Entspricht die Exadata den höchsten Sicherheitsanforderungen?

Borys Neselovskyi, OPITZ CONSULTING Deutschland GmbH

Die Oracle-Exadata ist für den Betrieb von hochkritischen, durchsatzintensiven Datenbanken nicht mehr wegzudenken. Mit einer hervorragenden Hardware-Ausstattung und eigenen Software-Lösungen wie etwa Smart Scans findet sie Einsatz in unternehmenskritischen Umgebungen, die gesondert behandelt werden sollen. Was die Perfomance betrifft, ist die Exadata also die beste Lösung für den Betrieb von Oracle-Datenbanken. Aber wird sie auch modernen Sicherheitsanforderungen gerecht? Diese Frage ist zu komplex, um in einem Satz mit „ja“ oder „nein“ beantwortet zu werden.

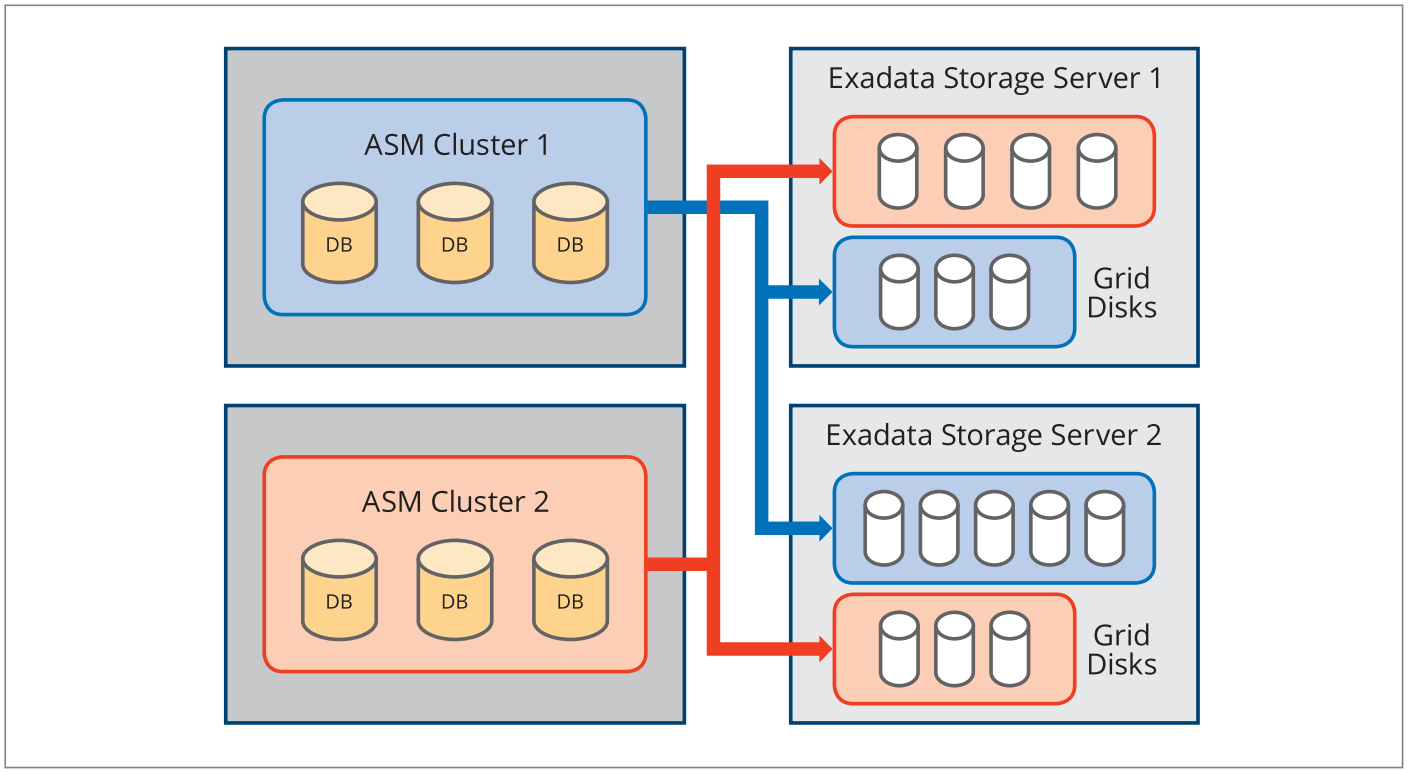

Abbildung 1: ASM-Scoped Security

Sicherheit hat viele Fassetten. Folgende Aspekte wurden für die Bewertung des Sicherheitsstandards einmal genauer angesehen:

- Ist eine Isolierung von unterschiedlichen Umgebungen innerhalb einer Exadata-Maschine möglich? Mit anderen Worten: Ist die Exadata mandantenfähig?
- Ist die Exadata nach der Installation sicher genug?
- Wie sieht es mit der Härtung der Betriebssysteme aller Komponenten aus?
- Sind Netzwerk-Komponenten sicherheitskonform installiert und konfiguriert?
- Entspricht die IT-Infrastruktur rund um die Exadata den Sicherheitsanforderungen?

Ist die Exadata mandantenfähig?

Die Isolierung verschiedener Umgebungen innerhalb der Exadata ist in vielen Fällen durchaus sinnvoll. So können zum Beispiel Datenbank-Anwendungen von unterschiedlichen Firmen (oder Abteilungen) komplett voneinander getrennt auf einer Exadata betrieben werden. Ein anderes Anwendungsszenario wäre die Trennung von Test- und Produktions-Umgebungen innerhalb einer Exadata: Da sich viele Unternehmen keine Exadata leisten können, die nur zu Testzwecken dient, ist die Trennung unterschiedlicher Umgebungen durchaus sinnvoll. Doch die technische Umsetzung ist aufwendig und kompliziert. Tiefgreifendes Know-how und exzellentes Verständnis der Arbeitsweise einer Exadata sind absolut notwendig, um die Isolierung zu vollziehen.

Eine Exadata besteht aus mehreren Komponenten und Modulen, die bei der Konfiguration der Isolierung einzeln betrachtet werden sollten. Die folgenden Begriffe sind für das Verständnis der Konfiguration der Mandantenfähigkeit sehr wichtig:

- *Datenbank-Server (engl. „Compute Node“)*
  Dieser besteht aus mindestens zwei physikalischen Maschinen, die für den Betrieb von Datenbanken verantwortlich sind. Die Datenbanken werden hier im Cluster betrieben. Die Cluster-Komponenten sind auf jedem Datenbank-Server installiert.

- *Storage-Server (engl. „Storage Cell“)*
  Dieser besteht aus mindestens drei Speicher-Systemen, die den Plattenplatz für die Speicherung von Daten in Datenbanken bereitstellen.

- *InfiniBand-Switches*
  Hierbei handelt es sich um Netzwerk-Switches für die Netzwerk-Kommunikation zwischen Datenbank- und Storage-Servern. In der Standard-Ausstattung sind zwei InfiniBand-Switches vorhanden, die als eine Einheit namens „InfiniBand Fabric“ für die Cluster-Kommunikation verantwortlich sind.

- *Automatic Storage Management (ASM)*
  Oracle ASM besteht aus einem Volume-Manager und einem Dateisystem für Oracle-Datenbank-Dateien, die den Inhalt des Storage aufbereiten und ihn Datenbanken zur Verfügung stellen.

- *Oracle-Clusterware*
  Alle Exadata-Hardware-Komponenten sind redundant ausgelegt und vor Ausfällen ausreichend geschützt. Die Datenbanken, Listener und andere notwendigen Dienste werden auf mehreren Datenbank-Servern in einem (oder mehreren) Real Application Clustern (RAC) betrieben. Wenn eine Datenbank-Instanz auf einem Datenbank-Server ausfällt, übernimmt die Instanz auf einem anderen

Cluster-Mitglied die Arbeit. Mit der Cluster-Funktionalität erhöht sich die Ausfallsicherheit der Datenbanken.

