

Einfache und schnelle Logdaten-Archivierung mit zentraler Speicherung und Auswertung

Die neuen tacLOGHosts 2100 und 2200 von terreActive bieten eine leistungsfähige und preiswerte Lösung für das zentrale Logdaten Management.

Highlights

- **Kosten sparen:** Lizenzierung pro Appliance mit unlimitierter Anzahl Logclients
- **Normalisierung:** zentrale Speicherung unterschiedlicher Logclients
- **„Google your logs“:** noch nie war Logdaten Analyse so schnell
- **Beweissicherung:** durch Speicherung und Schutz der originalen Logdaten
- **Hohe Performanz:** empfangen von über 15'000 Logmessages pro Sekunde
- **Nachhaltig:** einfache Erweiterung zur umfassenden SEM-Lösung

"Listen to your Logs"



Logdaten sind eine wertvolle Informationsquelle in jedem Unternehmen. Der immer stärker werdende Einfluss von Informationstechnologie auf die Geschäftsprozesse der Unternehmen, führt zu einer wachsenden Abhängigkeit von den IT-Infrastrukturen.

Gleichzeitig nimmt die Logdaten Menge ständig zu, was zu einer eigentlichen Datenflut geführt hat. Logdaten müssen als wertvolle Informationsquellen erachtet werden um die Qualität und Sicherheit des IT-Betriebs zu verbessern.

Transparenz und Kontrolle über die IT-Infrastrukturen sind die Ziele beim zentralen Logdaten Management. Alle Unternehmen können davon profitieren.

Logdaten Management ein Muss

Neben den erwähnten Vorteilen, stehen beim Entscheid für ein aktives Logdaten Management auch immer mehr regulatorische Anforderungen (Compliance) im Vordergrund. Vorgaben von Gesetzgebern und Auditoren verlangen von einem Unternehmen, dass es sich durch lückenlose Beweissicherung und starke Kontrollmechanismen vor Missbrauch der IT-Systeme schützt. Hier stehen wichtige Funktionen wie Archivierung von grossen Mengen von Logdaten im Originalformat und deren Schutz vor Veränderung im Vordergrund. Aber auch die schnelle Auswertung grosser Datenmengen für die Erkennung von Sicherheitsvorfällen oder Betriebsproblemen müssen gewährleistet sein.

All diese Anforderungen sind nun in einer kompakten und kostengünstigen Appliance integriert und in Form des tacLOGHost auch schon für kleine IT-Infrastrukturen sinnvoll einsetzbar.



Hauptfunktionen

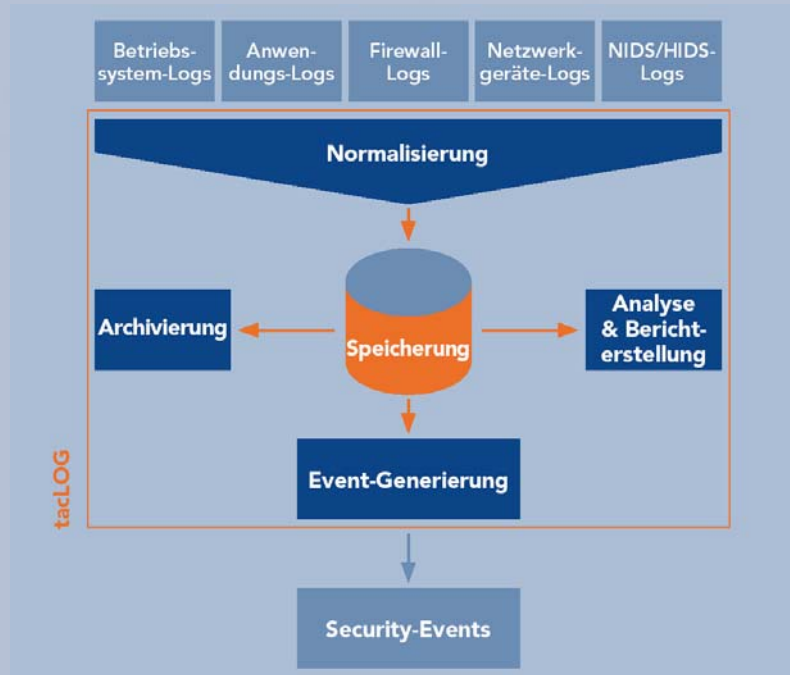


Abbildung 1: Funktionsübersicht

Normalisierung:

- breite Unterstützung von Logclients unterschiedlicher Hersteller

Archivierung:

- für die Beweissicherung, den Integritätsschutz und die Nachvollziehbarkeit

Analyse & Berichterstellung:

- über benutzerfreundliches Web-Interface (siehe Beispiel auf Abbildung 2)
- einfache und schnelle grafische Darstellung von grossen Logdaten Mengen

Event-Generierung:

- Alarmierung von vordefinierten Events



Abbildung 2: Grafisches Web-Interface



Szenarien für den Einsatz von tacLOGHost

Der tacLOGHost ist für den punktuellen Einsatz in einer Sicherheitszone (DMZ etc.), die umfassende Überwachung wichtiger Applikationen (E-Business, ERP etc.) und in mittleren IT-Infrastrukturen gedacht. Überall wo grosse Logdaten-Volumen entstehen, welche archiviert, korreliert und ausgewertet werden sollen, ist der Einsatz des tacLOGHosts ein Muss.

Für die folgenden Szenarien wurde der tacLOGHost entwickelt und ständig weiter optimiert:

Archivierung und Gewaltentrennung:

Die schnelle und kostengünstige Archivierung von grossen Datenmengen bedingt eine entsprechende Architektur. Die spezielle RIT-Technologie macht den tacLOGHost besonders performant. Der eingebaute Schutz vor Veränderung der originalen Logdaten erlaubt die Beweissicherung und garantiert gleichzeitig die wichtige Gewaltentrennung. Die Logdaten auf dem tacLOGHost sind durch die Systemverantwortlichen der Logclients nicht mehr manipulierbar und können von einer unabhängigen internen oder externen Stelle betreut werden.

Audittrail:

Hier geht es in erster Linie um Nachvollziehbarkeit und Beweissicherung. Die Anzahl der Audits hat in vielen Unternehmen stark zugenommen. Der Aufwand ist enorm und benötigt immer mehr Ressourcen. Deshalb unterstützt der tacLOGHost diese Aufgabe durch eine Vielzahl von Funktionen. Der Zugriff auf die Logdaten kann über Rollen und Gruppen genau bestimmt werden und erlaubt es berechtigten Personen Informationen zu überprüfen, ganz ohne Zugriffsrechte auf die Logclients. Reports sind vordefiniert und über ein Web-Interface können beliebige Auswertungen (Views) und Filter definiert werden, um schnell zu den gewünschten Informationen zu gelangen.

IT-Sicherheits Monitoring:

Durch die Realtime-Auswertung aller ankommenden Logdaten kann ein bekannter Event sofort erkannt und entsprechend alarmiert werden. Die mitgelieferten Tools erlauben ein sogenanntes "baselining" um das typische Verhalten der eigenen IT-Infrastruktur besser kennen zu lernen und zu überwachen. Durch diese Tools ist es auch möglich Abweichungen vom Normalverhalten schnell und sicher zu erkennen und diese Vorfälle gezielt zu untersuchen. Das System kann durch die Erweiterung der Event- und Alarm-Erkennung ständig ausgebaut werden, was auch die IT-Sicherheit laufend erhöht.

Operation Monitoring:

Was für die IT-Sicherheit gilt, stimmt auch für den IT-Betrieb. Mit dem gleichen Vorgehen ("baselining") kann das Betriebsverhalten der IT-Infrastruktur aufgezeichnet und visualisiert werden. Dabei werden nicht nur Konfigurationsfehler schnell sichtbar, sondern auch auftretende Fehlermeldungen aller Art können erkannt und für das proaktive Monitoring verwendet werden. Dies verbessert die Transparenz und erhöht die Betriebsqualität.

