions to NonStop kernel security system• Safeguard process components and their functions | <ul style="list-style-type: none">• Safeguard disk file components and global configuration options• Safeguard warning mode and OSS audit options• Lab |
| Module 3: User Authentication | <ul style="list-style-type: none">• Authentication defined• User profile management considerations• Safeguard configuration options for password management and system access control• Guardian user IDs and OSS UID | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• Safecom session commands and displays• User IDs and aliases management• File sharing group(s) for OSS usage• User audit attributes | <ul style="list-style-type: none">• Default protection for users• Safeguard authentication service• Lab |
| Module 5: Guardian Security | <ul style="list-style-type: none">• System product files and sensitive utilities• TACL specific considerations• Guardian disk file access and ownership control• Process and ownership control• Guardian disk file security | <ul style="list-style-type: none">• OSS UGO bits, umask, and profile file• OSS sticky bit, SETUID, SETGID• OSS file ownership access and control• Lab |
| Module 6: Securing OSS Files | <ul style="list-style-type: none">• OSS file system layout• File security• Permission modes• File and directory permissions• User and group IDs | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• Object types and their management• Safecom to create and manage protection records on objects• Apply ACLs on objects• Object warning mode | <ul style="list-style-type: none">• ACL persistence• Node names on ACLs• DISKFILE-PATTERN• Lab |
| Module 8: Safeguard Audit Configuration | <ul style="list-style-type: none">• Sources of security event audit information• Create, manage, and activate audit pools• Audit pool recovery modes• OSS API and process audit | <ul style="list-style-type: none">• Safeguard configuration for OSS audit• AUDITENABLED option for OSS filesets• SAFEART utility• Lab |

Course data sheet

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

Onsite Delivery Equipment Requirements

- Workstation with terminal emulator to access lab host system
-

Learn more at
hpe.com/ww/learnnonstop

Follow us:



© Copyright 2020 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. The OpenStack Word Mark is either a registered trademark/service mark or trademark/service mark of the OpenStack Foundation, in the United States and other countries and is used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation or the OpenStack community. Pivotal and Cloud Foundry are trademarks and/or registered trademarks of Pivotal Software, Inc. in the United States and/or other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other third-party trademark(s) is/are property of their respective owner(s).

U4196S I.01, March 2020