- *Interconnect (Cluster-Kommunikation)*
  Alle Cluster-Mitglieder kommunizieren miteinander über das sogenannte „Cluster Interconnect". Diese Kommunikation erfolgt über ein InfiniBand-Netzwerk. Alle Server haben InfiniBand-Netzwerkkarten und sind darüber mit beiden InfiniBand-Switches redundant verbunden.

- *Public- oder Client-Netzwerk*
  Über dieses Netzwerk erfolgt die Kommunikation zwischen Datenbanken und Anwender (beziehungsweise Anwendungen).

- *Virtualisierte Plattform/Bare Metal*
  Exadata kann als „Blech" (Bare Metal) oder virtualisiert betrieben werden. Die Virtualisierung bringt mehr Komplexität bei der Konfiguration und Lifecycle-Operationen mit sich. Auf der anderen Seite erlaubt die Virtualisierung mehr Flexibilität bei der Exadata-Konfiguration.

Nachdem die Begriffe klar sind, können wir die Konfiguration der Mandantenfähigkeit auf allen Ebenen besprechen.

Exadata: virtualisiert oder Bare Metal?

Die Trennung von Umgebungen innerhalb einer Exadata kann auf der Cluster-Ebene realisiert werden. In der Regel sollen zwei Cluster für die Isolierung sorgen. In der virtualisierten Exadata-Variante können auf jedem physikalischen Datenbank-Server beliebig viele virtuelle Server aufgesetzt sein, die in separate Cluster segregiert sind. In der Bare-Metal-Variante müssen physikalische Datenbank- und Storage-Server in zwei Cluster aufgeteilt sein. Dabei ist wichtig zu wissen, dass zu einem Cluster mindestens zwei Datenbank- und drei Storage-Server gehören. Dem entsprechen die Exadata-Modelle Half- und Full-Rack. Die kleineren Modelle Eight- und Quarter-Rack eignen sich dagegen nicht für die physikalische Isolierung. In diesem Fall bleibt nur die Option, die Exadata zu virtualisieren.

Trennung der Clusterkommunikation

In einer Zwei-Cluster-Umgebung muss auch die Cluster-Kommunikation getrennt stattfinden. Für diese Kommunikation ist die InfiniBand Fabric zuständig. Deren Hardware lässt sich nicht pro Cluster isolieren; lediglich die Netzwerk-Kommunikation kann in zwei Ströme unterteilt werden. Das Verfahren nennt sich „InfiniBand Partitionierung" und wird seitens Oracle nur in der virtualisierten Exadata-Variante unterstützt.

Isolierung von Storage-Bereichen pro Cluster beziehungsweise pro Datenbank

Die Isolierung von Clustern sollte auch auf der Storage-Ebene durchgeführt werden. Das Tool ASM gruppiert die physikalischen Platten logisch in sogenannte „Grid-Disks". Diese werden in ASM-Gruppen zusammengefasst und stellen Plattenplatz für die Datenbanken zur Verfügung. Der Zugriff auf den Storage wird durch folgende ASM-Modi geregelt:

- *Open Mode*
  Alle Datenbanken können auf alle vorhandenen Grid-Disks zugreifen; dabei gibt es keine Einschränkungen. Das ist die Standard-Einstellung, sie bietet keine Sicherheit auf der Storage-Ebene. Diese ASM-Konfiguration sollte daher nur für Test- oder Entwicklungs-Umgebungen verwendet werden.

