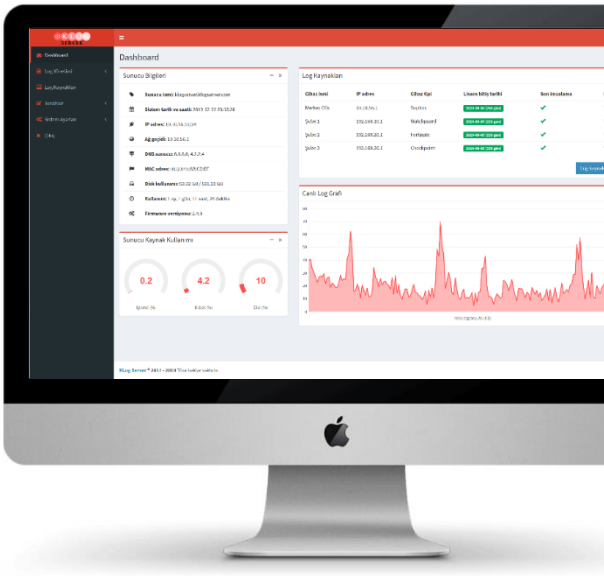
KLOG SERVER

ELEKTRONİK ZAMAN DAMGASI

KLog Server

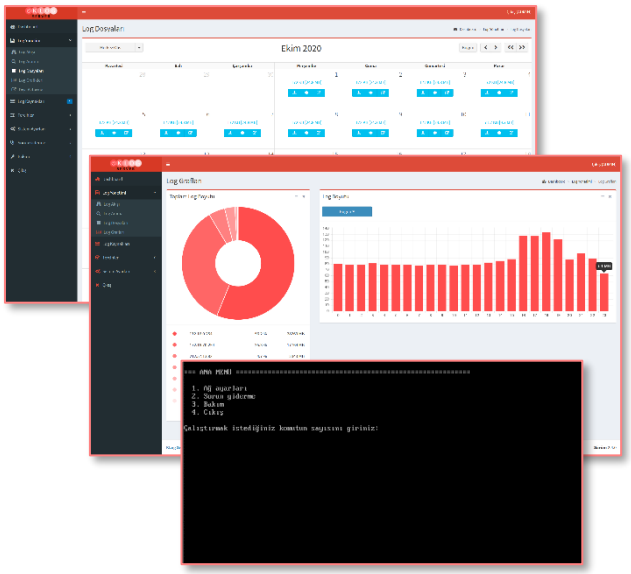


KLog Server 5651 yasasına uygun zaman damga hizmetini sağlayan, bir Syslog sunucusudur. Aynı zamanda KLog Server paylaşılmış klasörden log toplama ve imzalama özelliğine sahiptir. KLog Server Linux tabanlı VMware ve Microsoft Hyper-V platformlarıyla uyumlu hazır sanal makine olarak sağlanmaktadır.

KLog Server üretici bağımsız, standart Syslog protokolü ile log üreten tüm cihazlarla (Güvenlik Duvarı, Sunucu, vs.) bütünleşmiş çalışmaktadır.

KLog Server gün boyunca aldığı logları, günün sonunda Kamu SM (Kamu Sertifikasyon Merkezi) onaylı sertifika ile elektronik olarak imzalar ve log dosyasını, imza dosyası ile birlikte depolar.

Özellikler

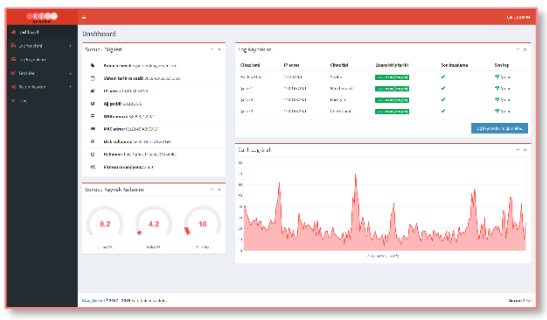


- KLog Server Linux tabanlıdır ve kurulumu Windows lisansı gerektirmez.
- Kamu SM onaylı SHA-512 karma algoritması log imzalama özelliğine sahiptir.
- Web tabanlı yönetim ekranına ve konsol bağlantısına sahiptir.
- Kurulum ve yapılandırması çok basittir.
- Log üreten cihazı otomatik olarak tespit eder ve log almaya başlar.
- Paylaşılmış klasörden (SMB) log toplama ve imzalama özelliğine sahiptir.
- Anlık log içeriği izleme ve loglarda arama özelliğine sahiptir.
- Loglama ve imzalama durumu Dashboard ekranından takip edilebilir.
- İhtiyaç durumunda imzalanmış loglar ve imza dosyaları web ara yüzden indirilebilir.
- İmzalanmış logları günlük olarak FTP sunucusuna veya paylaşılmış klasöre aktarılabilir.
- Çoklu yönetici veya bayi/müşteri yapısına sahiptir.

