Exadata Security: Was ist möglich?

Borys Neselovskyi
OPITZ CONSULTING Deutschland GmbH

Schlüsselworte

Exadata Virtualisierung, Isolierung, Infiniband-Partitionierung, VLAN Tagging, ASM Security, Firewall (iptables), SE Linux, TDE, Advanced Security, Database Vault, Auditing

Manuskript

In diesem Vortrag stelle ich die wichtigsten Sicherheitsbegriffe und Möglichkeiten im Exadata-Umfeld vor.

Bevor ein Unternehmen eine (oder mehrere) Exadata(s) anschafft, müssen sich die Entscheider mit vielen Fragen beschäftigen. Besonders wichtig ist es dabei, die Sicherheitsanforderungen aufzunehmen und ein passendes Konzept zu evaluieren. Die Datenbanken, die Reporting-Zwecken dienen, brauchen zum Beispiel ein anderes Sicherheitslevel als Datenbanken, die Daten von Kreditkartenbesitzern beinhalten.

Die Oracle Exadata lässt sich für hohe Sicherheitsstandards gut einsetzen. Sie kann „multimandantfähig“ konfiguriert werden. sodass die auf ihr laufenden Anwendungen, und somit auch die im Betrieb befindlichen Datenbanken, komplett voneinander isoliert betrieben werden können. Die Trennung von mehreren Umgebungen innerhalb einer Maschine geschieht auf unterschiedlichen Ebenen: Storage, Datenbankserver, Publik Netzwerk und Internes Netzwerk.

Eine zentrale Rolle bei dieser Trennung spielt die Virtualisierung: Die Datenbankserver werden als virtuelle Maschinen implementiert, die auf der Netzwerkebene mittels VLAN Tagging voneinander isoliert werden können. Interne Cluster-Kommunikation sowie die Anbindung von Storage erfolgt via Infiniband-Netzwerk. Auch dieses Netzwerk kann in der Version 12.1.2.1.2 pro Cluster partitioniert werden.

Ein weiterer wichtiger Aspekt ist, die Sicherheit auf der Storage-Ebene zu implementieren. Standardmäßig können alle Datenbanken auf alle ASM Disks in einer Exadata zugreifen (Modus: Open Security).

Der Administrator kann das Automatic Storage Management (ASM) so konfigurieren, dass auf einzelne Disks von nur einem Cluster (ASM-Scoped Security Mode) oder von nur einer Datenbank (Database-Scoped Security Mode) zugegriffen werden kann.

Anhand von Beispielen zeige ich die Schritte, die notwendig sind, um die Sicherheit auf der ASM-Ebene zu konfigurieren.

Als besonders wichtigen Punkt greife ich die Härtung der Umgebung auf der Server- bzw. Datenbankebene heraus. Diese Maßnahmen sind zwar nicht Exadata-spezifisch, sie sind aber für die Sicherheit der Systeme absolut notwendig. Zu den wichtigsten Maßnahmen auf Betriebssystemebene gehören:

- Die Aktivierung der Option SE (Security) in Linux
- Die Konfiguration einer Firewall, um die ein- und ausgehende Verbindungen zu kontrollieren
- Implementierung einer Passwort-Richtlinie für die Benutzerverwaltung

- Aktivierung des Auditings

Da eine Exadata für den Betrieb von Datenbanken konzipiert ist, spielt die Security auf der Datenbank-Ebene eine entscheidende Rolle in dem gesamten Sicherheitskonzept. Ich gebe einen Überblick über die wichtigsten Härtungsmaßnahmen, die in einer Oracle Datenbank möglich sind. Komplettiert wird der Vortrag mit der Auflistung von organisatorischen Maßnahmen, die notwendig sind, um einen hohen Sicherheitsstandard zu erzielen

Kontaktadresse:

Borys Neselovskyi

OPITZ CONSULTING Deutschland GmbH

Lazarettstraße 15

45127 Essen

Telefon: +49 (0) 2261-6001 0

Mobil: +49 (0) 173-7279029

E-Mail borys.neselovskyi@opitz-consulting.com

Internet: www.opitz-consulting.com

Vielen Dank für die Einreichung Ihres Vortrags.
Sie werden in Kürze eine E-Mail erhalten.
Ihre Daten:

Titel	Exadata Security: Was ist möglich?
Schwerpunkt des Vortrags	Exadata & ODA
Keywords zum Vortrag	Betrieb; Exadata
Vortragstyp	Tipps & Tricks
Schwierigkeitsgrad	Experten
Vortrag enthält Demo	Nein
Newcomer	Nein
Mentor benötigt?	Nein
Kurzinfo / Zusammenfassung des Vortrags	In diesem Vortrag stelle ich die wichtigsten Sicherheitsbegriffe und Möglichkeiten im Exadata-Umfeld vor. Bevor ein Unternehmen eine (oder mehrere) Exadata(s) anschafft, müssen sich die Entscheider mit vielen Fragen beschäftigen. Besonders wichtig ist es dabei, die Sicherheitsanforderungen aufzunehmen und ein passendes Konzept zu evaluieren. Die Datenbanken, die Reporting-Zwecken dienen, brauchen zum Beispiel ein anderes Sicherheitslevel als Datenbanken, die Daten von Kreditkartenbesitzern beinhalten. Die Oracle Exadata lässt sich für hohe Sicherheitsstandards gut einsetzen. Sie kann

	„multimandantfähig“ konfiguriert werden. sodass die auf ihr laufenden Anwendungen, und somit auch die im Betrieb befindlichen Datenbanken, komplett voneinander isoliert betrieben werden können. Die Trennung von mehreren Umgebungen innerhalb einer Maschine geschieht auf unterschiedlichen Ebenen: Storage, Datenbankserver, Publik Netzwerk und Internes Netzwerk. Eine zentrale Rolle bei dieser Trennung spielt die Virtualisierung: Die Datenbankserver werden als virtuelle Maschinen implementiert, die auf der Netzwerkebene mittels VLAN Tagging voneinander isoliert werden können. Interne Cluster-Kommunikation sowie die Anbindung von Storage erfolgt via Infiniband-Netzwerk. Auch dieses Netzwerk kann in der Version 12.1.2.1.2 pro Cluster partitioniert werden. Ein weiterer wichtiger Aspekt ist, die Sicherheit auf der Storage-Ebene zu implementieren. Standardmäßig können alle Datenbanken auf alle ASM Disks in einer Exadata zugreifen (Modus: Open Security). Der Administrator kann das Automatic Storage Management (ASM) so konfigurieren, dass auf einzelne Disks von nur einem Cluster (ASM-Scoped Security Mode) oder von nur einer Datenbank (Database-Scoped Security Mode) zugegriffen werden kann. Anhand von Beispielen zeige ich die Schritte, die notwendig sind, um die Sicherheit auf der ASM-Ebene zu konfigurieren. Als besonders wichtigen Punkt greife ich die Härtung der Umgebung auf der Server- bzw. Datenbankebene heraus. Diese Maßnahmen sind zwar nicht Exadata-spezifisch, sie sind aber für die Sicherheit der Systeme absolut notwendig. Zu den wichtigsten Maßnahmen auf Betriebssystemebene gehören: - Die Aktivierung der Option SE (Security) in Linux - Die Konfiguration einer Firewall, um die ein- und ausgehende Verbindungen zu kontrollieren - Implementierung einer Passwort-Richtlinie für die Benutzerverwaltung - Aktivierung des Auditings Da eine Exadata für den Betrieb von Datenbanken konzipiert ist, spielt die Security auf der Datenbank-Ebene eine entscheidende Rolle in dem gesamten Sicherheitskonzept. Ich gebe einen Überblick über die wichtigsten Härtungsmaßnahmen, die in einer Oracle Datenbank möglich sind. Komplettiert wird der Vortrag mit der Auflistung von organisatorischen Maßnahmen, die notwendig sind, um einen hohen Sicherheitsstandard zu erzielen
Zustimmung zur Datenweitergabe	Ja
Sprache	deutsch
	, ich räume der DOAG die Rechte ein, meine Präsentation und alle diesbezüglichen Dokumente für interne und externe Zwecke zu nutzen. Dies beinhaltet die Nutzung und Verbreitung innerhalb der DOAG und durch das Netzwerk der Gesellschaften der DOAG. Das Recht beinhaltet nicht den kommerziellen Gebrauch. Weitere Einzelheiten regeln die Teilnahmebedingungen im Referentenhandbuch.
Bemerkungen	

Anrede	Herr
Titel	
Vorname	Borys
Nachname	Neselovskyi
Firma	OPITZ CONSULTING Deutschland GmbH
Abteilung	
Branche	
Straße	Lazarettstr. 15
PLZ	45127
Ort	Essen
Land	Deutschland

Telefon/Handy	+49 (0) 173-7279029
E-Mail	borys.neselovskyi@opitz-consulting.com
Ihre User Group	