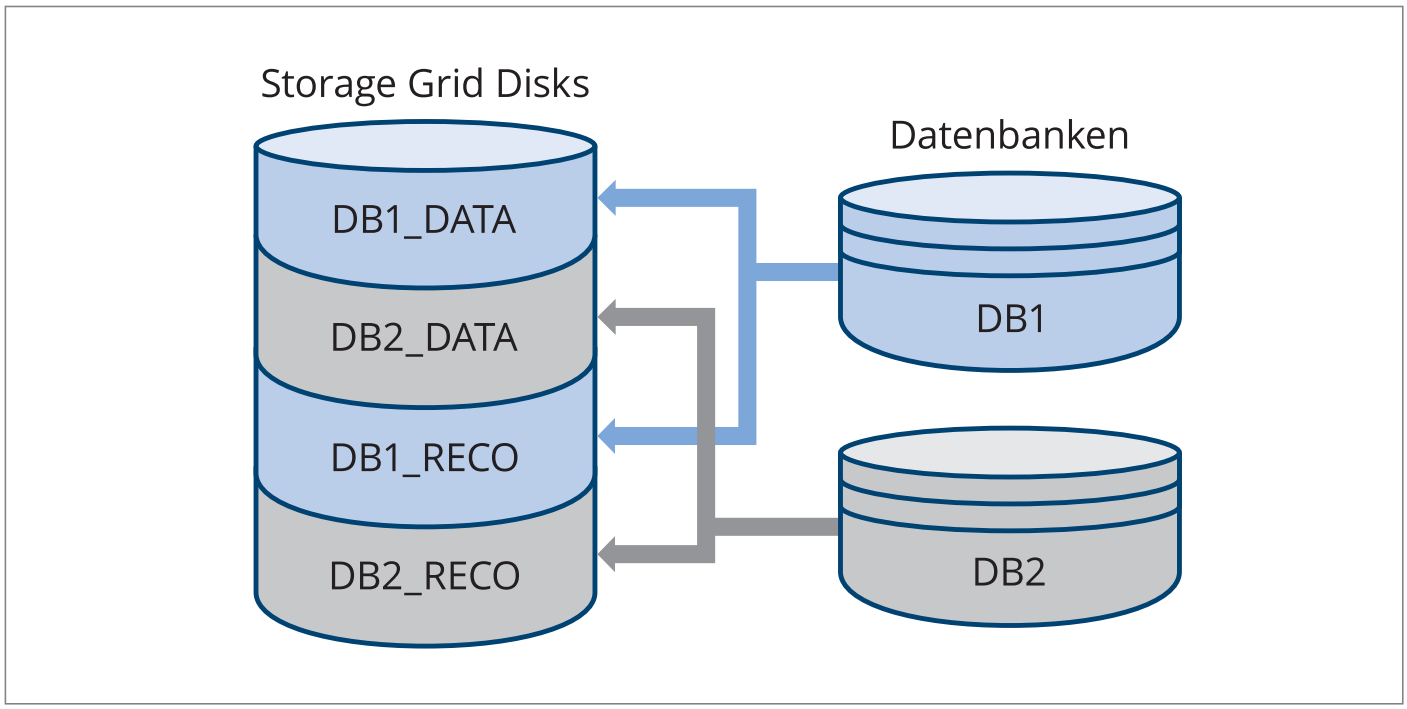

Abbildung 2: Database-Scoped Security

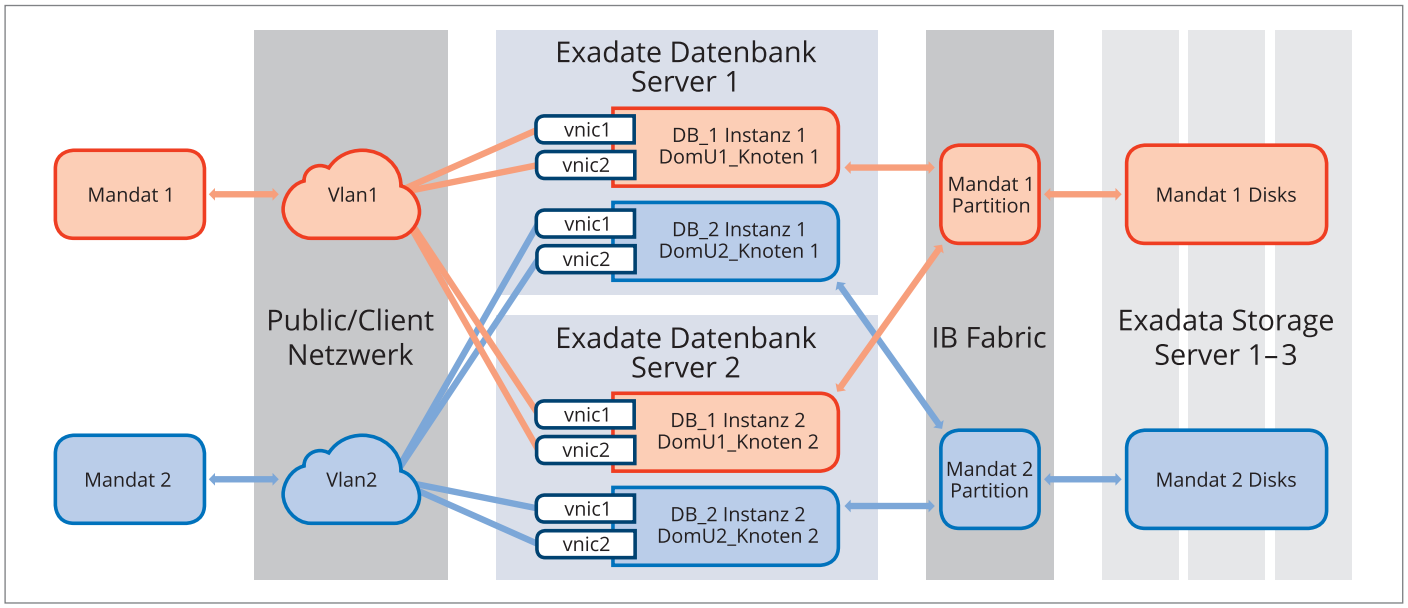

Abbildung 3: Exadata-Isolierung

- *ASM-Scoped Security-Mode*
  Grid-Disks werden einem Cluster zugeteilt und können nur von Datenbanken verwendet werden, die zu diesem Cluster gehören. Datenbanken aus einem anderen Cluster bekommen keinen Zugriff auf diesen Storage-Bereich *(siehe Abbildung 1)*.

- *Database-Scoped Security-Mode*
  Dieser Modus entspricht dem höchsten Sicherheitsstandard. Dabei wird jeder Datenbank ein eigener Plattenbereich zugeteilt. Dieser Modus ist eine Stufe härter als der ASM-Scoped Security-Mode *(siehe Abbildung 2)*.

Partitionierung des Public-Netzwerks

Der Zugriff auf Datenbanken in einer Exadata erfolgt über ein sogenanntes „Public- oder Client-Netzwerk". Wenn mehrere Cluster innerhalb einer Exadata betrieben werden, kann auch das Client-Netzwerk pro Cluster separiert werden, was durch das VLAN-Tagging-Verfahren realisiert wird. Dieses ermöglicht, ein bestehendes physikalisches Netzwerk zu partitionieren und mehrere virtuelle Netzwerke zu kreieren, die voneinander getrennt sind. VLAN