Diagnose & secure your network

YATEM LogCollector®
Event Monitor™

Ne yapar?

Microsoft işletim sistemleri üzerinde kullanıcı faaliyetlerini, maliyet etkin ve dayanıklı bir "değişiklik izleme" imkanı sağlar.

Kim?
Ne Zaman?
Nerede?
Ne Yaptı?

Sistem yükü?

İşlemci ve ağ üzerinde neredeyse yokmuş gibi çalışır.

Rapor ve Sorgulama

Arayüz ve raporlar aradığınız bilgiye kolayca ulaşmanızı sağlar.

Hızlı, basit, sade

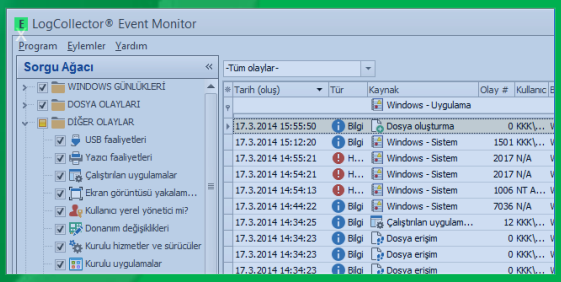
Kurulum sadece dakikalar alır. Ayarlarla sizi yormaz. Öğrenilmesi ve kullanılması basittir.

Kapsamlı ve dayanıklı

Ağınızın büyüklüğü, karmaşası ve hızı ne olursa olsun uzun süre sorunsuz çalışır.

Yasal Uyumluluk

5651 sayılı yasaya uyumluluğunuzu destekler.



"LogCollector Event Monitor", Microsoft işletim sistemine sahip bilgisayarlar üzerinde kullanıcıların faaliyetlerine yönelik bıraktığı sayısal izlerin toplanması, saklanması ve analiz edilmesini sağlayan bir yazılım çözümüdür. Böylece, ağdaki kullanıcı bilgisayarında oluşan teknik ve güvenlik sorunlarını gerçek zamanlı gözlemle zamanında saptamış olursunuz. Benzer şekilde, bu ortam, geçmişte oluşmuş ancak etkileri yeni ortaya çıkan sorunları da geriye doğru inceleme ortamını elinizde bulunmasını sağlamaktadır.

Temel Kazanımlar

- **Farkındalık sağlar.** Ağınızda olanları ilk fark eden siz olursunuz.
- **Yatırım maliyetlerinizin korur.** Değerli emek ve maliyetlerle oluşturduğunuz ağınızı ve kurumsal verilerinizi titizlikle korumanızı sağlayarak yatırımlarınızı düşük maliyet ve iş gücü ile korumanıza destek olur.
- **Kolay ve esnek raporlama sağlar.** Her türlü isteğinize uyum sağlayabilen karmaşık raporları dahi saniyeler içinde ve kolayca hazırlayabilirsiniz.
- **Sürdürülebilir güvenlik altyapısına destek verir.** Güvenlik politikalarınızın etkinliğinin korunması ve geliştirilmesinde gerçek zamanlı ve ön kestirimli bilgiler sunarak, sürdürülebilir bir güvenlik altyapısı kurulmasını sağlar.
- **Hazır ve özel raporlama olanağı sağlar.** Yazılım kutudan kullanıma hazır raporlar ile birlikte gelmektedir. Bunun yanında uyarı veya otomatik olarak kullanılabilecek özel raporlar hazırlamaya da olanak sağlamaktadır.
- **Ölçeklenebilir.** Yazılım ölçeklenebilir bir yapıda oluşturulmuştur. DC ve kullanıcı sayısının miktarına ve ağ iletişim yapısının durumuna uygun olarak değişik çalışma tekniklerini desteklemektedir.
- **Zaman kazandırır.** Sistem yöneticisine merkezi kontrol sağlaması nedeniyle zaman kazandırır.

Ne Yapabilirsiniz?

- "abc.doc" adlı dosyayı kimler yazdırdı?
- Son 7 gün içinde hangi bilgisayarlara, hangi yazılımlar yüklendi?
- Ağda USB depolama aygıtı kullanan kullanıcılar kimler?
- Ağdaki bilgisayarlarda, bilgi işlem merkezinin bilgisi dışında donanım eksiltmesi yapıldı mı?
- "K" kullanıcısı dün hangi yazılımları çalıştırdı?
- "K" kullanıcısı kendi bilgisayarında hangi dosyalara erişti?
- Kendi bilgisayarında "yerel yönetici" olarak çalışan kullanıcı var mı?
- Kendi bilgisayarında ağ kartı ayarlarını değiştiren kullanıcılar kimler?
- "K" kullanıcısı ağda nerelere bağlandı?
- Bilgisayarlarda sistem olay günlüğünde "kritik" olarak kayıtlanmış olaylar neler?

Özellikler

Genel

- **Lisanslama**: Sunucu ve kullanıcı başına lisanslama yapılmaktadır.
- **Veritabanı:** Toplanan veriler MS SQL veya PostgreSQL Server veritabanında saklanır.

