

KLOG SERVER

ELEKTRONİK ZAMAN DAMGASI ve LOG YÖNETİMİ ÇÖZÜMÜ

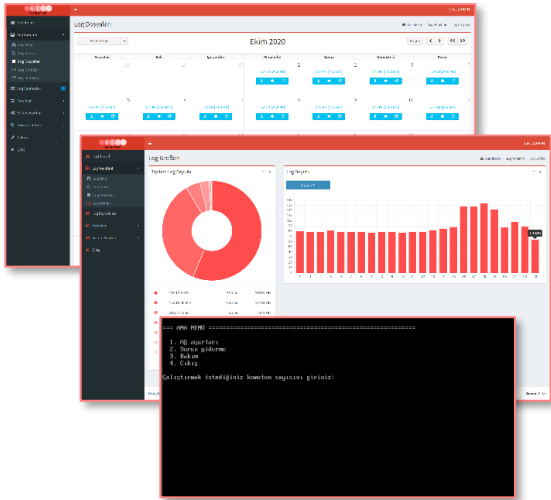
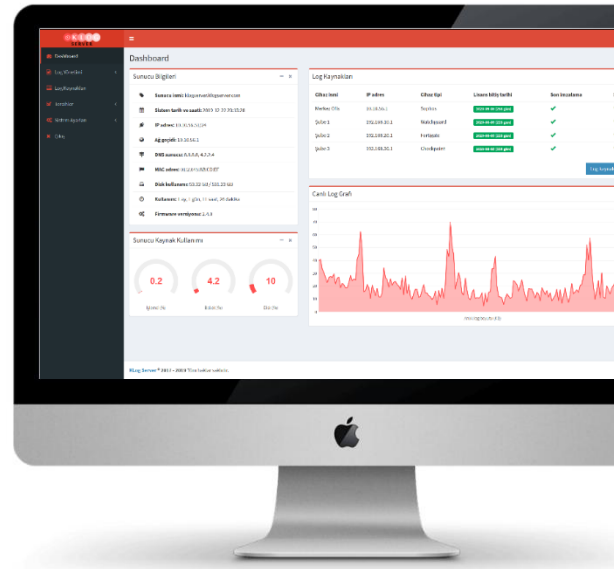
KLog Server

KLog Server, 5651 yasasına uygun zaman damgası hizmeti sağlayan bir Syslog sunucusudur. KLog Server, paylaşımlı klasörlerden ve AWS S3 ve Azure Files bulut platformlarından log toplama ve imzalama özelliklerine de sahiptir. Linux tabanlı olan KLog Server, VMware ve Microsoft Hyper-V platformlarıyla uyumlu, kullanıma hazır sanal bir makine olarak sunulmaktadır.

KLog Server, üretici bağımsız olarak, standart Syslog protokolü ile log üreten tüm cihazlarla (güvenlik duvarları, sunucular, vb.) entegre çalışır. Gün boyunca aldığı logları, her gün sonunda Kamu SM (Kamu Sertifikasyon Merkezi) onaylı bir sertifika ile elektronik olarak imzalar ve log dosyalarını imza dosyaları ile birlikte güvenle depolar.