Tagging basiert auf der 802.1Q-Technologie. Es ist nicht Exadata-spezifisch, sondern findet auch im Linux/Unix-Umfeld Verwendung. Die Partitionierung des Public-Netzwerks kann ab Exadata-Version 12.1.2.1.1 bei der initialen Exadata-Konfiguration mittels Oracle Exadata Deployment Assistant (OEDA) durchgeführt werden.

Abbildung 3 zeigt eine virtualisierte Exadata. Zwei Cluster (farblich rot und blau gekennzeichnet) wurden konsequent voneinander isoliert und zwar auf allen Ebenen: Der Client-Zugriff auf jedes Cluster erfolgt über eine virtuelle Partition des Public-Netzwerks. Die Cluster-Kommunikation wurde auch auf der InfiniBand-Ebene partitioniert und verläuft somit getrennt. Auf der Storage-Ebene hat jedes Cluster einen eigenen Plattenbereich.

Fazit: Eine Exadata ist mandantenfähig. Die konsequente Isolierung mehrerer Umgebungen innerhalb einer Exadata setzt aber folgende Maßnahmen voraus:

- Die Exadata muss virtualisiert sein.
- Das InfiniBand-Netzwerk muss partitioniert sein.
- ASM-Scoped Security-Mode oder Database-Scoped Security-Mode muss konfiguriert sein.
- Das Client-Netzwerk muss durch das VLAN-Tagging partitioniert werden.

