Keep them out of the database !

It all started on Twitter :

Hi Martin 🙂
I hope you are doing well and are ready for DOAG !
I think I stumbled upon some tweet/blogpost from you someday, talking about CMAN.
Do you have any experience to share about CMAN ? I am curious. If you have time during DOAG, I would love to have a chat about it. And if you don't, we can still have a beer and talk about Enterprise Manager 😂
I wish you a nice week-end !
Flora

16 Nov 2018

Hi Flora,
it will be my pleasure to talk with you about CMAN.
I had some experiences in the past - it's a powerful tool if you accept & understand the way it works :-)
I'm looking forward to see you again; that's the real reason to go to conferences!
Also for you a nice and quiet weekend. I'll try to sleep in-advance as DOAG will be hard work :D
cu there,

16 Nov 2018 ✓

Martin Berger

Oracle DBA since 2000

ORACLE ACE

@martinberx

martin.a.berger@gmail.com

http://berxblog.blogspot.com

Flora Barriele

8 years in IT, 3 years DBA

French living in Switzerland

Geek Girls Carrots

ORACLE ACE Associate

@floo_bar

https://floobar0.wordpress.com

Ask network admins to filter with firewall ?

Ask network admins to filter with firewall ?

Ask network admins to filter with firewall ?

Use a dedicated listener for each instance ?

Ask network admins to filter with firewall ?

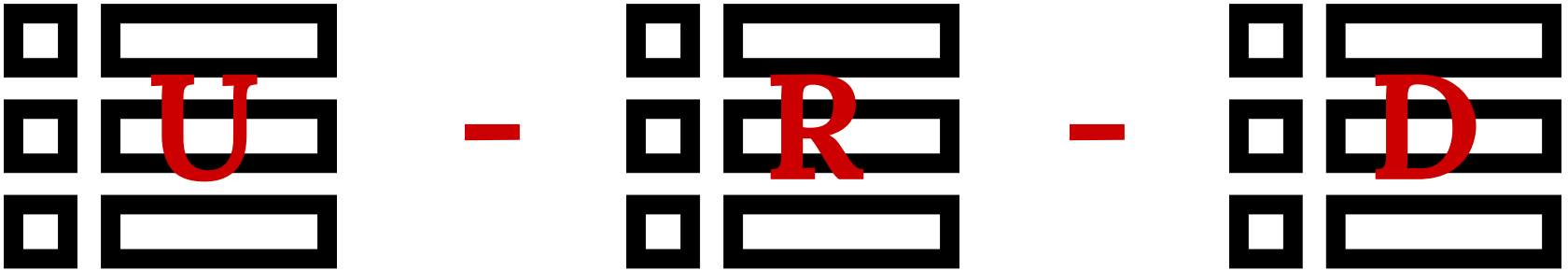
Use a dedicated listener for each instance ?

600+ databases

65 hosts

How to handle the situation better ?

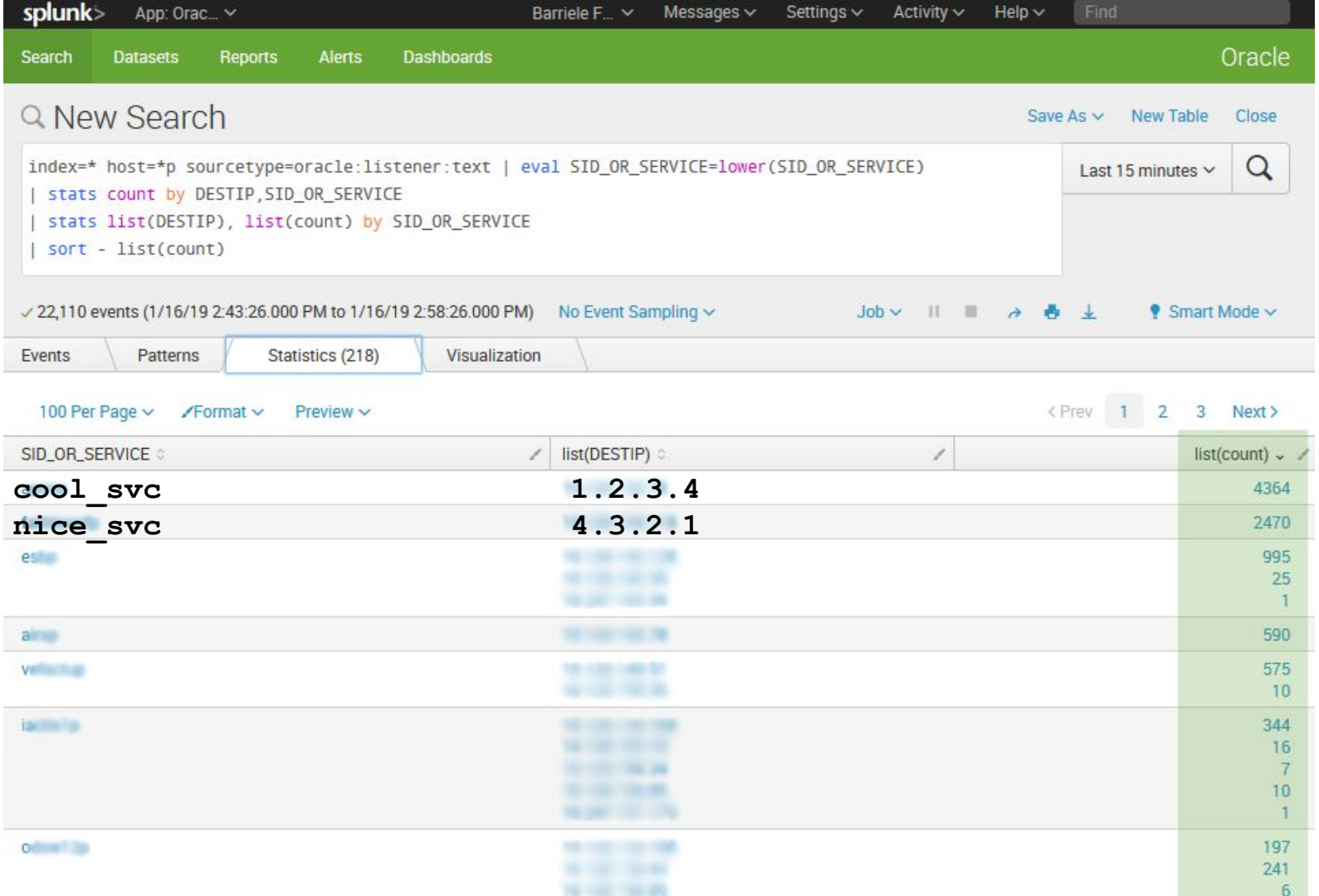
How to handle the situation better ?



How to handle the situation better ?

