Progress® WhatsUp®

WhatsUp® Log Management

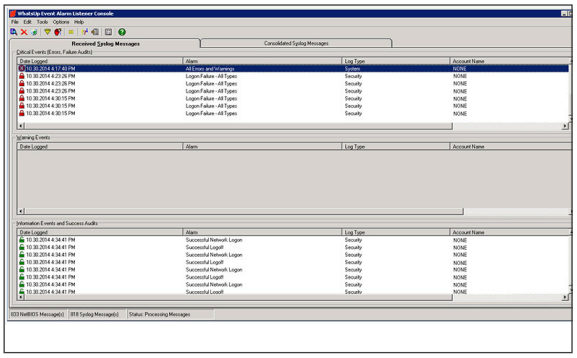
Log Management Suite für WhatsUp Gold

Protokolldateien enthalten eine Fülle von Informationen, mit deren Hilfe sich Organisationen vor Angreifern, Malware, Schaden, Verlust und rechtlichen Konsequenzen schützen können. Protokolldateien müssen in Echtzeit erfasst, gespeichert, verschlüsselt, analysiert und überwacht werden, damit Sie europäische Datenschutzauflagen, wie das Bundesdatenschutzgesetz oder die britischen und französischen Datenschutzgesetze, einhalten können. Es ist jedoch unmöglich, Protokolldateien ohne die richtigen Tools zu überwachen, da die Protokolldateien von vielen verschiedenen Quellen in unterschiedlichen Formaten und in riesigem Umfang erzeugt werden.

WhatsUp Log Management Suite – Übersicht

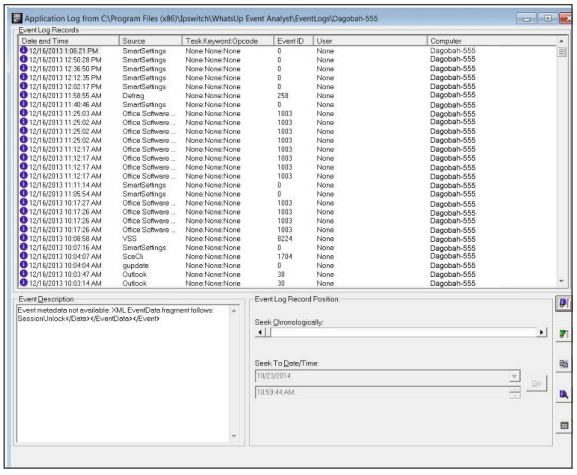
WhatsUp Log Management sorgt automatisch für die Erfassung, Speicherung, Überwachung und Analyse von Syslog-Protokollen, Windows-Ereignisprotokollen oder W3C-Protokollen, die von Webanwendungsservern, Lastenausgleichsmodulen, Firewalls, Proxyservern oder Content-Sicherheitsanwendungen erstellt werden, und erstellt Berichte zu diesen.

Event Archiver:
Ermöglicht die Erfassung, Bereinigung und Konsolidierung von Protokolldaten. Sehr hilfreich zur Einhaltung von Prüfungs- und Compliance-Richtlinien.



Event Alarm:
Überwachen Sie Protokolldateien und erhalten Sie Benachrichtigungen bei wichtigen Ereignissen. Sehr hilfreich für Intrusion-Detection und zur Überwachung von Aussperrungen durch den Domänencontroller, oder Datei- und Ordner-Zugriff.

Event Analyst:
Ermöglicht die Analyse von Protokolldaten und –trends, und die Berichterstellung zu diesen. Verteilen Sie automatisch Berichte an das Management, Sicherheitsverantwortliche und Prüfer.



Event Rover:
Bietet eine einfache Ansicht zur detaillierten Forensik über alle Server und Workstations, so können Sie Ihre Effizienz steigern und Zeit sparen.