Wie sicher ist die Exadata?

Die Software-Ausstattung eines Exadata-Datenbank-Servers besteht aus Betriebssystem, Cluster- und Datenbank-Software. Das Betriebssystem wird durch den Benutzer „root" administriert. Die Administration von Oracle Cluster Software und Datenbank erfolgt standardmäßig über den Benutzer „oracle". Für Umgebungen mit erhöhten Sicherheitsanforderungen sollten sogenannte „Separations of Duties" konfiguriert sein. Dabei wird die Administration von Cluster und Datenbank getrennt. Der Benutzer „grid" administriert den Cluster. Die Datenbank-Administration auf der Betriebssystem-Ebene erfolgt weiterhin über den Benutzer „oracle". Somit sind Cluster- und Datenbank-Bereiche voneinander getrennt. Der Nachteil dieser Lösung ist die erhöhte Komplexität der Umgebung und der größere Aufwand bei Administration und Lifecycle-Operationen.

Die initiale Installation einer Exadata beinhaltet eine Härtung aller Komponenten nach den besten Sicherheitsstandards. So sind sowohl auf Datenbank- als auch auf Storage-Servern nur die notwendigen Betriebssystem-Pakete installiert. Vergeblich sucht man Kommandos wie „telnet" oder „nc", um die Netzwerk-Konnektivität zu prüfen. Diese und viele andere Binaries sind per Default nicht installiert. Exadata-Administratoren können natürlich weitere Pakete nachinstallieren, müssen aber sicherstellen, dass dabei keine Sicherheitslücken geöffnet werden.

Überflüssige Linux-Dienste und -Protokolle sind per Default deaktiviert. So werden die Internet-Kommunikationsdienste „inetd"/„xinetd" auf der Exadata nicht gestartet. Die für den Exadata-Betrieb notwendigen Dienste wie Secure Socket Lay-

er (SSH) und Network Time Protokol (NTP) bieten erweiterte Möglichkeiten für Sicherheitskonfigurationen. Alte und unsichere SSH-Versionen werden nicht unterstützt.

Alle Verzeichnisse und Dateien sind mit den minimal notwendigen Berechtigungen ausgestattet. Daten, die auf der Exadata gespeichert und transportiert werden, können sicher verschlüsselt werden: Die Exadata-Linux-Server unterstützen den höchsten Verschlüsselungsstandard 140 of FIPS (Federal Information Processing Standards).

Auf allen Storage-Servern ist die Linux-Firewall „iptables" aktiviert. Direkte Verbindungen zu den Storage-Servern von außen sind per Default nie erlaubt. Die Datenbank-Server sind hingegen nicht mit einer aktiven Firewall ausgestattet. Für die Einhaltung von Sicherheits-Richtlinien sollten die Firewall-Regeln realisiert und der Dienst „iptables" aktiviert werden. Zudem sollte man die Daten über das Netzwerk verschlüsselt übertragen. Für die Kontrolle der Netzwerk-Zugriffe ist die Zugriffs-Tabelle („Access Control Lists") zu pflegen. Die Netzwerk-Switches sollten folgendermaßen nach Best Practices konfiguriert sein:

- AAA-Prinzip einhalten (Authentifizierung/Autorisierung/Accounting)
- Port Mirroring aktivieren: Netzwerk-Daten werden zusätzlich an eine Prüfstelle (Intrusion Detection System) für die Sicherheits-Analyse weitergeleitet (Intrusion Detection System)
- Auto-Trunking deaktivieren

Die Standard-Passwort-Richtlinien sind bereits sicher. Ein neues Passwort darf dem alten nicht ähnlich sein. Die Laufzeit eines Passworts beträgt 90 Tage. Die Komplexität ist wie folgt geregelt:

- Erlaubte Zeichen
  - Ziffern, Klein- bzw. Großbuchstaben, Sonderzeichen
- Passwortlänge
  - Bei der Verwendung der drei Zeichenklassen muss ein Passwort mindestens zwölf Zeichen lang sein
  - Bei der Verwendung der vier Zeichenklassen muss ein Passwort mindestens acht Zeichen lang sein

Fehlgeschlagene Anmeldungen an der Exadata werden wie folgt geregelt:

- Nach einem fehlgeschlagenen Log-in-Versuch wird der Account für zehn Minuten gesperrt.
- Nach fünf fehlgeschlagenen Log-ins wird der Benutzer dauerhaft gesperrt.