Olay Toplama

- **Mimari:** Ajan tabanlı olarak çalışmaktadır.
- **Olaylar:** Olay bilgileri kural bazlı toplanmaktadır. Bunlardan bazıları:
  - Windows olay günlükleri
  - Dosya sistemi değişikliklerin izlenmesi (oluşturma, silme, yeniden adlandırma, taşıma vb.)
  - USB faaliyetleri
  - Yazıcı faaliyetleri
  - Ekran görüntüsü yakalama faaliyetleri
  - Çalıştırılan uygulamalar
  - Yerel yönetici denetimi
  - Donanım değişikliklerinin izlenmesi
  - Uygulama kurulum/kaldırımlarının izlenmesi
  - Ağ faaliyetleri
  - Ağ kartı ayarları değişikliği
  - Oturum faaliyetleri (açma, kapatma, kilitleme vb.)
  - Paylaşım faaliyetleri
- **Olay Detayı:** Her olay için, hangi kullanıcı (kim), hangi bilgisayarda (nerede), hangi nesne üzerinde (neyi), hangi zamanda (ne zaman), gerçekleştirdiği işlem (ne) bazında tespit edilmektedir. Nesneler üzerinde yapılan değişikliklerin önceki ve sonraki değerleri birlikte gösterilmektedir.
- **Gerçek Zamanlı Toplama:** Olay gerçekleştiği anda gecikmeksizin ajan tarafından kayıt altına almaktadır.
- **Çevrimdışı Çalışma:** Ajan yazılımı, ağ bağlantısının olmadığı durumlarda da gerçek zamanlı çalışmasını sürdürür, topladığı bilgileri korur, bağlantı sağlandığı anda merkeze aktarır. Böylece ağ kesinti halinde olay kaybı oluşmaz.
- **Ajan Koruması:** Ajan yazılımı ve topladığı veriler merkeze gönderilme öncesinde disk üzerine koruma altındadır. LogCollector dışında kullanıcıların müdahalesine ve erişime kapalıdır.
- **Ajan Performansı:** LogCollector ajanı, oluşan olayları kaçırmadan toplayarak işleyen güçlü ve sürekli geliştirilen takip motoruna sahiptir.
- **Ajan İzi:** LogCollector ajanı; CPU, bellek ve ağ kullanımında çok düşük profilli çalışma (footprint) özelliği ile benzerleri arasında oldukça iddialıdır.
- **Veri Bütünlüğünün Korunması:** Her kayıt, değişmezlik garantisini sağlamak maksadıyla olayın için olduğu yerdeki ajan tarafından hazırlanan MD5 özet (hash) bilgisi ile saklanmaktadır.

Olayların Sorgulanması, Analizi ve Raporlama

- **Gerçek Zamanlı Olay İzleme:** LogCollector, toplanan olayların gerçek zamanlı olarak izlenmesi, analizi, ekran ve yazıcı raporları alınabilmesi için güçlü bir arayüze sahiptir.
- **Dinamik Sorgular:** LogCollector görüntüleme arayüzü, veritabanında istenen verilere ulaşmak için dinamik sorgular oluşturmayı destekleyerek basit ve esnek arayüzlere sahiptir.
- **Sorgu Performansı:** LogCollector, veritabanından biriken çok miktarda veri üzerinde oldukça hızlı analiz ve inceleme yapma olanağı sağlar.
- **Hazır Sorgu ve Raporlar:** Arayüz üzerinde, önceden hazırlanmış çok sayıda sorgu, rapor ve grafikler raporlar yer almaktadır.
- **Etkileşimli Grafiksel Analiz –** Ara yüzler üzerinde görülen tablosal veriler grafik olarak ta görülebilir ve üzerinde çok seviyeli ayrıntıya inme (drill down) analizleri yapılabilir.
- **Veri Aktarma:** Ekranda görüntülenen veri ve raporları metin, PDF, CSV/Excel, HTML, ve XML biçiminde dışarıya aktarılabilmektedir.
- **Otomatik Raporlar:** Raporların zamanlı ve otomatik olarak hazırlanarak (PDF, Excel, metin vb.) disk üzerinde saklanması ve/veya belirtilen adreslere e-posta ile gönderilmesi mümkündür.
- **Otomatik Uyarılar (alarm):** Belirlenecek koşullara uygun olay oluşması durumunda istenen adreslere uyarı (e-posta) gönderme özelliğine sahiptir.

Yönetim

- LogCollector, izleme yapılacak bilgisayarlara ajanların kurulması, kaldırılması ve durumlarının gerçek zamanlı olarak izlenmesi için merkezi yönetim arayüzüne sahiptir.

Arşivleme

- LogCollector, veritabanında belirli bir zaman öncesine ait verilerin arşivlenmesi için bir arayüze sahiptir.
- Arşivleme elle veya zaman dayalı otomatik olarak yapılabilir.
- Arşivlenen verileri çevrimdışı olarak analiz etmek için aynı arayüz kullanılabilmektedir.

Sistem Gereksinimleri

Merkezi Sunucu Bilgisayarı:

- CPU: 2 GHz Pentium veya üstü
- İşletim sistemi: Microsoft Windows 7 ve sonrası
- Bellek: 1 GB+
- Microsoft SQL Server 2008+ veya PostgreSQL 9+
- Disk alanı: 100 MB+ kurulum için. Veriler için yeteri kadar.

Ajan Kurulumu:

- İşletim sistemi: Windows 7 ve sonrası
- Disk alanı: 100 MB+

yatem yazılım teknolojileri merkezi

YATEM Bilişim ve Teknoloji Sistemleri A.Ş.
E-posta: yatem@yatem.com.tr
Tel : +90 (312) 479 4088 Faks: +90 (312) 479 4088
http://www.yatem.com.tr

YETKİLİ DİSTRİBÜTÖR

Belge kodu: B-LC-EVENTMON-R6-3