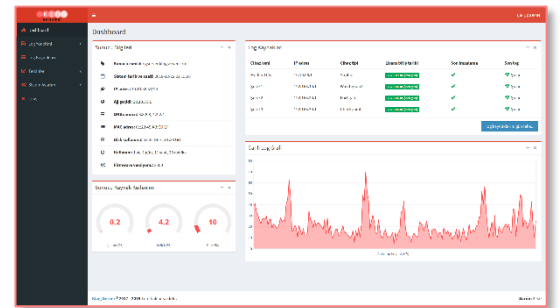
Özellikler

- Kamu SM onaylı SHA-512 karma algoritması ile imzalama özelliği sunar.
- Web tabanlı yönetim ekranı ve konsol arayüzüne sahiptir.
- Kolay kurulum ve yapılandırma imkanı sunar.
- Log üreten cihazları otomatik olarak algılar ve log toplamaya başlar.
- Paylaşılan klasörlerden (SMB) log toplama ve imzalama desteği bulunur.
- AWS S3 ve Azure Files platformlarından dosya toplama ve imzalama yapabilir.
- Anlık log izleme ve loglarda arama yapma özelliğine sahiptir.
- Alınan loglara dayanarak 300'den fazla kapsamlı grafik oluşturur.
- İmzalama durumunu Dashboard ekranından takip etme imkanı sunar.
- İmzalanmış loglar ve imza dosyaları web arayüzü üzerinden indirilebilir.
- Günlük olarak veya toplu şekilde imzalanmış logları FTP, SCP sunucusu, paylaşımlı klasör, AWS S3 veya Azure Files'a aktarabilir.
- Çoklu yönetici desteğiyle bayi/son kullanıcı yapılarına uyum sağlar.
- E-posta ile bildirim mekanizmasına sahiptir.
- Linux tabanlıdır ve yüksek stabiliteyle çalışır.



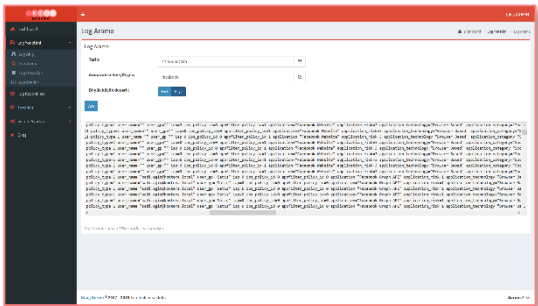
Dashboard Ekranı

Dashboard ekranı, sistem ve log alma/imzalama ile ilgili genel bilgileri tek bakışta 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 da görüntülenir. Dashboard ekranı, aynı zamanda her bir log kaynağı için canlı log boyutunu grafiksel olarak göstermektedir.



Log İçeriği İzleme ve Loglarda Arama

Alınan loglar, anlık olarak Log Akışı ekranından izlenebilir. Loglarda gelişmiş arama özelliği, imzalama bekleyen veya imzalanmış loglarda belirlenen log kaynağı, tarih, anahtar kelime veya Regex'e göre arama yapma imkanı sağlar ve sonuçlar web arayüzünde görüntülenir. Sık kullanılan arama anahtar kelimeleri ve ifadeleri, daha kolay kullanım için kaydedilebilir.



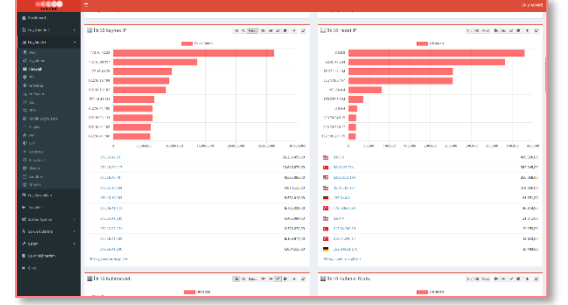
Log Analizi

Log analizi özelliği, toplanan log verilerini gerçek zamanlı görselleştirerek içgörüler sunar ve oluşum sayısı, veri hacmi, paket sayısı gibi metrikleri grafiklerle gösterir. Yöneticiler, çubuk, çizgi ve pasta grafik türleri arasında geçiş yapabilir. KLog Server, IP adresi, MAC adresi, kullanıcı, dosya, alan adı, URL, kural/ilke, gibi varlıkları otomatik tanıyarak, tek tıkla bu varlıklara ait log aktivitelerini bir arada sunar ve web, uygulama, güvenlik duvarı, VPN, kimlik doğrulama gibi log türleri arasında bütünsel bir bakış sağlar.

Her grafik, logları tablo formatında incelenebilmesi seçeneğini sunar. Tablolar anahtar kelimeye dayalı arama, sütun sıralama ve zaman aralığı filtreleme gibi özelliklerle geniş log verileri arasında gezinmeyi kolaylaştırır. Daha iyi bir anlaşılabilirlik sağlamak amacıyla, KLog Server IP adresleri ülke bayrakları ile eşleştirir ve MAC adresleri üretici ikonlarıyla etiketler.