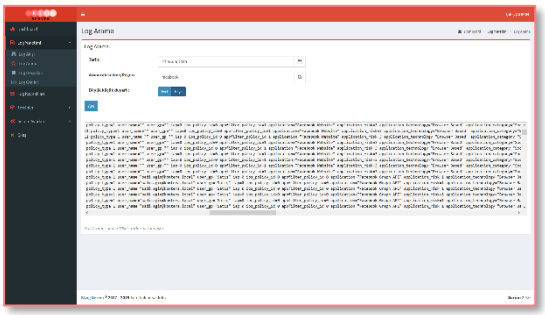
Dashboard Ekranı

Dashboard ekranı tek bakışta sistem ve log alma/imzala ile ilgili genel bilgi sunmaktadır. Bu ekranda tarih ve saat, ağ ayarları, işlemci, bellek ve disk kullanımı gibi sistemsel bilgiler bulunmaktadır. Ayrıca log kaynağı bazında, lisans durumu, son imzalama durumu ve alınan son log kaydının zamanı bulunmaktadır.

Log kaynağı bazında canlı log boyutu grafik olarak Dashboard ekranında yer almaktadır.



Log içeriği izleme ve loglarda arama



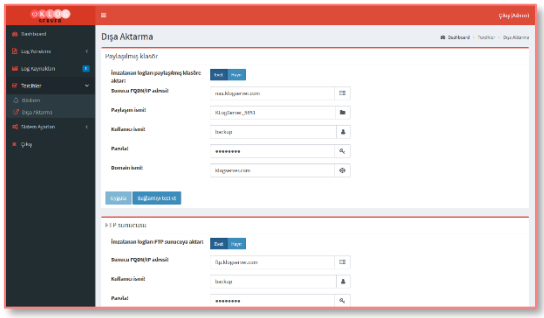
Alınan logları anlık olarak metin biçiminde Log Akışı ekranından izlenebilmektedir. Birden fazla log kaynağı tanımlandığı durumda, izlemek istenilen log kaynağı listeden seçilebilir ve anlık loglar takip edilebilir.

Loglarda arama özelliği imzalama bekleyen veya imzalanmış loglarda belirlenen log kaynağı, tarih ve anahtar kelimeye göre arama imkanı sağlar ve sonuçlar metin biçiminde web ara yüzde görüntülenir.

Log Dosyaları Dışa Aktarma

Günlük log dosyaları imzalandıktan sonra, imza dosyaları ile birlikte otomatik olarak dışa aktarılabilir. Desteklenen harici depolama alanları FTP sunucusu ve paylaşılmış klasördür. Dışa aktarılan dosyalar isteğe bağlı olarak silinebilir.

Günlük dışa aktarım dışında, loglar toplu şekilde de dışa aktarılabilir, web ara yüzden indirilebilir veya disk'ten silinebilir.



Çoklu Yönetici Yapısı

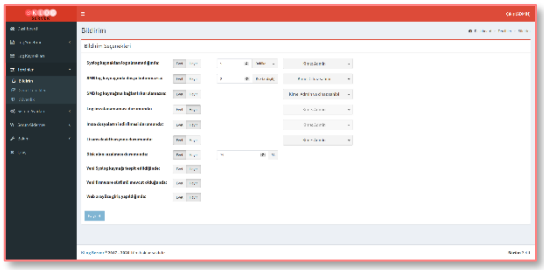
KLog Server yönetici veya bayi/müşteri yapısına sahiptir. Bu sayede birden fazla yönetici hesabı tanımlanıp, her log kaynağı bir yöneticiye atanabilir. Her yönetici web ara yüzden giriş yaptığında kısıtlı menülere erişebilerek, sadece kendisine tahsis edilmiş log kaynağı ve kaynaklarına ait logları kontrol edebilir. Admin kullanıcısı ise,

Bu özellik, çoklu lokasyon/şube ve merkezi log toplama durumunda tavsiye edilir.

Bildirim

KLog Server, log alınamama, başarısız imzalama işlemi, disk alanı azalma, yeni log kaynağı tespit edilme vb. gibi sistem olaylarında eposta yoluyla bildirim yapmaktadır. Bu seçenekler Bildirim menüsünden ayarlanabilir.

Çoklu yönetici tanımlandığı durumda, bildirim, Admin kullanıcısına, cihaz sahibi olarak tanımlanan yöneticiye veya ikisine gönderilebilir.



Kamu SM Onaylı Zaman Damgası

KLog Server imzaladığı logların Kamu SM onaylı olduğunu, bu amaç için Kamu SM tarafından sunulan doğrulama aracı (Zamane) ile doğrulayabilirsiniz. TÜBİTAK BİLGEM tarafından geliştirilen Kamu SM Zamane, Zaman Damgası İstemci Yazılımı uygulaması ücretsiz olarak Kamu SM web sitesinden indirilebilir.

Daha fazla bilgi: www.klogserver.com