Als Betriebssystembenutzer „root" können gesperrte Benutzer mit dem Kommando „pam_tailly2" angezeigt und entsperrt werden:

- *Gesperrte Benutzer anzeigen*
  „/sbin/pam_tally2"

- *Benutzer entsperren*
  „/sbin/pamm_tally2 -user <username> --reset"

Die Exadata-Storage- und Datenbank-Server werden über das Tool „Integrated Lights Out Manager" (ILOM) administriert. Darüber können die Hardware-Komponenten geprüft und verwaltet werden. Das Tool kann über eine Web-Oberfläche oder über ein Command Line Interface (CLI) bedient werden: Der Zugriff auf ILOM über das Web-Interface erfolgt über einen Internet-Browser. Die Kommunikation ist mit SSL verschlüsselt. Der Zugriff auf ILOM CLI erfolgt entweder über Secure Socket Shell (SSH) oder Intelligent Platform Management Interface (IPMI). Sowohl bei SSH als auch bei IPMI wird die zweite Version verwendet, die erweiterte Sicherheitseinstellungen unterstützt.

Die Funktion „Standard-Betriebssystem-Auditing" kann mit Linux-Mitteln aktiviert werden. Auf dem Storage-Server gibt es die Möglichkeit, die erweiterte Auditing-Funktion zu aktivieren, indem man den Parameter „sysLogConf" setzt.

Sicherheit von Datenbank und Infrastruktur

Die Härtung der gesamten Infrastruktur sowie der Datenbanken ist eine wichtige Aufgabe. Diese Maßnahmen können sehr umfangreich sein. Die Härtung der Exadata sollte Teil des gesamten Sicherheitskonzepts sein, bei dem alle Elemente der Infrastruktur berücksichtigt werden.

Tipp 1: Der Zugriff auf die Exadata-Komponenten über privilegierte Betriebssystem-Benutzer sollte deaktiviert werden. Der Zugriff erfolgt mit einem nicht privilegierten Benutzer, der mithilfe des Werkzeugs „sudo" zu einem System-Account (wie etwa „root"/„oracle"/„grid") wechseln kann.

Tipp 2: Der direkte Zugang zu Exadata-Systemen mittels SSH sollte für Anwendungsbenutzer unterbunden werden.

Tipp 3: Für die Überwachung von Storage-Servern durch den Enterprise Manager sollte der Betriebssystembenutzer „cellmonitor" eingesetzt werden.

Tipp 4: Die direkte SSH-Verbindung zum Storage-Server kann deaktiviert werden. Alle administrativen Aufgaben können vom Datenbank-Server via ExaCLI oder REST-API ausgeführt werden.

Fazit

Die Exadata entspricht grundsätzlich den höchsten Sicherheitsanforderungen. Konfiguration und Implementierung sind allerdings sehr aufwendig und setzen einen hohen Kompetenzgrad des Personals voraus. Erforderlich ist zudem ein Konzept, das es ermöglicht, Exadata immer auf dem aktuellsten Stand zu halten. Unter anderem sollte darauf geachtet werden:

- Die Installation von Sicherheitspatches dauerhaft zu planen und zu terminieren
- Monitoring von neuen Sicherheitslücken in regelmäßigen Abständen durchzuführen
- Zeitnah die dafür vorgesehenen Lösungen zu implementieren, wenn Sicherheitslücken entdeckt werden.

Diese und weitere Maßnahmen, kontinuierlich geplant und umgesetzt, gewährleisten die Sicherheit der Exadata während des gesamten Lebenszyklus.

Borys Neselovskyi
borys.neselovskyi@opitz-consulting.com