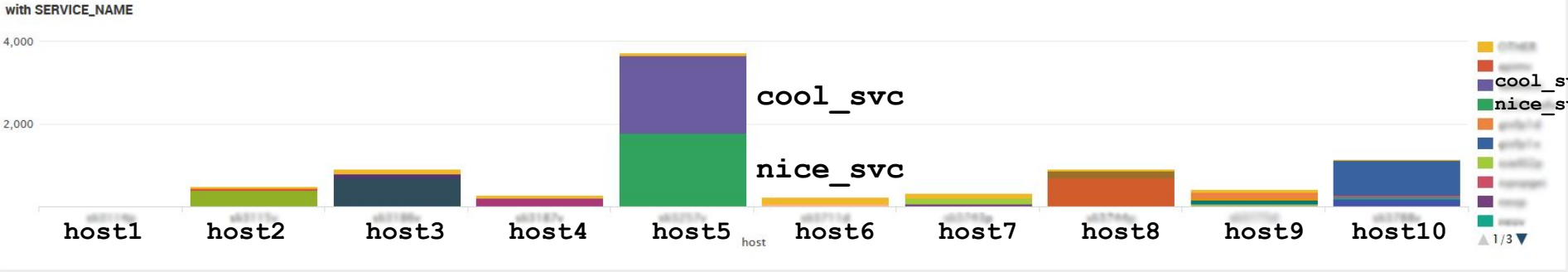
- Understand your ecosystem
  - Example :

Splunk + listener.log = 


splunk> App: Orac... Barriele F... Messages Settings Activity Help Find
Search Datasets Reports Alerts Dashboards Oracle
New Search
Save As New Table Close
index=* host=*p sourcetype=oracle:listener:text | eval SID_OR_SERVICE=lower(SID_OR_SERVICE)
| stats count by DESTIP,SID_OR_SERVICE
| stats list(DESTIP), list(count) by SID_OR_SERVICE
| sort - list(count)
Last 15 minutes
22,110 events (1/16/19 2:43:26.000 PM to 1/16/19 2:58:26.000 PM) No Event Sampling Job Smart Mode
Events Patterns Statistics (218) Visualization
100 Per Page Format Preview
Prev 1 2 3 Next
SID_OR_SERVICE list(DESTIP) list(count)
cool_svc 1.2.3.4 4364
nice_svc 4.3.2.1 2470
995
25
1
590
575
10
344
16
7
10
1
197
241
6

Connections to production databases

Show Filters | Edit | Export | ...



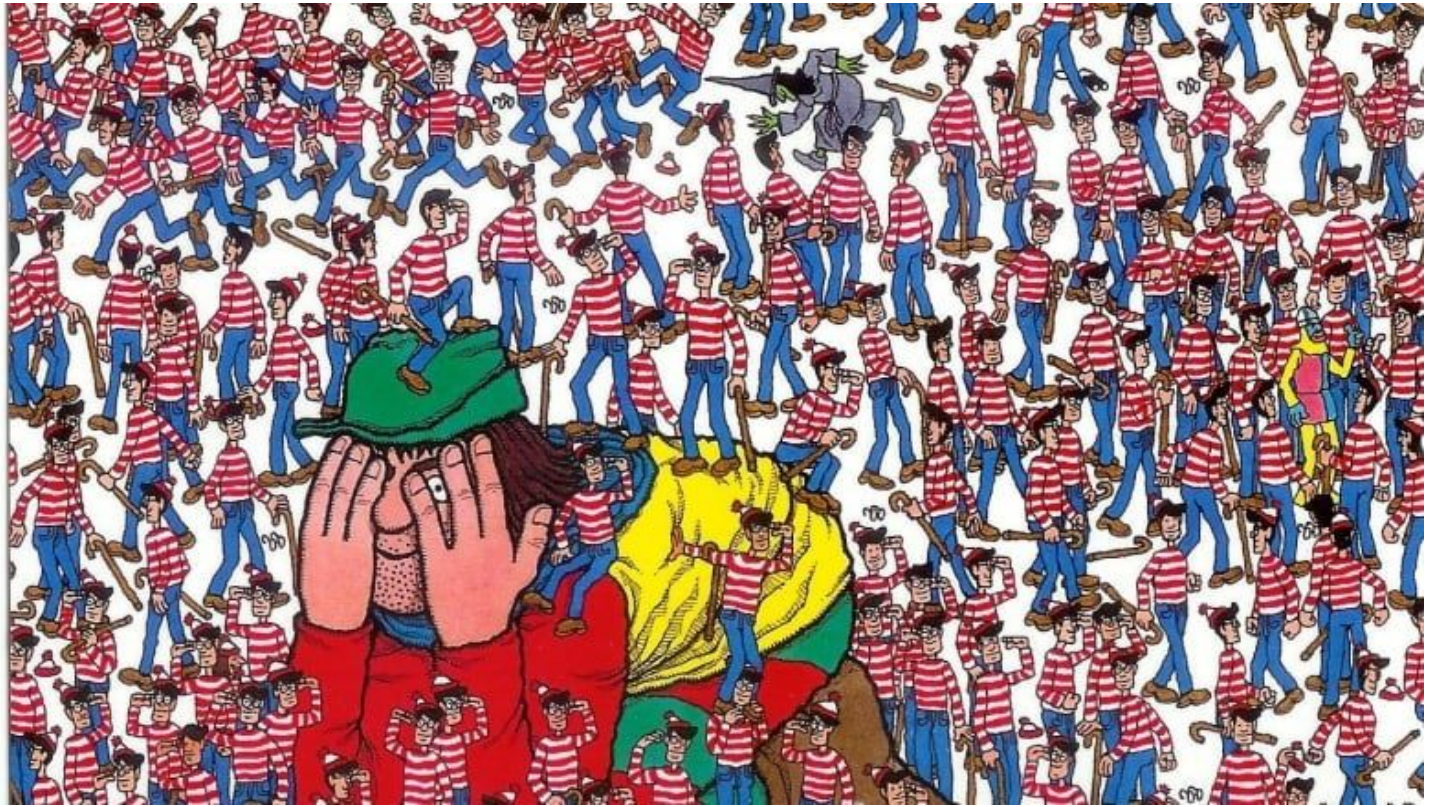
How to handle the situation better ?

- ... and most important :

