Securing HPE NonStop Servers using Safeguard Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Bu eğitim, **HPE NonStop sistemlerinin**, NonStop işletim sistemi araçları ve **Safeguard** kullanılarak güvenli hale getirilmesi için gerekli bilgi ve uygulama becerilerini kazandırmayı amaçlar.

Program kapsamında NonStop kernel security architecture, Safeguard kurulumu ve yönetimi, kullanıcı kimlik doğrulama ve yönetimi, Guardian security ve OSS dosyalarının güvenliğinin sağlanması gibi temel konular ele alınır.

Teorik konular, katılımcıların ilgili utility'leri ve Safeguard özelliklerini doğrudan kullanabileceği hands-on laboratuvar çalışmalarıyla desteklenir. Dört günlük eğitim yaklaşık **%70 teorik anlatım ve %30 uygulamalı laboratuvar** şeklinde yürütülür ve laboratuvar çalışmalarında HPE sunucuları kullanılır.

Önkoşullar

Katılımcıların aşağıdaki bilgi ve becerilere sahip olması beklenir:

- HPE NonStop Systems Concepts and Facilities (U4147S) kapsamında ele alınan bilgiler
- Bilgi toplamak için STATUS, FILEINFO ve WHO gibi TACL komutlarını kullanabilme
- FUP, SCF ve DSAP gibi Guardian utility'lerine aşinalık
- Temel OSS komutları ve utility'leri hakkında bilgi
- PASSWORD ve DEFAULT programları aracılığıyla user profile yönetebilme

Kimler Katılmalı

Bu eğitim özellikle aşağıdaki roller için uygundur:

- Bilgi Güvenliği Yöneticileri
- Electronic Data Processing (EDP) Auditor'ları
- Security operations alanında görev yapan System Operations Management personeli

Securing HPE NonStop Servers using Safeguard Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Neler Öğreneceksiniz

Eğitim sonunda katılımcılar:

- $CMON interface ve TACL ile ilgili güvenlik hususlarını açıklayabilecek,
- Safeguard yazılımını kurup yapılandırabilecek,
- User ID oluşturabilecek ve yönetebilecek,
- System object'lere Access Control List (ACL) uygulayabilecek,
- Audit event kaynaklarını açıklayabilecek,
- Safecom command utility'yi kullanabilecek,
- SAFEART utility ile audit report oluşturabilecek,
- OSS object'lerinde standart OSS security mekanizmalarını ve OSS ACL'lerini uygulayabilecektir.

Eğitimin Sağladığı Faydalar

Katılımcılar eğitim boyunca authentication, authorization ve auditing mekanizmalarını kullanarak ihtiyaç duyulan koruma seviyesinin nasıl seçici biçimde uygulanabileceğini öğrenir. Amaç, güvenliği artırırken application veya user productivity üzerinde gereksiz kısıtlamalar oluşturmamaktır.

Safeguard üzerinde gerçekleştirilen uygulamalı çalışmalar sayesinde kritik production application'lar için kaynakların korunması, uygulamalara yalnızca yetkili client'ların erişmesinin sağlanması ve kritik verilerin yetkisiz veya yanlışlıkla gerçekleştirilen değişikliklere karşı korunması konusunda pratik deneyim kazanılır.

Eğitim İçeriği

Modül 1 – NonStop Kernel Security Architecture

- Guardian ve OSS application environment'ları
- Authentication, authorization ve audit
- NonStop kernel standard security hedefleri
- NonStop kernel security architecture bileşenleri
- Memory address isolation ve disk file protection
- $CMON process
- Licensed program files
- OSS programları için Setuid ayarı
- Uygulamalı laboratuvar

Modül 2 – Safeguard Özellikleri

- Safeguard ile NonStop kernel arasındaki ilişki
- Safeguard'ın NonStop kernel security system'e sağladığı genişletmeler
- Safeguard process component'leri ve görevleri
- Safeguard disk file component'leri
- Global configuration seçenekleri
- Safeguard warning mode
- OSS audit seçenekleri

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Uygulamalı laboratuvar

Modül 3 – User Authentication

- Authentication kavramı
- User profile management sırasında dikkate alınması gereken noktalar
- Password management için Safeguard configuration seçenekleri
- System access control
- Guardian User ID ve OSS UID
- Administrative ve file sharing group'ları
- Guardian ve OSS için user profile seçenekleri
- Network users ve remote passwords
- Safecom kullanarak User ID oluşturma
- Uygulamalı laboratuvar

Modül 4 – Safecom ile User Management

- Safecom session command'ları ve display'leri
- User ID ve alias yönetimi
- OSS kullanımı için file sharing group'ları
- User audit attributes
- Kullanıcılar için default protection
- Safeguard authentication service
- Uygulamalı laboratuvar

Modül 5 – Guardian Security

- System product files ve hassas utility'ler
- TACL'e özgü güvenlik hususları
- Guardian disk file access ve ownership control
- Process ve ownership control
- Guardian disk file security
- OSS UGO bits, umask ve .profile dosyası
- OSS sticky bit, SETUID ve SETGID
- OSS file ownership, access ve control
- Uygulamalı laboratuvar

Modül 6 – OSS Dosyalarının Güvenliğinin Sağlanması

- OSS file system yapısı
- File security
- Permission modes
- File ve directory permissions
- User ve Group ID'leri
- Sticky bit ayarlama
- OSS file ownership ve group association değişiklikleri
- OSS Access Control Lists (ACLs)
- File ve directory ACL'leri
- Uygulamalı laboratuvar

Modül 7 – Authorization ve Object Access Control

- Object type'ları ve yönetimi

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Safecom ile object protection record oluşturma ve yönetme
- Object'lere ACL uygulama
- Object warning mode
- ACL persistence
- ACL'lerde node name kullanımı
- DISKFILE-PATTERN
- Uygulamalı laboratuvar

Modül 8 – Safeguard Audit Configuration

- Security event audit information kaynakları
- Audit pool oluşturma, yönetme ve etkinleştirme
- Audit pool recovery mode'ları
- OSS API ve process audit
- OSS audit için Safeguard configuration
- OSS fileset'lerinde AUDITENABLED seçeneği
- SAFEART utility kullanımı
- Uygulamalı laboratuvar

Modül 9 – Safeguard Administration ve Installation

- Safeguard security administration özellikleri
- Safeguard kontrolünün atanması
- Safeguard security group'ları
- Safeguard installation seçenekleri
- Undeniable Super ID
- Security Event Exit Process (SEEP)
- Learning check