Ausbau zur umfassenden SEM/Monitoring-Lösung:

Der tacLOGHost kann einfach zur firmenweiten Security Event Management-Lösung, kurz SEM-Lösung, erweitert werden. Der Ausbau erfolgt über die Verteilung der Software-Module auf einzelne Appliances. Dies erhöht nicht nur die Performance, sondern erlaubt es auch über Sicherheitszonen oder mehrere Standorte hinweg Logdaten zu sammeln und zentral auszuwerten. Zusätzlich kann über die terreActive Monitoring-Lösung tacMON eine kombinierte Monitoring/SEM-Lösung aufgebaut werden.



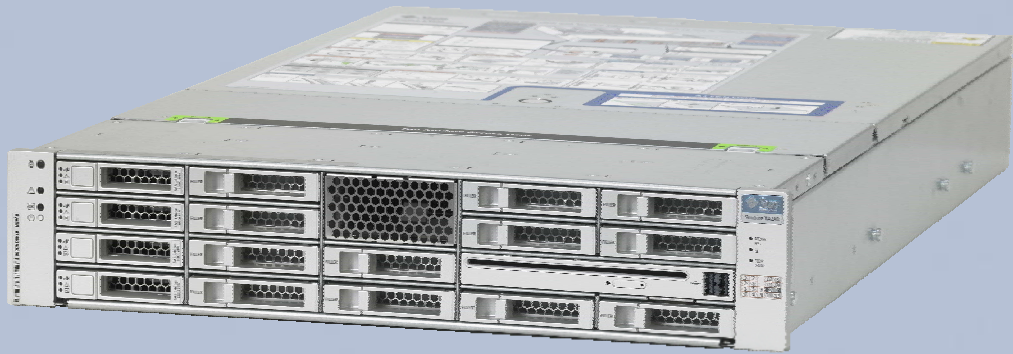


Abbildung 3: tacLOGHost

Technische Daten

tacLOGHost 2100

- Management: Web-GUI und Command Line Interface (CLI)
- Input: Syslog, File, Opsec, SNMP-Trap, Mail, Eventreporter etc.
- Input Performanz: > 15'000 Logzeilen pro Sekunde
- Event Generierung: > 500 Events pro Sekunde
- CPU: 1 AMD oder Intel
- RAM: 4 GB (ausbaubar auf max. 16 GB)
- Chassis: 2U rack mountable appliance
- Datenhaltung: System 73 GB RAID-1 und Daten 147 GB RAID-1 ausbaubar; bis 300 GB RAID-1 in unkomprimiertem Zustand und Archivierung bis 5 TB RAID-1 in komprimiertem Zustand
- Power: redundante Netzteile
- Interfaces: 2 x 1 Gbit Netzwerkinterfaces

tacLOGHost 2200

wie 2100 aber mit:

- CPU: 2 AMD oder Intel
- RAM: 8 GB (ausbaubar auf max. 16 GB)

Über terreActive AG

terreActive ist Ihr Vertrauenspartner für umfassende und nachhaltige IT-Sicherheit.

terreActive ist ein unabhängiges Schweizer Unternehmen, das 1996 gegründet wurde und sich seither auf IT-Sicherheit spezialisiert hat. Dabei beschäftigen sich die 25 Mitarbeiter, hauptsächlich Ingenieure, mit Beratung, Integration und Betrieb von sicherheitsrelevanten Informatik-Systemen. Als Managed-Security-Service-Anbieter kann terreActive auch Ihre Sicherheit rund um die Uhr garantieren.

Zu den Kunden von terreActive zählen namhafte Firmen unter anderem aus Finanzwirtschaft, Verwaltung und Industrie.

Detaillierte Angaben über die Produkte und Dienstleistungen können im Internet unter <http://www.terreActive.ch/> entnommen werden.