Choose a solution

that fits your needs

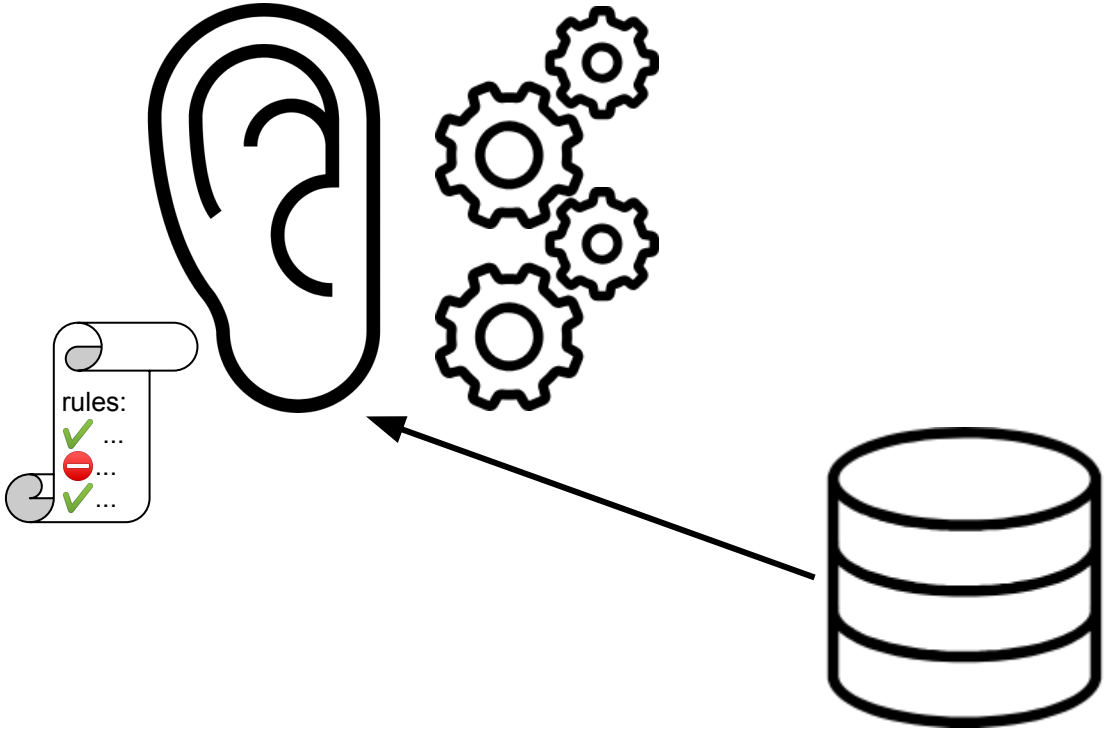
What’s the problem ?



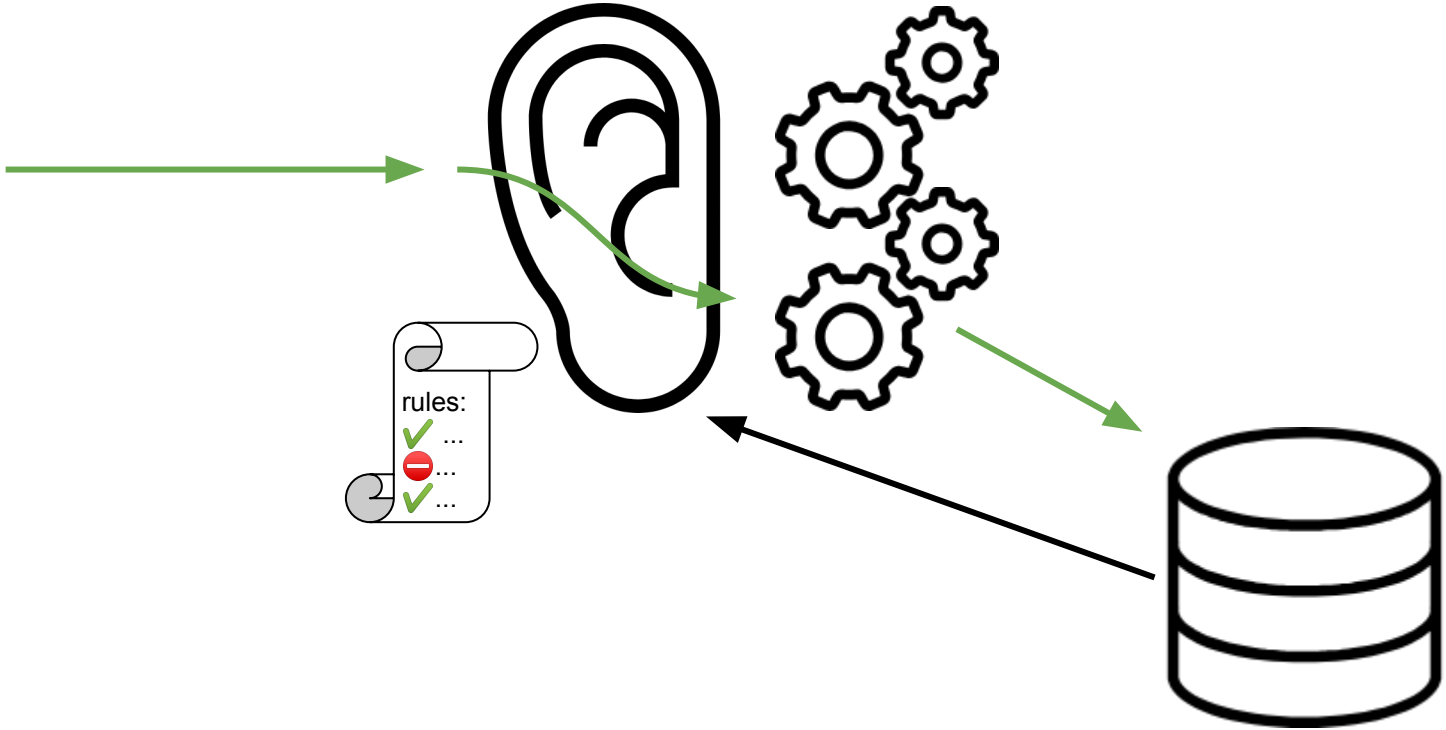
Connection Manager

Connection Manager

Connection Manager



Connection Manager



Example: connection refused

- rules
  - (rule=(src=oracledev)(dst=127.0.0.1)(srv=cmon)(act=accept))

