

Wir  Lebensmittel.

Brauche ich ein Database Activity Monitoring?

DOAG SIG Monitoring | 26.06.2018 | Sebastian Kilchert | Lunar GmbH





- EDEKA steht seit über 100 Jahren für das genossenschaftliche Prinzip der Eigenverantwortung
- Kerngeschäftsfeld ist das von rund 3.800 selbstständigen Unternehmern geführte Vollsortimentsgeschäft
- Zweite Säule: Netto Marken-Discount



Daten & Fakten 2017

- EDEKA ist ausschließlich in Deutschland aktiv
- 7.227 EDEKA-Märkte & 4.200 Netto Marken-Discount-Filialen
- bis zu 50.000 Produkte
- 12 Mio. Kundenkontakte täglich
- 369.300 Mitarbeiter
- 17.150 Auszubildende in rund 40 Ausbildungsberufen
- 58 Existenzgründer
- das größte Markenartikelsortiment im deutschen Handel



Die LUNAR GmbH...

- beeinflusst maßgeblich die IT-Strategie der EDEKA-Verbund
- ist der IT-/Prozessdienstleister in der EDEKA-Verbund
- realisiert und betreut innovative Templatelösungen
- verzahnt die Prozesse des Einzel- und Großhandels sowie der EDEKA-Zentrale
- deckt diverse IT-Leistungen für die EDEKA-Verbund ab
- beschäftigt ca. 600 MitarbeiterInnen an den Standorten Mannheim und Hamburg

01 Was ist ein Database Activity Monitoring (DAM)?

02 Welche Vorteile bringt mir ein Database Activity Monitoring (DAM)?

03 Übersicht/Unterschiede von drei größeren Anbietern

01 Was ist ein Database Activity Monitoring (DAM)?

02 Welche Vorteile bringt mir ein Database Activity Monitoring (DAM)?

03 Übersicht/Unterschiede von drei größeren Anbietern

Was ist ein DAM?

DAM = *Database Activity Monitoring*

Ich überwache doch schon
meine Datenbank!

Noch ein Monitoring?
Ich hab doch schon ein
SYSLOG-Server & SIEM



Brauche ich da wieder einen
Agenten auf dem Server?

Database Activity
Monitoring ?

**Auditing oder Security-Maßnahmen bringen
ohne entsprechendes Monitoring nichts!**

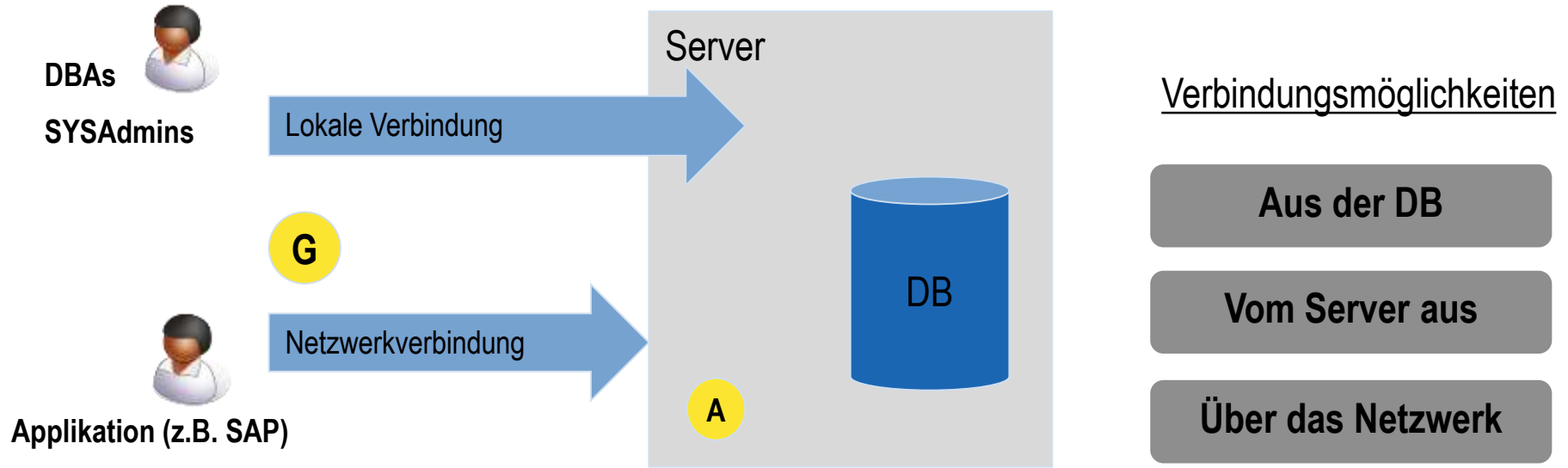
Wie unterscheidet sich ein „DAM“ von einem „normalen“ Monitoring?



