Oracle Audit Vault & Database Firewall in der Praxis

Torsten Husmann
Essener Systemhaus
Stadt Essen

Suvad Sahovic
Oracle Deutschland B.V. & Co. KG
Potsdam

Schlüsselworte

Oracle Datenbank Server, Audit Vault, Firewall, Sicherheit, Auditing, Oracle Advanced Security

- **Einführung**

  Essener Systemhaus verwaltet zurzeit insgesamt ca. 14.000 IT-Arbeitsplätze in der gesamten Stadtverwaltung, in 40 städtischen Beteiligungsunternehmen sowie im pädagogischen Bereich aller 213 Schulen.

  Die IT-Arbeitsplätze verteilen sich auf ca. 450 Lokationen, die überwiegend über LWL angebunden sind. Es gibt 529 verschiedene Anwendungen, die durch das Haus betreut werden.

  - **Was war die Ausgangssituation?**

  Jeder kennt die Problematik mit der Sicherheit. Es ist ein kleines Wort, aber es hat unendlich viele Aspekte. Interne und externe Sicherheit, Netze, Server und vieles mehr. Aber wo fängt man an?

  Unser Haus betrachtet seit Jahren alle Teilgebiete separat. Somit erhoffen wir uns eine möglichst umfassende Analyse aller möglichen Problematiken.

  Daher haben wir ebenfalls unsere Oracle-Datenbankserver einer genauen Sicherheitsüberprüfung unterzogen. Wie alle Überprüfungen wurde diese neutral durch externe Dienstanbieter durchgeführt.

  - **Welche Probleme und Sorgen hatten wir?**

  Die Überprüfung hat verschiedene Sicherheitsprobleme aufgeworfen, auf die ich hier im Einzelnen nicht eingehen möchte. Soviel kann ich erwähnen: Da wir eine öffentliche Einrichtung mit sensiblen Daten sind, müssen wir die einschlägigen Gesetze und Regelungen im besonderen Sinne einhalten. U.a. sollte für jede Tätigkeit der Ausführende eindeutig ermittelt werden können.

  Ein großes Problem war jedoch die Überwachung der Systeme an sich. Egal ob es um Hackversuche, Datenmanipulationen, unberechtigte Zugriffe oder sogar Spionage geht, wie sollen wir im täglichen Betrieb sicherstellen, dass so etwas nicht passiert? Wenn etwas einmal passiert, wie können wir mit brauchbaren Daten nachweisen, wer hat wann und wo was gemacht?

- **Welche Lösungsansätze gab es?**

Zum einen haben wir überlegt, die Oracle-seitigen Bordmittel zu verwenden. Mit Hilfe dieser hätten wir die Log-Level von den Servern als auch den Datenbanken auf den höchsten Level gestellt, um möglichst alle relevanten Daten zur Verfügung zu haben.

Ein weiterer Ansatz war dieselbe Idee, jedoch in Verbindung mit einem externen Syslogserver, mit dessen Hilfe man die gewonnen Daten effektiver auswerten kann.

Ein dritter Ansatz war eine sehr extreme Einschränkung sämtlicher Nutzer, Verfahren und weiteren Privilegien.

Als letzten Ansatz hatten wir Audit Vault betrachtet.

- **Gründe für Audit Vault**

Da wir wie bei vielen Verwaltungen nicht nur Oracle Datenbanken verwalten, sondern eine stark heterogene Umgebung haben, besitzen wir nicht die Kapazitäten, regelmäßig Logfiles zu sichten, um nach Auffälligkeiten Ausschau zu halten.

Ein externer Syslogserver könnte zwar bei der automatisierten Suche sehr helfen,

jedoch würde er nicht pro aktiv arbeiten und somit nur nachträglich auf Gefahren hinweisen.

Die Beschränkung der User und Verfahren stellt aufgrund der oft extrem ungenauen Angaben der Hersteller ein zu großes Risiko dar. Nach Updates oder bestimmten unregelmäßigen Jobs besteht die Gefahr, dass eines der über 40 verschiedene auf unseren Oracle Datenbank-Servern laufenden Verfahren nicht mehr läuft. Zusätzlich würde es bedeuten, dass weitere zeitintensive Tätigkeiten erforderlich werden.

Da Audit Vault

- sowohl aktiv als auch pro-aktiv arbeitet,
- gezielt nur relevante Daten sammelt,
- es fast native im Datenbanksystem integriert ist und
- zudem zu unserer "Alles aus einer Hand"-Strategie passte,
- durch getrennten Bereiche für Administration und Überwachung gleichzeitig auch Gefahren durch Anwendungsverwalter sowie Datenbank-Administratoren selber schützen kann,

haben wir uns entschieden, dieser Lösung durch eine Probeinstallation eine Chance zu geben.

- **Erfahrungen**

  - **Betriebserfahrungen**

Wir nutzen das System nun seit einigen Monaten, haben jedoch wegen vieler anderer Aufgaben die Tests noch nicht abschließen können.