- errors
  - reject
  - drop
  - no service

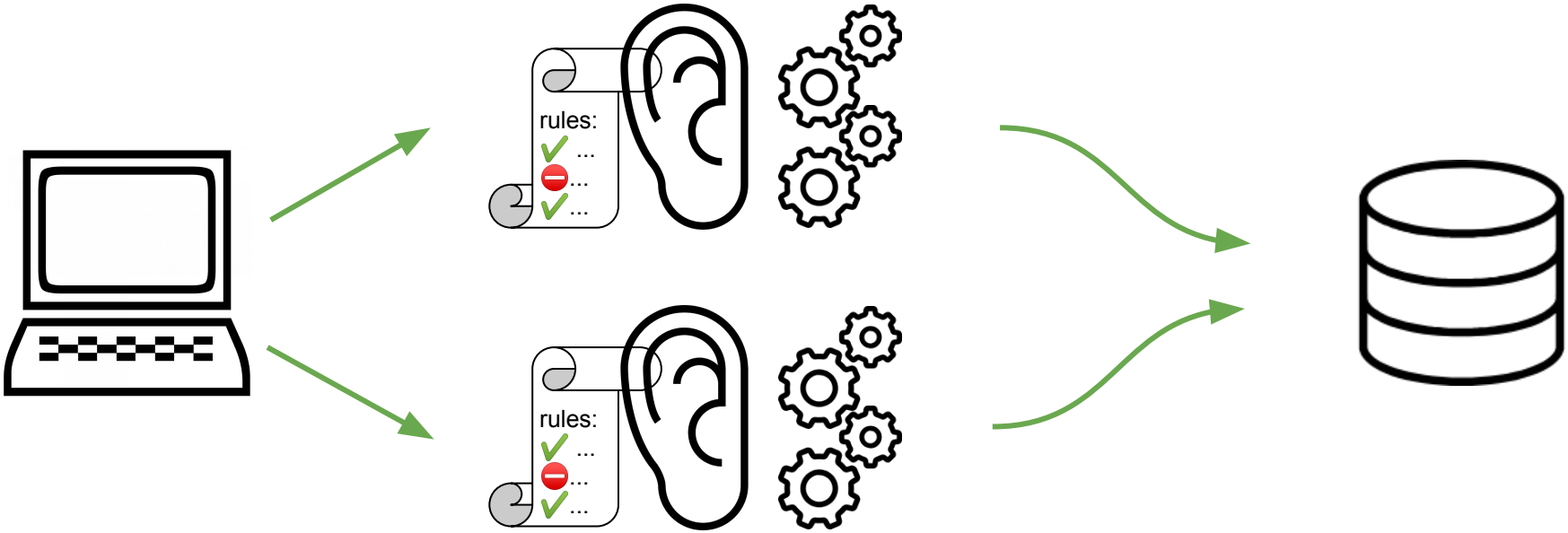
Example: connection refused

- rules
  - (rule=(src=oracledev)(dst=127.0.0.1)(srv=cmon)(act=accept))
    - src & dst: hostname or net/mask
    - srv: service
    - act: accept, reject, drop
- errors
  - reject -
  - drop -
  - no service -

Example: connection refused

- rules
  - (rule=(src=oracledev)(dst=127.0.0.1)(srv=cmon)(act=accept))
    - src & dst: hostname or net/mask
    - srv: service
    - act: accept, reject, drop
- errors
  - reject – ORA-12529: TNS:connect request rejected based on current
  - drop – ORA-12537: TNS:connection closed
  - no service – ORA-12514: TNS:listener does not currently know of service requested in connect descriptor

High Availability

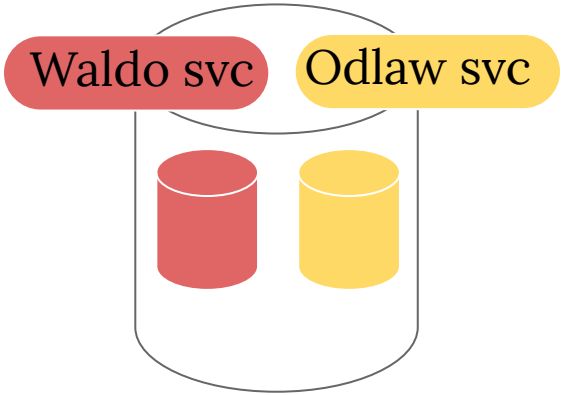


High Availability

- tnsnames.ora
  - net_service_name=(DESCRIPTION=
    (ADDRESS_LIST=
    (LOAD_BALANCE=on)
    ADDRESS=((PROTOCOL=tcp)(HOST=cman1)(PORT=1521))
    ADDRESS=((PROTOCOL=tcp)(HOST=cman2)(PORT=1521))
) (CONNECT_DATA=(SERVICE_NAME=DB1)))