-  Normales Monitoring z.B. Nagios, Patrol, OpenView oder check_mk u.v.m.
-  Database Activity Monitoring z.B. McAfee, Imperva, Oracle

Was ist Database Activity Monitor

- Kombiniert Auditing (Protokollierung) und Firewall/Alerting für die DATENBANK
- Sinnvolle und wichtige Ergänzung zu anderen Sicherheitsprodukten
- Dient der Sichtbarkeit und dem Aufdecken von Auffälligkeiten oder Angriffen
- Aktives Einwirken möglich
- Agent- und/oder Netzwerkbasierend
- Zugriffe auf Objekte für alle Benutzerarten einschränkbar
- Abgrenzung von Verantwortungsbereichen möglich
- Auswertung/Reporting bzw. Analysemöglichkeiten
- Generell für die gängigsten Datenbanken verfügbar
- Zusätze Sicherheitsprüfungen (Compliance Checks) möglich



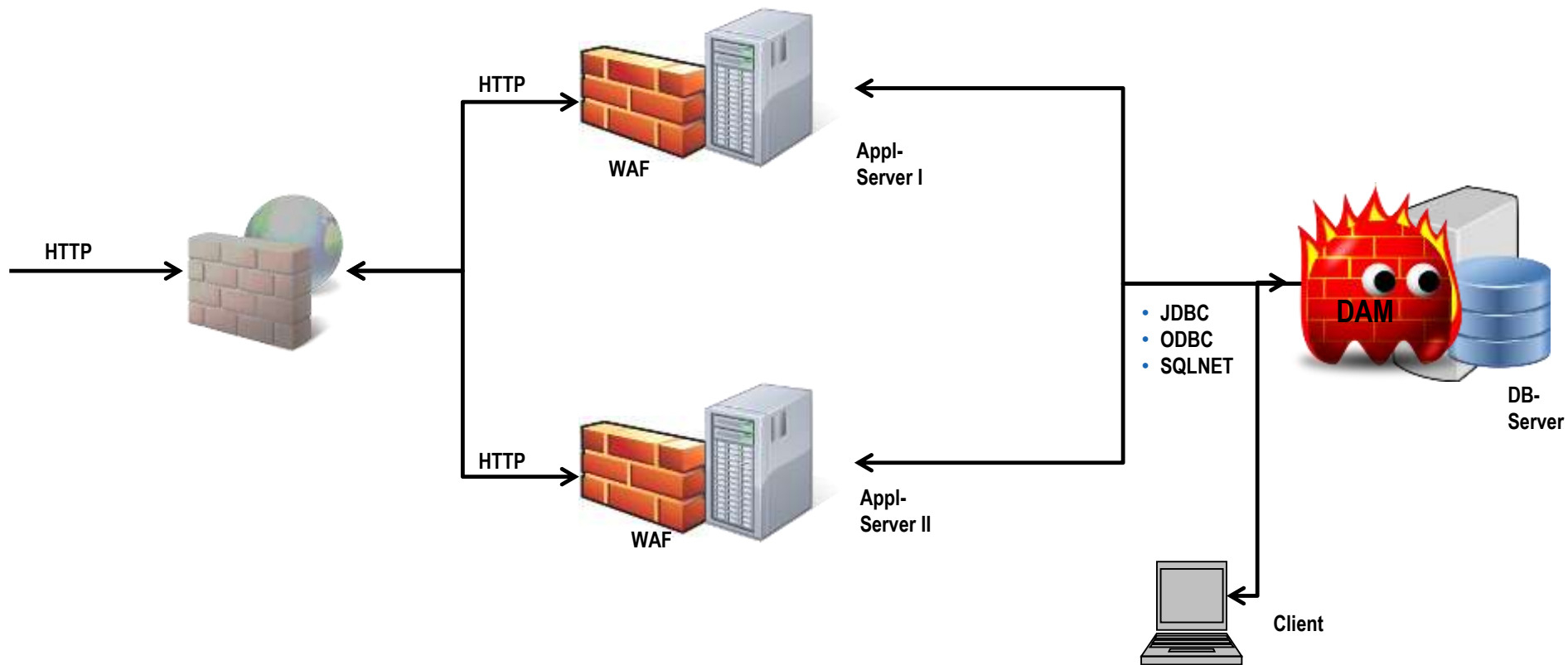
G = Gateway

A = Agent

Unterschiede DAM, Syslog-Server und WAF (Web Application Firewall)