Wir haben bereits feste Regeln für das Logging.

Erste Anfragen aus Fachbereichen und internen Nachforschungen konnten geklärt werden. So hat z.B. ein User unberechtigt weitere User erstellt und Rechte verändert.

In einem anderen Fall konnten wir ungewöhnliche Login-Ereignisse nachvollziehen.

In zwei weiteren Fällen konnten Probleme nur durch den Einsatz von AuditVault geklärt werden.

  - **Betriebsprobleme**

Ein großes Problem haben wir mit den Agents gehabt, welche sich selbstständig deaktiviert hatten und wir jeden Morgen neu starten durften. Ebenfalls gab es Probleme, ein System einzubinden, nachdem ein Mitarbeiter dieses System mit einem falschen Key einbinden wollte. Eins der Probleme wurde durch ein Update behoben, das andere Problem durch einen Neustart.

  - **Cleaning**

Ganz wichtig ist es, zu beachten, dass sich die Daten, welche von Text-Logfiles nach XML umgestellt wurden, nicht automatisch bereinigen.

Es findet kein automatisches Truncating der Logfiles statt, so dass die gesammelten Daten auf den Knoten unendlich anwachsen würden. Es gibt jedoch eine Möglichkeit, alle Daten die bereits übertragen wurden, durch ein Script zu löschen.

  - **Patching**

Wie jedes System muss auch dieses System gepatched werden, angefangen vom Linux-Grundsystem über den AuditVault Server selber bis hin zu den Agents. Alle 3 Patches sind jedoch sehr leicht durchzuführen.

Das Updaten des Linux-Betriebssystems geschieht durch ein einzelnes Kommando (yum update), beim AuditVault-Server ist es eine Datei, die heruntergeladen und ausgeführt werden muss. Die Agents updaten sich automatisch mit einem Neustart, diese bekommen die Updates vom AuditVault Server.

  - **Strategie der Polices**

Es gibt 2 verschiedene Strategien, wie man seine Polices aufbauen kann.

Eine Methode ist es, dass man nur bestimmte User protokolliert. User, die besondere Rechte haben (Admins, Verwalter, ...) und solche, die unter besonderer Aufmerksamkeit stehen.

Dieses Verfahren hat jedoch zwei Nachteile: Wenn man alle Aktivitäten dieser Benutzer sammelt, kommt eine enorme Masse an Daten zusammen, zum anderen werden alle anderen Benutzer dabei gar nicht überwacht.

Der zweite Weg ist es, die 20 wichtigsten Befehle für alle zu protokollieren, darunter fallen natürlich Befehle wie: create, drop, alter,... und einige mehr. Damit hat man den Vorteil, das von allen Usern das Wichtigste festgehalten wird und man jederzeit nachvollziehen kann, wer was gemacht hat auch ohne dass man eine bestimmte Person überwacht oder in Verdacht hatte.

- **Berichtswesen & Benachrichtigung**

Es gibt vordefinierte Berichte als auch Templates, durch die man sich individuelle Berichte zusammenstellen kann. Des Weiteren hat man die Möglichkeit, die wichtigsten Informationen zusammen auf einer Übersicht anzeigen zu lassen.

Benachrichtigungen können sofort bei einmaligen Ereignissen erstellt werden als auch beim Erreichen von Schwellwerten.

Man kann für jede Aktion individuell entscheiden, ob man nur auf der Seite alarmiert wird oder eine EMail, SMS oder ein HTTP Push gesendet wird.

- **Umgang mit Alt-Daten**

Auch der AuditVault Server hat begrenzte Kapazitäten. Somit sollte man sich auch hier frühzeitig Gedanken machen, wie lange man die Infos benötigt und was man danach mit den Informationen macht.

Man kann diese nach einem bestimmten Zeitraum automatisch löschen oder auf eines der vielen Wege auslagern.

- **Ausblick in der Zukunft**

Nachdem wir unsere Basisinformationen über einen bestimmten Zeitraum gesammelt haben, wollen wir detaillierter protokollieren und auch weitere Maschinen einbinden, denn AuditVault ist nicht nur für Oracle DB verfügbar, sondern kann alle gängigen Plattformen auditieren.

Kontaktadresse:

Torsten Husmann

Systemadministrator

Essener Systemhaus / Stadt Essen

Kruppstrasse 82-100

45145 Essen

Telefon: +49 (0)201-88 17 342

Fax: +49 (0) 201-88 91 17 342

E-Mail: torsten.husmann@esh.essen.de

Internet: www.essen.de

Suvad Sahovic

Leitender Systemberater

Oracle Deutschland B.V. & Co. KG

Schiffbauergasse 14

14467 Potsdam

Telefon: +49 (0) 331-2007-181

Fax: +49 (0) 331-2007-561

E-Mail: suvad.sahovic@oracle.com

Internet: http://www.oracle.com