Der GI Admin hat meine Daten geklaut – Wie das?

Daniel Westermann
dbi services
Schweiz

Schlüsselworte

Grid Infrastructure, Clusterware, Job role separation, Security, ASM

Einleitung

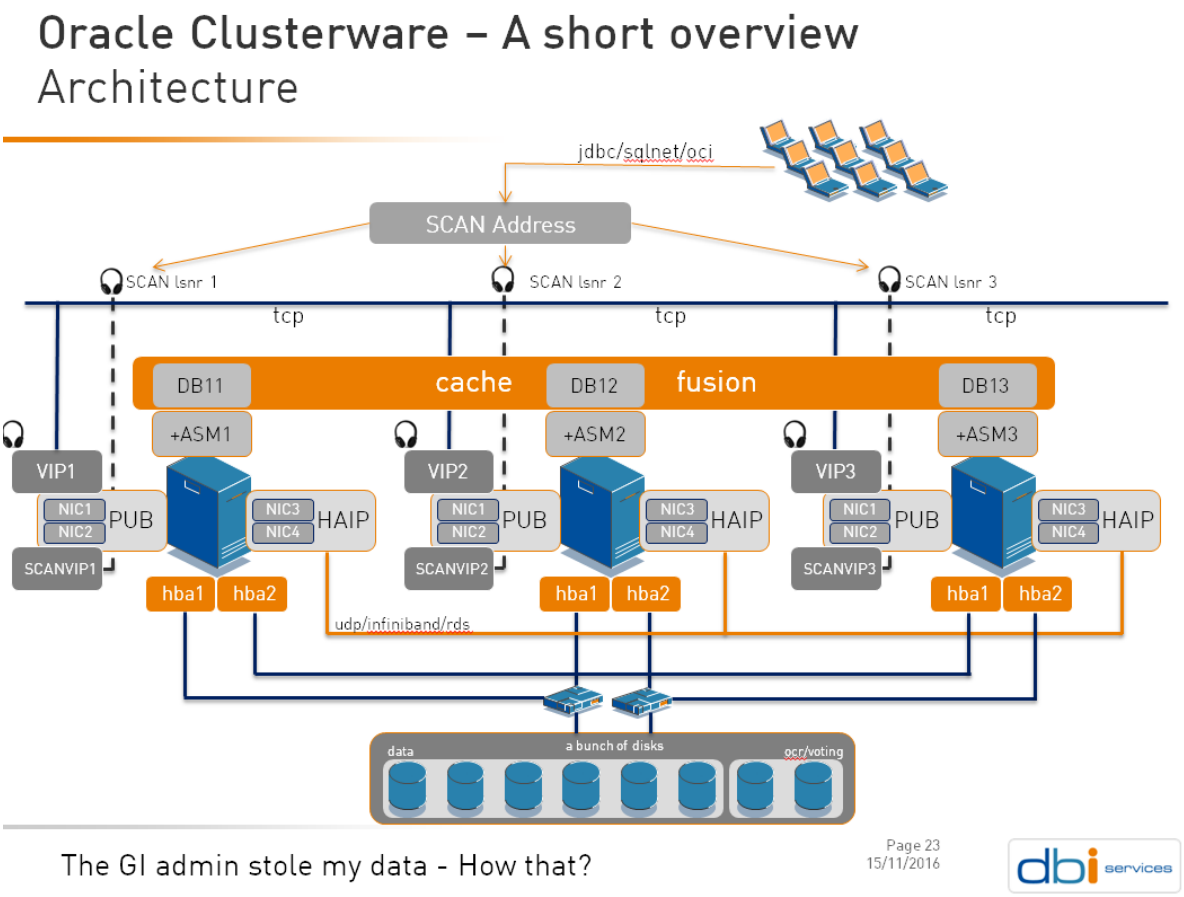
Diese Session beginnt mit einer kleinen Historie der Oracle Clusterware (Oracle Grid Infrastructure). Wo kommt sie her, wie hat sie sich entwickelt und was ist der heutige Stand? Was definiert überhaupt einen Cluster? Darauf aufbauend wird erläutert wo im Cluster-Stack die Daten überall zu finden sind und welche Möglichkeiten ein GI-Admin hätte diese Daten abzuziehen. Zum Ende geht es um mögliche Schutzmechanismen.