Database Activity Monitoring	Syslog-Server	Wep Application Firewall
Kann Angriffe mitbekommen, bevor sie in der Datenbank ausgeführt werden	Bekommt die Informationen erst wenn Sie passiert sind	Sitzt zw. Client und Applikationsserver
Kann aktiv einwirken und ggf. Session beenden oder ins Leere laufen lassen	Kann nicht direkt Angriffe verhindern	Firewall für Webanwendungen – Nicht für Datenbanken
Kann Konfigurationen gegen einen „Standard“ prüfen (Compliance)	-	Für statische Requests geeignet
Zieht Daten direkt über den Agent und/oder im Netzwerk ab. Braucht größtenteils keine/wenig extra Mechanismen	Oftmals müssen extra Logging etc. eingeschaltet werden	
Dient einer revisionssicheren Protokollierung		
Versteht die SQL-Sprache und kann somit verdeckten Angriffen zuvor kommen		

Kombination DAM & WAF empfohlen!



01 Was ist ein Database Activity Monitoring (DAM)?

02 Welche Vorteile bringt mir ein Database Activity Monitoring (DAM)?

03 Übersicht/Unterschiede von drei größeren Anbietern

In der Regel sind Daten in Datenbanken gespeichert...



Geschäftsinteressen

- Schutz vor gezielten Angriffen
- Schutz der geschäftskritischen Daten
- Verfügbare Systemabläufe

Betrieb

- Verfügbarkeit der Datenbanken
- Änderungsnachvollziehbarkeit
- Schutz der Datenbanken

Compliance & rechtl. Verpflichtungen

- Schutz sensibler Daten
- Schutz vor Datendiebstahl
- Ggf. grenzüberschreitender Datenverkehr

Zugangskontrolle (Zutrittskontrolle)

- Meistens kein DB Thema

Zugangskontrolle

- ✓ Zuordnung Benutzerrechte
- ✓ Passwortvergabe
- ✓ Authentisierung
- ✓ Protokollierung
- ✓ Einsatz IDS
- ✓ Erstellung Benutzerprofilen
- ✓ Einsatz Firewalls

Datenträgerkontrolle (Weitergabekontrolle)

- ✓ Anonymisierung vor Weitergabe
- ✓ Kontrolle der Zugriffsberechtigungen von Datenträgern

Speicherkontrolle (ehem. Teil der Zugriffskontrolle)

- ✓ Verschlüsselung von Datenträgen
- ✓ Protokollierung
- ✓ Protokollierung von Zugriffen
- ✓ Rechteverwaltung

Benutzerkontrolle (Weitergabekontrolle)

- ✓ Übersicht der Abrufe
- ✓ Anonymisierung vor Weitergabe
- ✓ Rechteverwaltung

Zugriffskontrolle

- ✓ Protokollierung von Zugriffen
- ✓ Verschlüsselung von Datenträgen
- ✓ Rechteverwaltung
- ✓ PW-Konzepte/Richtlinien

Übertragungskontrolle (Weitergabekontrolle)

- ✓ Protokollierung von Zugriffen

Eingabekontrolle

- ✓ Protokollierung, Wer hat wann, was gemacht
- ✓ Vergabe von Rechten

Transportkontrolle (Weitergabekontrolle)

- ✓ Anonymisierung vor Weitergabe
- ✓ Netzwerkverschlüsselung
- ✓ Integritätsprüfung

Wiederherstellbarkeit (Neu)

- ✓ Backup & Recovery Tests
- ✓ Hochverfügbarkeit

Zuverlässigkeit (Neu)

- ✓ Monitoring von Fehlern
- ✓ Hochverfügbarkeit

Datenintegrität (Neu)

- ✓ Protokollierung
- ✓ Bildung von HASH-Werten

Auftragskontrolle

- ✓ Sicherstellung der Vernichtung von Daten nach Auftrag
- ✓ Laufende Überprüfung des Auftragsnehmers
- Meistens kein reines DB Thema

