Sistem Bütünlüğü Testi

Bu dökümanda sistem bütünlüğü için test adımlarını içerir.

Kurulum ve kullanım adımlar izlenerek proxy sunucusu kurulur.

Herhangi bir playbook çalıştırıldıktan sonra sistem bütünlüğü için gerekli olan betikler otomatik olarak sisteme yüklenir ve belirlendiği zaman aralıklarında sistemi kontrol eder.

Bu periyodik kontroller paketler, kullanıcılar, gruplar ve konfigürasyon dosyalarını kontrol eder.

Paketler için test komutu:

#sudo apt install sl

Yukarıdaki komut çalıştırılıp sl paketi kurulduktan sonra **/var/log/syslog** dosyasına şu şekilde log düşmelidir:

2018-11-03T08:00:46.304978+03:00 ossimcik integrity-check: PACKAGE|sl

Eğer kullanıcı sistem bütünlüğünü **fix** parametresi **true** olarak ayarlamış ise kurulu paket kontrol sırasında kaldırılmış olmalıdır.

Kullanıcılar ve gruplar için test komutu:

#sudo adduser testuser

Yukarıdaki komut çalıştırıp istenilen değerler varsayılan olarak kaydedildiğinde sisteme yeni bir kullanıcı eklenir. **/var/log/syslog** dosyasına şu şekilde loglar düşmelidir:

2018-11-03T07:57:28.427761+03:00 ossimcik integrity-check: USER|testuser
2018-11-03T07:57:28.430638+03:00 ossimcik integrity-check: GROUP|testuser

Eğer kullanıcı sistem bütünlüğünü **fix** parametresi **true** olarak ayarlamış ise oluşturulmuş kullanıcı ve grup kontrol sırasında kaldırılmış olmalıdır.

Konfigürasyon dosyaları için test komutu:

#sudo echo -e “\n#test\n” >> /etc/hosts

Yukarıdaki komut çalıştırıldıktan sonra **/var/log/syslog** dosyasına şu şekilde log düşmelidir:

2018-11-03T08:00:46.354150+03:00 ossimcik integrity-check: CONF|/etc/hosts