Begründung

In der heutigen Zeit wird der Schutz der Daten immer wichtiger. Wenn mehrere Knoten zu einem Cluster verbunden werden erhöht sich auch die Zahl der möglichen Einfallstore. Sind die Aufgaben der klassischen DBAs von denen des Clusterware Administrators getrennt? Macht der DBA alles, vom Betriebssystem über den Cluster bis zur Datenbank? Wie sieht es mit den Oracle Engineered Systemen aus? Auf diesen ist die Oracle Grid Infrastructure essentieller Bestandteil und sowieso schon vorinstalliert. Wer hat Zugriff auf die sensitiven Daten? Mit diesen Fragen muss man sich in den heutigen Umgebungen und bei den heutigen Anfordungen an die Sicherheit zwingend auseinandersetzen.

Was ist ein Cluster?

Was ist denn ein Cluster? Den Begriff Cluster gibt es in den unterschiedlichsten Bereichen: Physik, Chemie, Biologie, Informatik. In der Informatik definiert sich ein Cluster durch mehrere verteilte Komponenten die zusammen an einem Ziel arbeiten und sich nach aussen als eine Einheit präsentieren. Das kann helfen die Last zu verteilen oder lokale Ausfälle einzelner Komponenten zu kompensieren ohne den Betrieb einstellen zu müssen.



Ein Cluster erhöht aber auch die Komplexität einer Umgebung enorm. Sehr viele Komponenten müssen reibungslos miteinander zusammenarbeiten um einen Cluster stabil betreiben zu können. Auch meine Daten sind potentiell auf allen Cluster-Knoten vorhanden.

Wo sind meine Daten?

Es ist gar nicht so einfach zu bestimmen wo meine Daten in einem Clusterverbund überall sind. Irgendwo auf den Disks ganz sicher. Im public Netzwerk und auf dem Interconnect Teile davon sicher auch. Wie sieht es mit dem Memory der einzelnen Knoten aus? Auf den Clients?

```
[root@rac1 ~]# tcpdump -i enp0s8:3 tcp  -A -s1500  -w sqlnet.dmp
```

Wenn ich meine Daten vor fremdem Zugriff schützen will, muss ich in einem Clusterverbund einige Grundregeln beachten: Wer in meiner Organisation ist zuständig für welche Aufgaben? Vertraue ich allen? Habe ich gar Teile meines Betriebs an Drittanbieter ausgegliedert? Wie sieht es dort mit der Sicherheit aus?

Wir schauen uns an welche Rolle, theoretisch wie, Zugriff auf die Daten hat und welche Möglichkeiten bestehen sich davor zu schützen.

Wenn die Rollen und Zugriffsmöglichkeiten klar sind geht es darum die Daten zu schützen. Hier gibt es nur eine einzige technische Lösung: Verschlüsselung auf allen Ebenen. Oracle bietet hierfür diverse Ansätze und Werkzeuge:

- TDE: Transparent Data Encryption aud Tablespace oder Tabellen oder Spalten-Ebene
- Verschlüsselung auf Netzwerkebene
- Verschlüsselung der Backups

Man sollte allerdings nicht vergessen, dass man auch schon viel erreichen kann, wenn man die von Oracle vorgeschlagegen Betriebssystem-Gruppen richtig einsetzt. dba,oper,asmadmin,asmdba und asmoper sind nicht nur zum Spass da: Richtig eingesetzt schützen sie auch.

Demo

In dieser Demo wird aufgezeigt wir ein GI Administrator, der keinen direkten Zugriff auf die Datenbank hat, dennoch eine komplette Datenbank kopieren kann und damit theoretisch an alle sensitiven Daten herankommt.

Kontaktadresse:

dbi services
Daniel Westermann

Rue de la Jeunesse 2
CH-2800 Delémont

Telefon: +41 32 422 96 00
Fax: +41 32 422 96 15
E-Mail daniel.westermann@dbi-services.com
Internet: www.dbi-services.com