Verfügbarkeitskontrolle

- ✓ Testen Datenwiederherstellung
- ✓ Aufbewahrung Datensicherung an sicheren Ort
- ✓ Backup & Recovery
- ✓ Protokollierung / Monitoring von Fehlern
- ✓ Hochverfügbarkeit

Trennungsgebot

- ✓ Physikalisch getrennte Speicherung
- ✓ Versehen Datensätze mit Zwecktrennung Attribute
- ✓ Mandantentrennung
- ✓ Verschlüsselung von Datensätzen
- ✓ Pseudonymisierung
- ✓ Trennung Prod. und Test-Umgebung
- ✓ Separate Tabelle, getrennte DBs

*TOM = technisch und/oder organisatorische Maßnahmen

**Blau gefärbter Text = Erfüllte TOMs durch DAM-Einsatz

Vorteile eines Database Activity Monitorings (1)

- DAM ist Auditing und Alerting mit Weiterleitungsfunktion an einen SIEM und/oder Syslog-Server
- DAM wertet das Ergebnis des „Execution Plans“ aus bzw. versteht SQL
 - Es sieht somit, was wirklich passiert
- Unterschiedliche Datenbankhersteller werden unterstützt mit einer zentralen Lösung
- DAM bietet einen direkten Schutz der Datenbanken, während Firewalls und Network Security die Infrastruktur schützen. DAM kann als "letzte" Verteidigungslinie betrachtet werden
- Minimierung des Risikos der Haftbarkeit, in dem man Angriffe sofort erkennt
- Eigene Compliance-Regeln können erstellt werden
- Im Zweifel fachgerechte Beurteilung und ggf. Eingreifen durch den DBA statt nur im Nachgang durch Analyse

Vorteile eines Database Activity Monitorings (2)

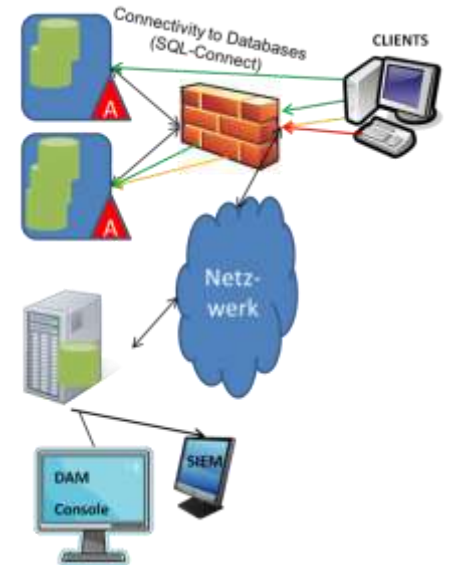
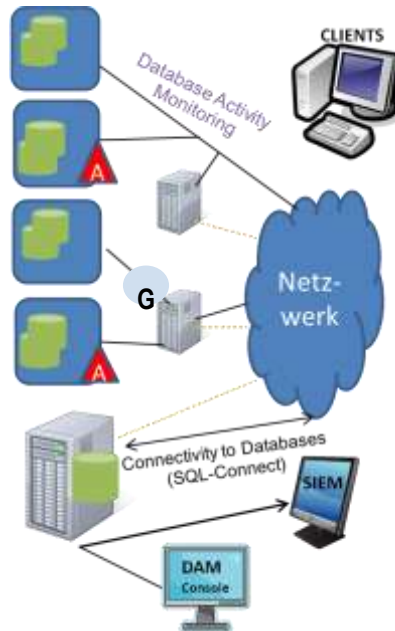
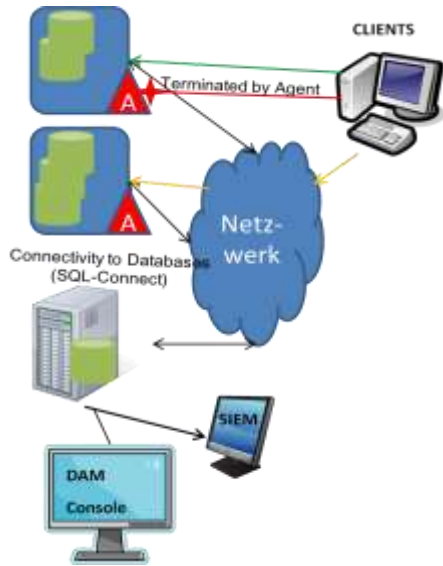
- DBA's und andere User können von den Applikationsdaten ferngehalten werden
- Absicherung der DBAs durch die Protokollierung (Auditing)
- unerlaubte Zugriffe auf die Applikationsdaten können protokolliert werden
- geringer Einfluss auf die Performance
- einfache Formulierung der Monitoring Regeln
- hunderte mögliche Regeln können definiert werden
- umfangreiche Reporting Möglichkeiten
- große Infrastrukturen werden unterstützt (skalierbar)
- Oft kann ein DAM mit weiteren Komponenten des Herstellers aufgestockt und ergänzt werden
- Oft sind zusätzliche Prüfungen und Scans durch's DAM möglich