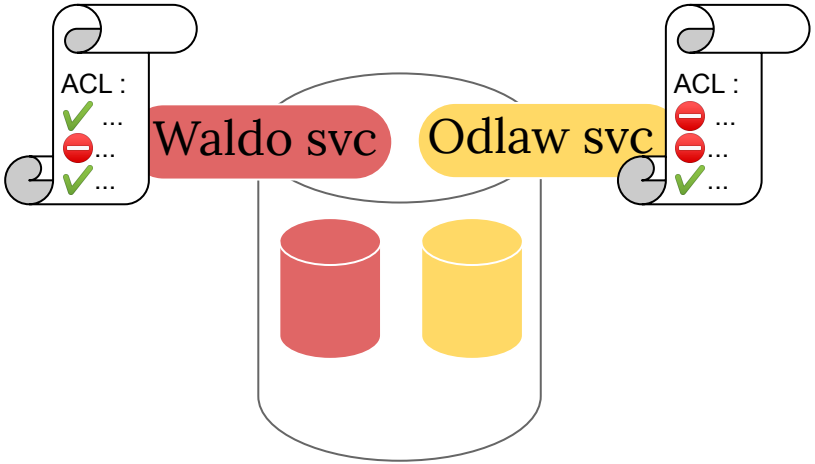
Database Firewall Service - ACL

Concept



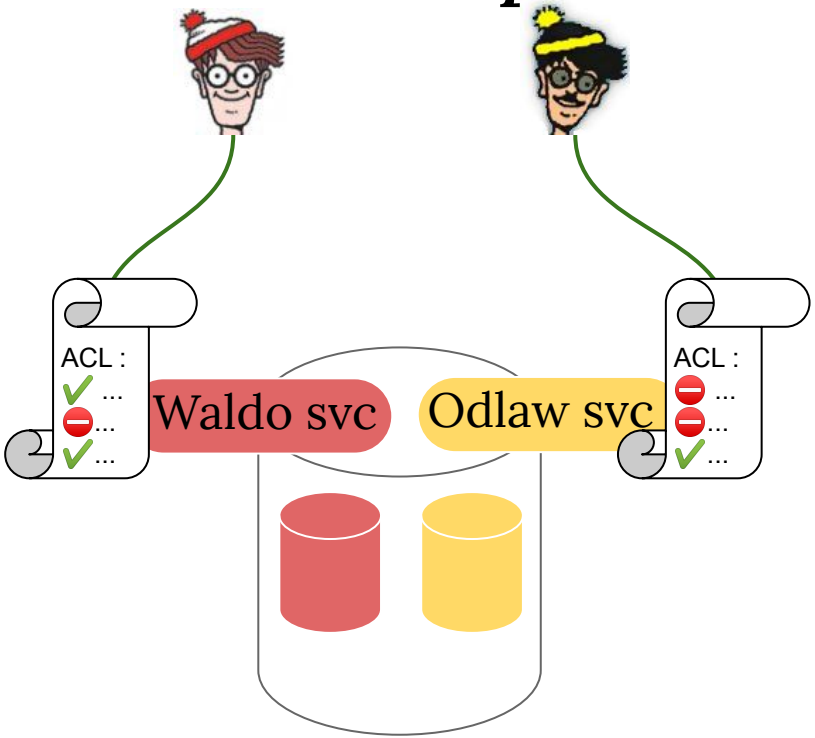
NEW IN
12.2

Concept



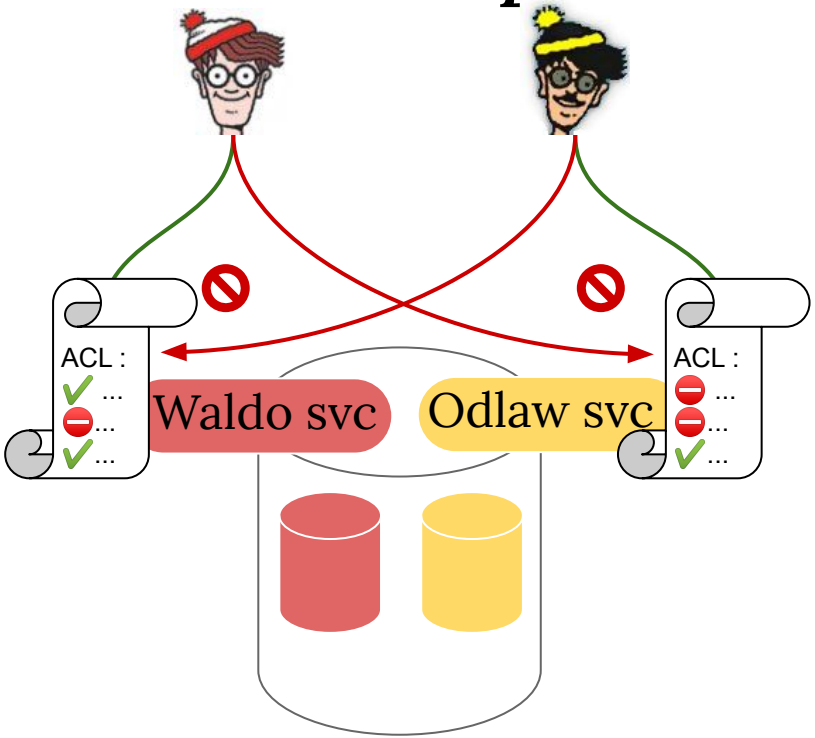
NEW IN
12.2

Concept



NEW IN
12.2

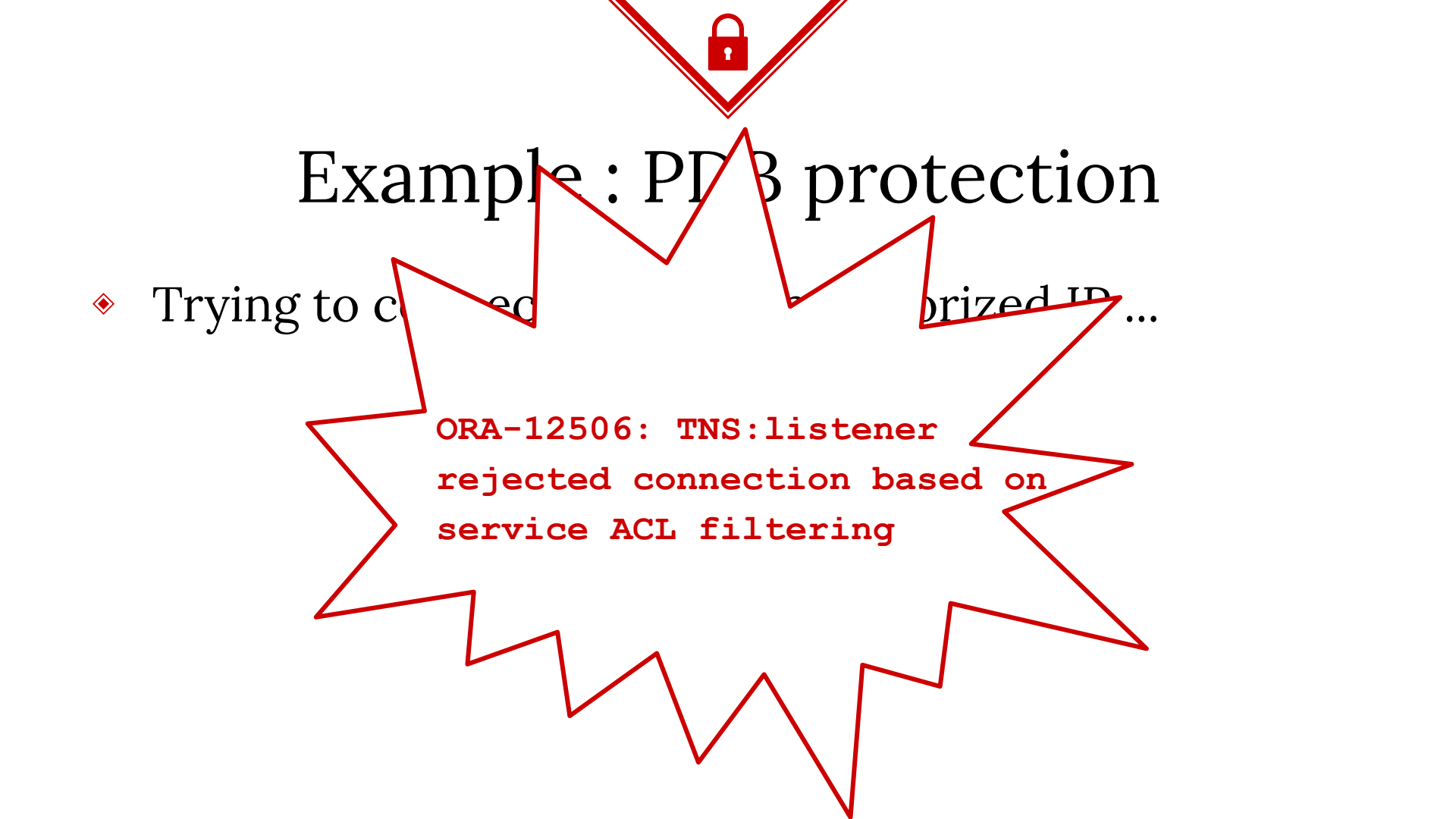
Concept



NEW IN
12.2

Example : PDB protection

- Trying to connect with an unauthorized IP ...



Example : PDB protection

- Trying to c ed orized ID ...

ORA-12506: TNS:listener rejected connection based on service ACL filtering

Why use ACL ?

- Fine-grained access control on each DB/PDB

but

- Decentralized management

Logon triggers

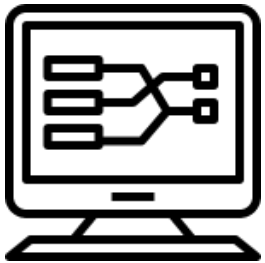
Concept

Concept

- User hostname / OS username
- OS Terminal
- User Application Module
- User IP Address

Concept

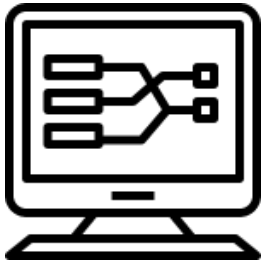
- User hostname / OS username
- OS Terminal
- User Application Module
- User IP Address



- Have a map table to describe what is allowed

Concept

- User hostname / OS username
- OS Terminal
- User Application Module
- User IP Address

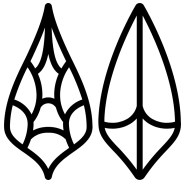


- Have a map table to describe what is allowed

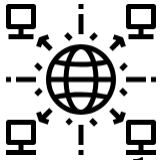
- Create a trigger to check if conditions are met before allowing connection

```
CREATE OR REPLACE TRIGGER TRG_FILTER_LOGON
    AFTER LOGON ON DATABASE
[...]
BEGIN
    [... perform checks from map table and insert result into V_CHECK ...]
    IF (V_CHECK <> 0)
    THEN
      NULL; --OK
    ELSE
      RAISE_APPLICATION_ERROR(-20000, 'YOU ARE NOT AUTHORIZED TO LOGIN WITH THIS
USERNAME. PLEASE CONTACT YOUR SECURITY MANAGER.');
    END IF;
[...]
END;
/
```

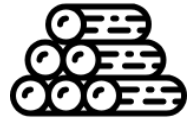
Why use logon triggers ?



but

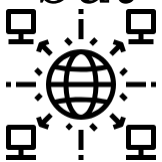


and



Why use logon triggers ?