AUSGEZEICHNET MIT DEM CERTIFICATE OF NETWORTHINESS (CON) DER U. S. ARMY: CERT #201004611
Uneingeschränktes Vertrauen, dass die WhatsUp Gold-Produktfamilie die strengen Anforderungen an Sicherheit, Zukunftsfähigkeit und Interoperabilität erfüllt.

UNTERSTÜTZT DIE FORMATE EVT UND EVTX
In einer heterogenen Umgebung generierte Windows-Ereignisse auf einer Konsole öffnen und zueinander in Bezie- hung setzen – 2008 und höher, XP, Vista, Server 2003, NT 4.0.

ABGESTUFTES „PRO SERVER/ WORKSTATION“
Preismodell zur einfacheren Budgetier- ung – Sie müssen nicht nachverfolgen, wie viele Protokolldaten generiert werden, und es gibt keine versteckten Kosten, wenn die Anzahl Ihrer Protokolldateien steigt.

ENTHÄLT PATENTIERTE LOG HEALER-TECHNOLOGIE
Unsere Software kann beschädigte Microsoft EVTX-Ereignisprotokolle verarbeiten und sogar reparieren.

Progress® WhatsUp®

- **MINIMIEREN SIE RISIKEN** überwachen und schützen Sie den Zugriff auf geschäftskritische Daten, weisen Sie die Einhaltung der europäischen Datenschutzgesetze mit integrierter Point-and-Click-Berichtsfunktion nach
- **SCHÜTZEN SIE ARCHIVIERTE** Protokolle durch kryptografisches Hashing (entscheidend für die Verwendung als Beweismittel)
- **IDENTIFIZIEREN SIE UNAUTORISIERTE** Ereignisse sofort (z. B. den Zugriff auf Ordner mit sensiblen Daten)
- **ERFASSEN UND VERSCHLÜSSELN** Sie Syslog-, Windows-Ereignis- oder W3C/IIS-Protokoll- dateien aus der gesamten Infrastruktur
- **SPEICHERN SIE PROTOKOLLDATEN** so lange wie nötig – mehrjährige Speicherfunktionen von Daten erleichtern Ihnen die Einhaltung europäischer Datenschutzauflagen
- **ANALYSIEREN UND EXTRAHIEREN** Sie die richtigen Informationen aus Tausenden von Protokolleinträgen
- **FERN- & AGENTEN-BASIERTE ERFASSUNG** von Syslog, W3C/IIS und Windows-Ereignis-Dateien. Log Management ist an Ihre Netzwerk-Sicherheitsrichtlinien anpassbar, vereinfacht Konfigurationsaufgaben und spart Zeit.

Jetzt können sich IT-Betriebe und Sicherheitsbeauftragte darauf verlassen, dass die WhatsUp Log Management Suite nicht nur jedes Ereignis erfasst und dokumentiert, sondern auch folgende Leistungen erbringt:

- Umfassenden Einblick in interne und externe Sicherheitsbedrohungen
- Automatische Erfassung von Syslog-, W3C/IIS- oder Windows Ereignis-Protokollen aus der gesamten Infrastruktur
- Point-and-Click-Berichte für die wichtigsten europäischen Datenschutzgesetze wie das Bundesdaten- schutzgesetz, den U.K. Data Protection Act oder das französische Gesetz über die finanzielle Sicherheit
- Schutz von archivierten Protokolldaten vor Manipulation durch kryptografisches Hashing – entscheidend für die Verwendung als Beweismittel
- Möglichkeit, Ereignisse aus verschiedenen Quellen in einer einzigen Gesamtansicht in Beziehung zueinander zu setzen
- FIPS 140-2-Verschlüsselung und -Validierung – das höchste Verschlüsselungslevel
- Echtzeitdatenansicht, -status und –warnfunktion
- Einfaches und schnelles Finden und Beheben von Fehlerereignissen
- Einhaltung von gesetzlichen Richtlinien zu einem reduzierten Preis

Mehr Informationen und eine kostenfreie Testversion finden Sie unter:
https://de.ipswitch.com/formulare/testversionen/log-management