01 Was ist ein Database Activity Monitoring (DAM)?



02 Welche Vorteile bringt mir ein Database Activity Monitoring (DAM)?

03 Übersicht/Unterschiede von drei größeren Anbietern





Unterstützte DB-Plattformen der Anbieter

	 McAfee™ Together is power.	 IMPERVA®	ORACLE
Oracle	✓	✓	✓
MySQL	✓	✓	✓
Microsoft SQL Server	✓	✓	✓
DB2	✓+	✓+	✓+
SYBASE	✓	✓	✓
TERADATA	✓	✓	
Maria DB	✓	✓	
PostgreSQL	✓	✓	
Progress OpenEdge		✓	
IBM Informix, Netezza		✓	
SAP HANA	✓	✓	

Die Ansicht, Menüführung und Steuerung der Konsolen ist Geschmackssache....





A screenshot of the McAfee console showing system status and configuration options. The interface includes a navigation menu and a main content area with various settings.

```
14:32:59 SYS@XE> grant dba to dd;
grant dba to dd
ERROR at line 1:
ORA-00028: your session has been killed
14:33:34 SYS@XE>
```

A screenshot of an Oracle alert log showing system details and error messages. The log includes information about the database instance, user, and a specific error.

A screenshot of the Oracle Enterprise Manager console showing a list of databases and their configurations. The interface includes a tree view and a main content area with various database details.

Date and Time	Source IP	Status	Destination IP	Service	Source Application	Event
June 10, 2018 10:44:48 PM	192.168.1.10	ERR	21.11.192.10	Oracle Database
June 10, 2018 10:44:48 PM	192.168.1.10	ERR	21.11.192.10	Oracle Database
June 10, 2018 10:44:48 PM	192.168.1.10	ERR	21.11.192.10	Oracle Database
June 10, 2018 10:44:48 PM	192.168.1.10	ERR	21.11.192.10	Oracle Database
June 10, 2018 10:44:48 PM	192.168.1.10	ERR	21.11.192.10	Oracle Database
June 10, 2018 10:44:48 PM	192.168.1.10	ERR	21.11.192.10	Oracle Database
June 10, 2018 10:44:48 PM	192.168.1.10	ERR	21.11.192.10	Oracle Database
June 10, 2018 10:44:48 PM	192.168.1.10	ERR	21.11.192.10	Oracle Database
June 10, 2018 10:44:48 PM	192.168.1.10	ERR	21.11.192.10	Oracle Database
June 10, 2018 10:44:48 PM	192.168.1.10	ERR	21.11.192.10	Oracle Database

A screenshot of the Oracle console showing a list of databases and their configurations. The interface includes a tree view and a main content area with various database details.

A screenshot of the Oracle console showing a list of databases and their configurations. The interface includes a tree view and a main content area with various database details.

A screenshot of the Oracle console showing a list of databases and their configurations. The interface includes a tree view and a main content area with various database details.

- Definieren Sie die Systeme / Datenbanken die geschützt werden sollen
- Definieren Sie die Plattformen für Betriebssystem / Datenbank
- Prüfen Sie die Voraussetzungen für Compliance Checks
- Definieren Sie Reports- und Analyseanforderungen
- Prüfen Sie Anforderungen aus Datenschutz Gesichtspunkten / Sicherheitsanforderungen
- Definieren Sie Prozessuale Abläufe zwischen DBA, Sicherheits-Admin und Sicherheitsabteilung
- Gewichten Sie Ihre Anforderungen und Bewertungen der Anbieter

Passendes Produkt für Ihre Anforderung

Einführung oder Durchführung eines Proof of Concept (PoC) mit einem Hersteller

ohne eine Überwachung/Monitoring...