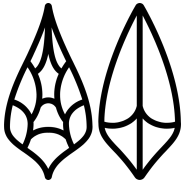
but



and

- Don’t forget to log rejections

Why use logon triggers ?



but

- Decentralized management too

and

- Don’t forget to log rejections

Why use logon triggers ?

- Works with older database versions

but

- Decentralized management too

and

- Don’t forget to log rejections

Audit & reports

Audit

Audit

conventional

logon

users manager

Audit

conventional

unified
(since 12.1, but don't use < 12.2!

logon

logoff
dml

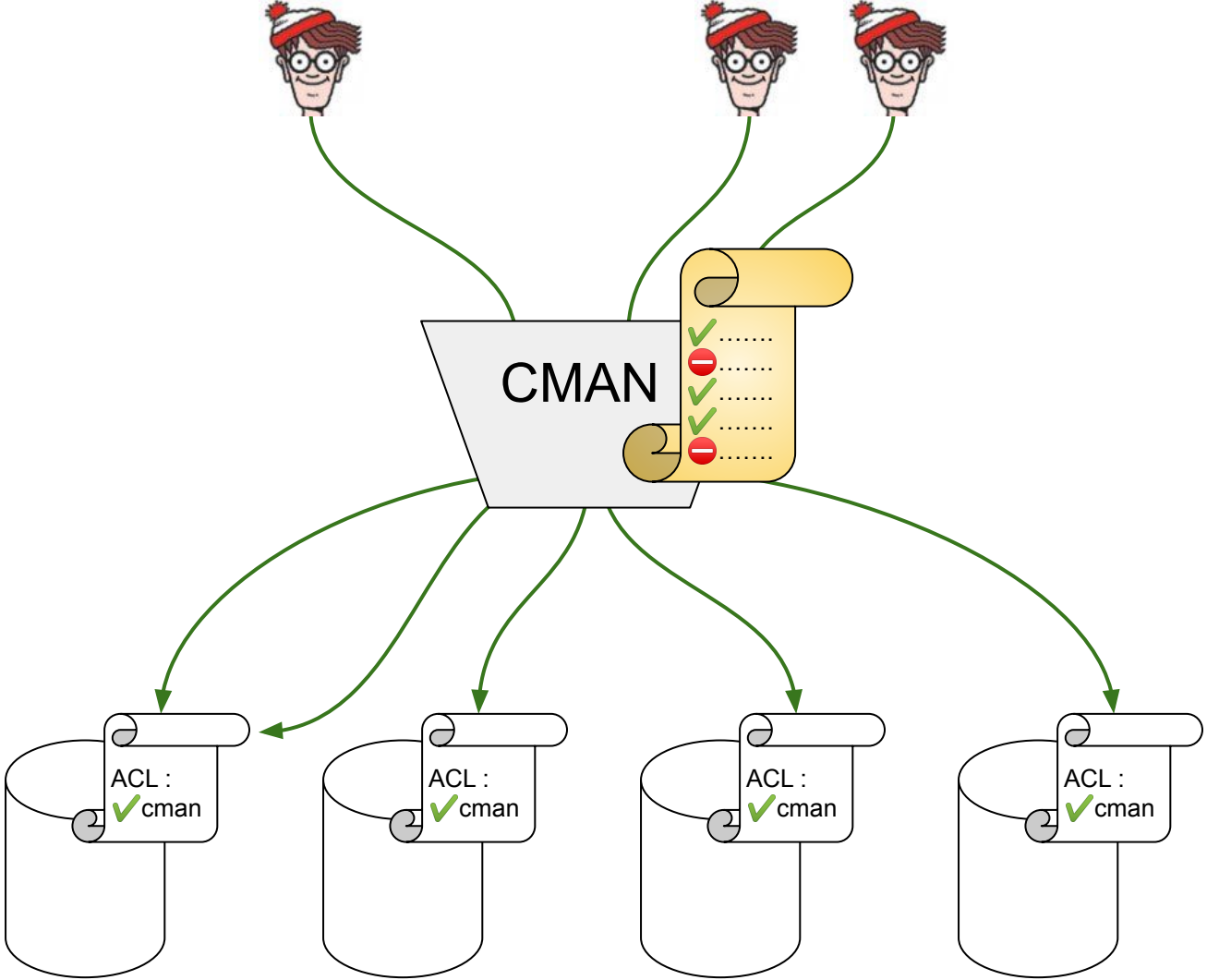
users manager

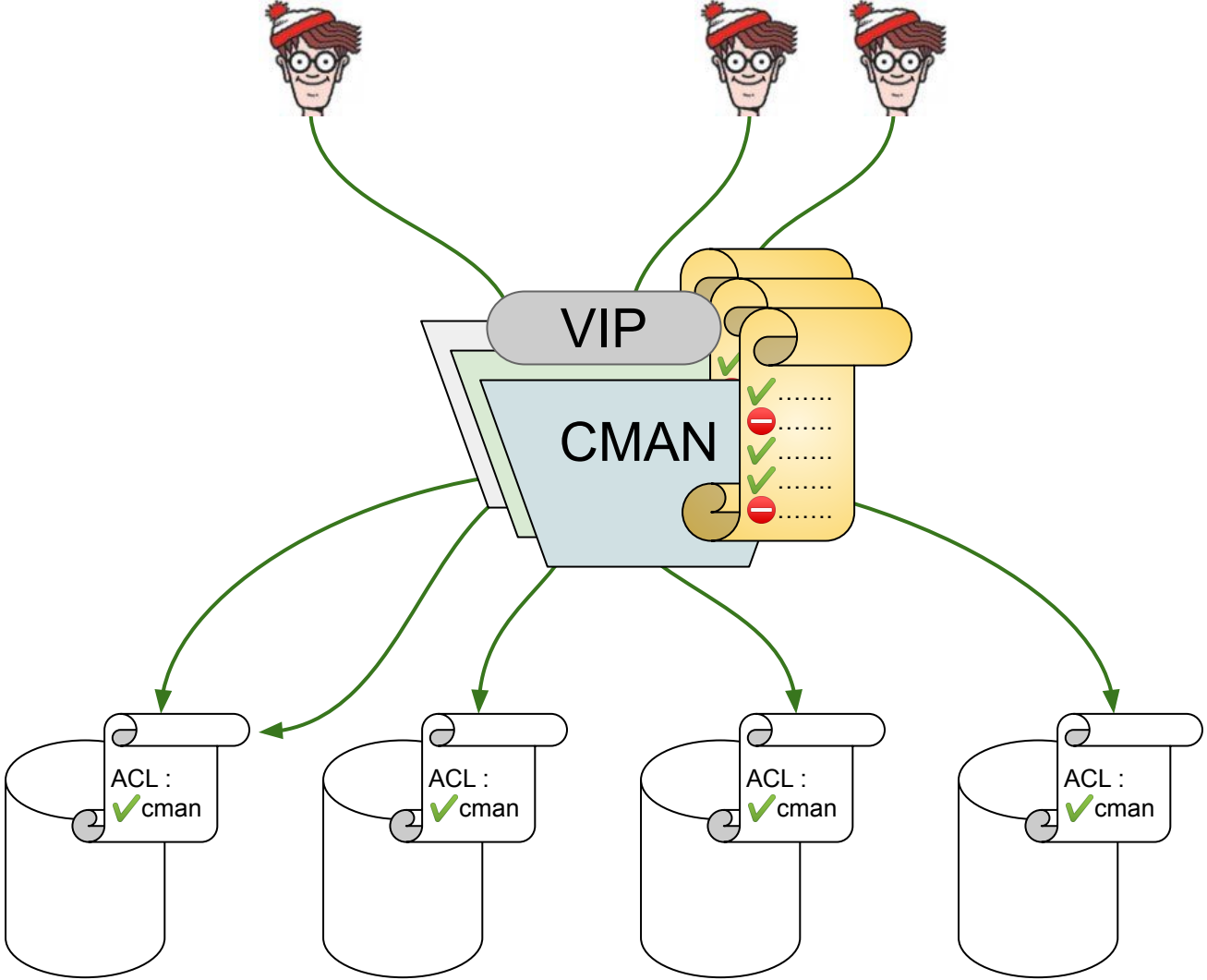
application manager
security manager

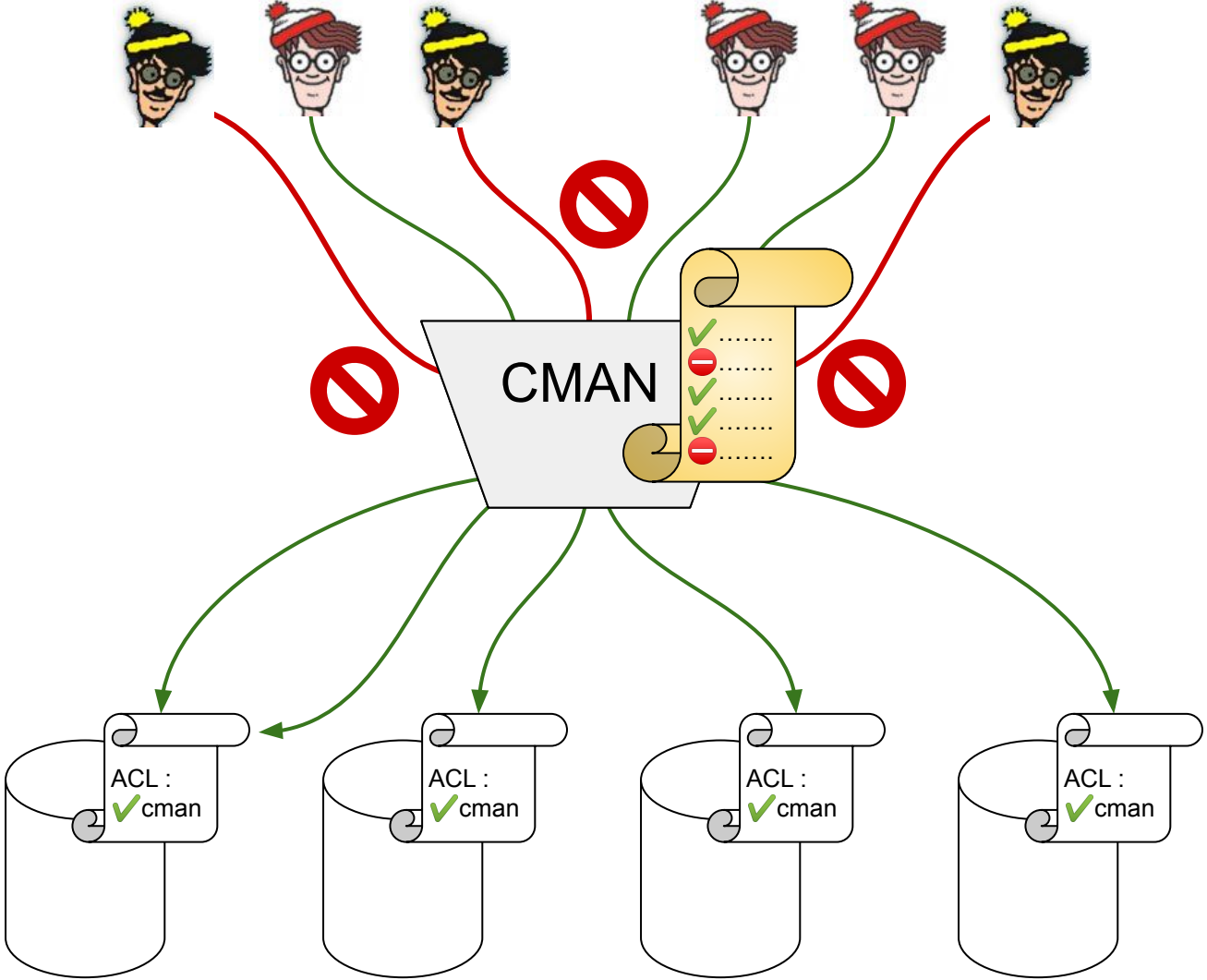
Connection Manager + ACL

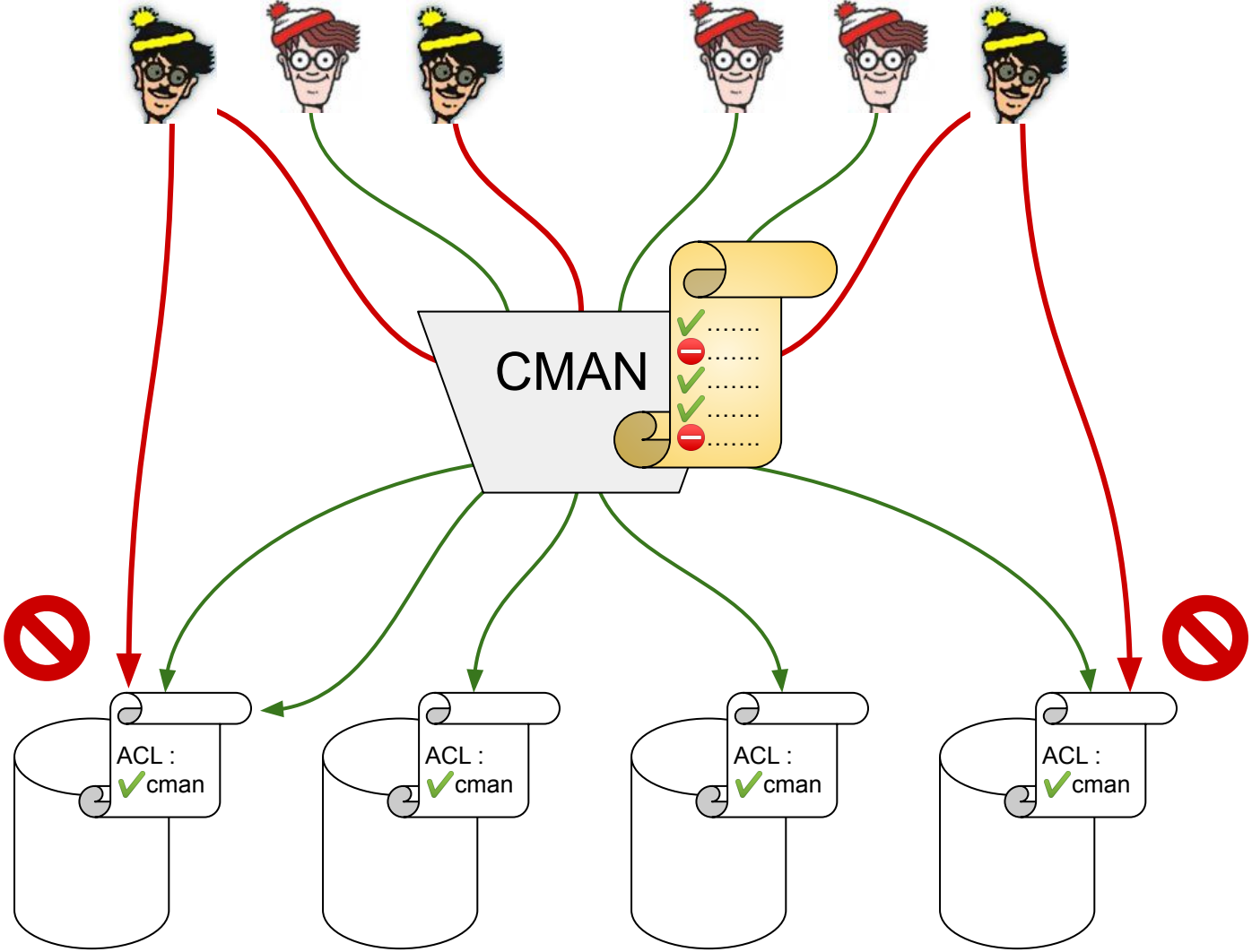