Uzun vadeli veri yönetimi için, kullanıcı tanımlı saklama süresine göre otomatik veri temizleme, eski logların disk alanını doldurmasını önlemeye yardımcı olur.

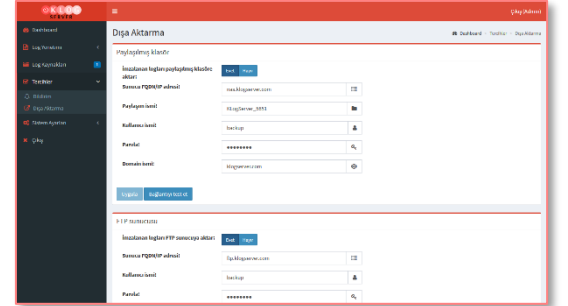
Bu özellikler sayesinde yöneticiler, ağ ve güvenlik verilerini daha etkin bir şekilde izleyebilir, analiz edebilir ve yönetebilir; olası sorunlara proaktif olarak yanıt verirken veri görünülüğünü ve erişilebilirliğini korur.



Log Dosyaları Dışa Aktarma

Günlük log dosyaları imzalandıktan sonra, imza dosyalarıyla birlikte otomatik olarak dışa aktarılabilir. Desteklenen harici depolama alanları FTP sunucusu, SCP sunucusu, paylaşımlı klasör, AWS S3 bucket ve Azure Dosyalar bulut platformlarıdır. Dışa aktarılan dosyalar, disk alanını kolaylıkla yönetmek için isteğe bağlı olarak silinebilir.

Günlük dışa aktarıma ek olarak, loglar toplu şekilde dışa aktarılabilir, web arayüzünden indirilebilir veya diskten silinebilir.

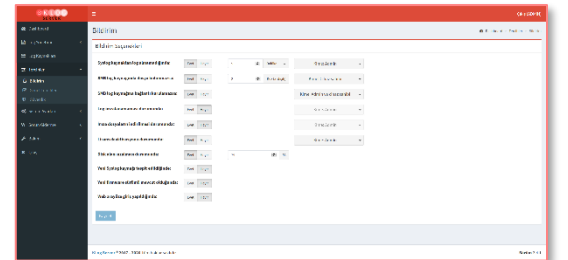


Çoklu Yönetici Yapısı

KLog Server, yönetici veya bayi/müşteri yapısına sahiptir. Bu sayede birden fazla kullanıcı hesabı tanımlanabilir ve her log kaynağı belirli bir kullanıcıya atanabilir. Her kullanıcı, web arayüzüne giriş yaptığında yalnızca kendisine tahsis edilen log kaynakları ve onlara ait logları yönetebilir, erişebileceği menüler ise kısıtlıdır. Admin kullanıcısı ise tüm kaynaklara erişim yetkisine sahiptir. Bu özellik, çoklu lokasyon/şube ve merkezi log toplama durumlarında hiyerarşi yönetimine imkan tanır.

Bildirim

KLog Server, log alınamaması, imzalama işleminin başarısız olması, disk alanının azalması, yeni bir log kaynağının tespit edilmesi gibi sistem olaylarında e-posta yoluyla bildirim yapar. Birden fazla yönetici tanımlandığı durumlarda bildirim, Admin kullanıcısına, kaynak sahibi olarak belirlenen yöneticiye veya her ikisine birden gönderilebilir.



Kamu SM Onaylı Zaman Damgası

KLog Server tarafından imzalanan logların Kamu SM onaylı olduğunu TÜBİTAK BİLGEM tarafından geliştirilen Kamu SM Zaman Damgası uygulaması ile doğrulayabilir ve her log dosyası için sertifika bilgilerini içeren beraat belgesini indirebilirsiniz.

Daha fazla bilgi: www.klogserver.com