

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.

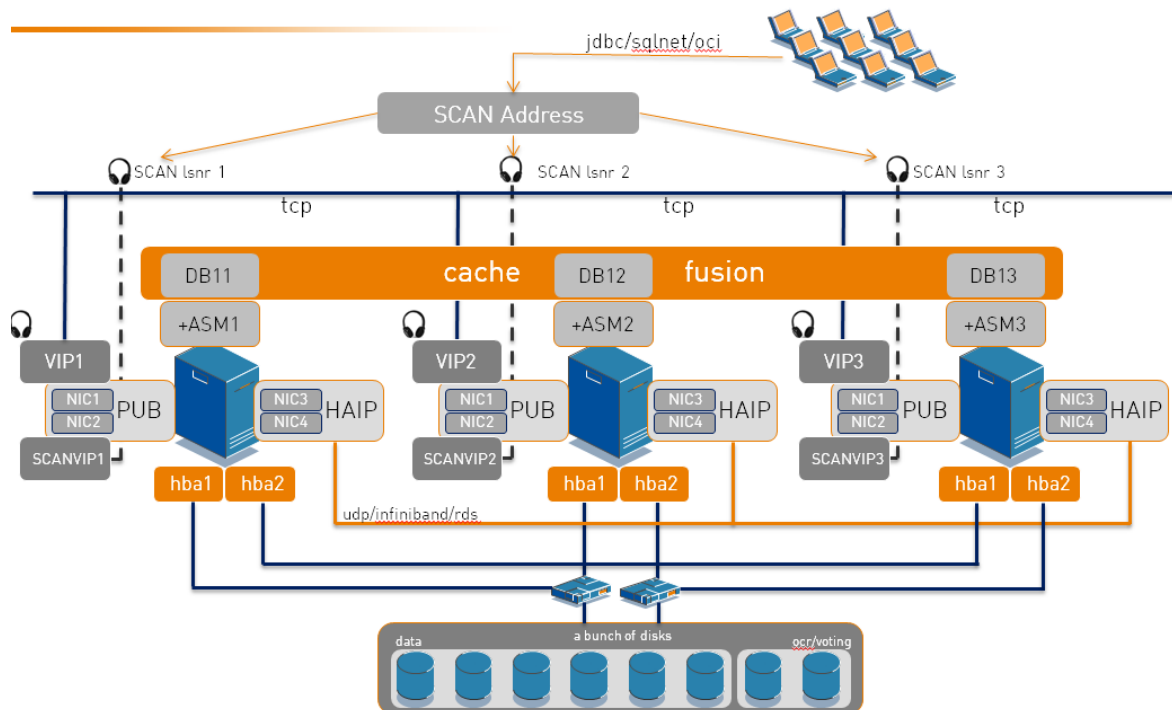
Begründung

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 Anforderungen 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.

Oracle Clusterware – A short overview Architecture



The GI admin stole my data - How that?

Page 23
15/11/2016



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
```

```
0000 0a 00 27 00 00 00 08 00 27 51 34 e6 08 00 45 00  ..'Q4...E.
0010 01 22 8e b2 40 00 40 06 fd 95 c0 a8 16 3c c0 a8  ..".@.@. ....<..
0020 16 01 05 f1 c9 32 3e 30 cf f3 3c 4f a7 bc 80 18  .....2>0 ..<0...
0030 04 ad ae a2 00 00 01 01 08 0a 00 b3 3a f5 00 49  .....I
0040 4c 4f 00 00 00 ee 06 00 00 00 00 10 17 32 87  LO.....2.
0050 ec 6e 87 b7 37 f1 b1 72 8f 78 fb 76 c4 fd 78 74  ..n..7..r .x.v..xt
0060 09 1a 0e 1b 1e 01 48 01 02 51 01 80 00 00 01 32  .....H. .Q.....2
0070 00 00 00 00 01 b2 01 01 32 01 04 01 04 04 4e 41  .....2....NA
0080 4d 45 00 00 00 02 00 00 81 7f 01 16 00 00 00  ME.....
0090 00 00 00 00 01 06 01 06 06 53 41 4c 41 52 59 00  .....SALARY
00a0 00 01 01 00 01 07 07 78 74 09 1a 0e 23 21 01 01  .....x T...#!..
00b0 02 1f e8 01 0a 01 0a 00 06 22 01 02 00 01 32 00  .....".2.
00c0 00 00 07 05 6c 61 72 72 79 02 c4 06 07 04 6d 61  ..larry..ma
00d0 72 6b 02 c4 05 15 01 02 03 07 03 74 6f 6d 02 c4  rk.....tom.
00e0 04 08 01 06 03 1c 57 cb 00 01 03 00 00 00 00 00  .....W.
00f0 00 04 01 01 01 81 01 03 02 05 7b 00 00 01 03 00  .....{.....
0100 03 00 01 20 00 00 00 00 00 00 00 00 00 00 02 00  .....
0110 01 01 00 00 00 00 19 4f 52 41 2d 30 31 34 30 33  .....0 RA-01403
0120 3a 20 6e 6f 20 64 61 74 61 20 66 6f 75 6e 64 0a  ; no dat a found.
```

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 auf 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 vorgeschlagenen 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 wie ein GI Administrator, der keinen direkten Zugriff auf die Datenbank hat, dennoch eine komplette Datenbank kopieren kann und damit theoretisch an alle sensiblen 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