Looks like we are on the right track ...

CMAN + ACL


CMAN
ACL :
cman
ACL :
cman
ACL :
cman
ACL :
cman


VIP
CMAN
ACL :
cman
ACL :
cman
ACL :
cman
ACL :
cman


CMAN
ACL :
cman
ACL :
cman
ACL :
cman
ACL :
cman


CMAN
ACL :
cman
ACL :
cman
ACL :
cman
ACL :
cman

... but who takes decision about security policies ?

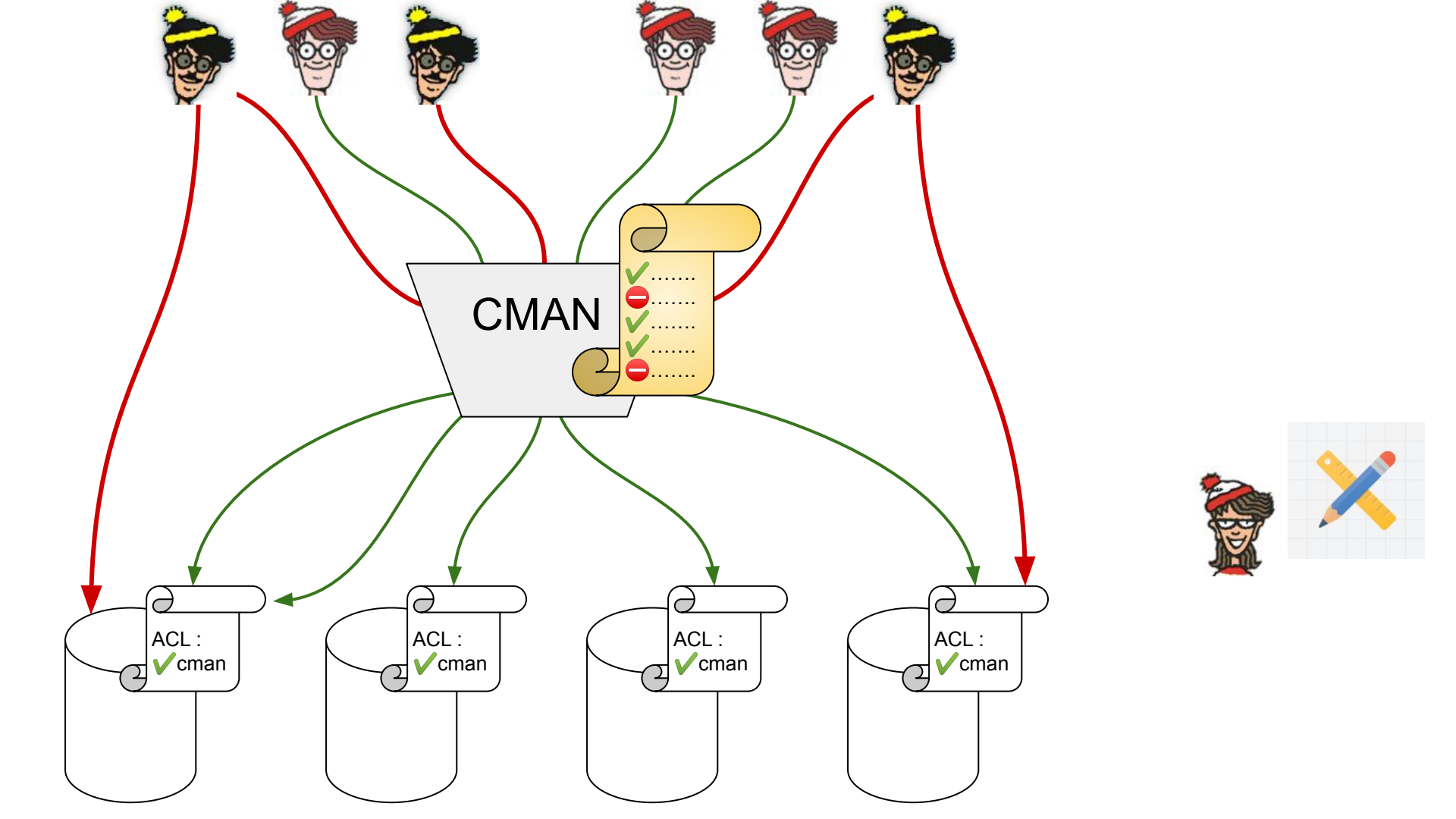
- DBAs ?

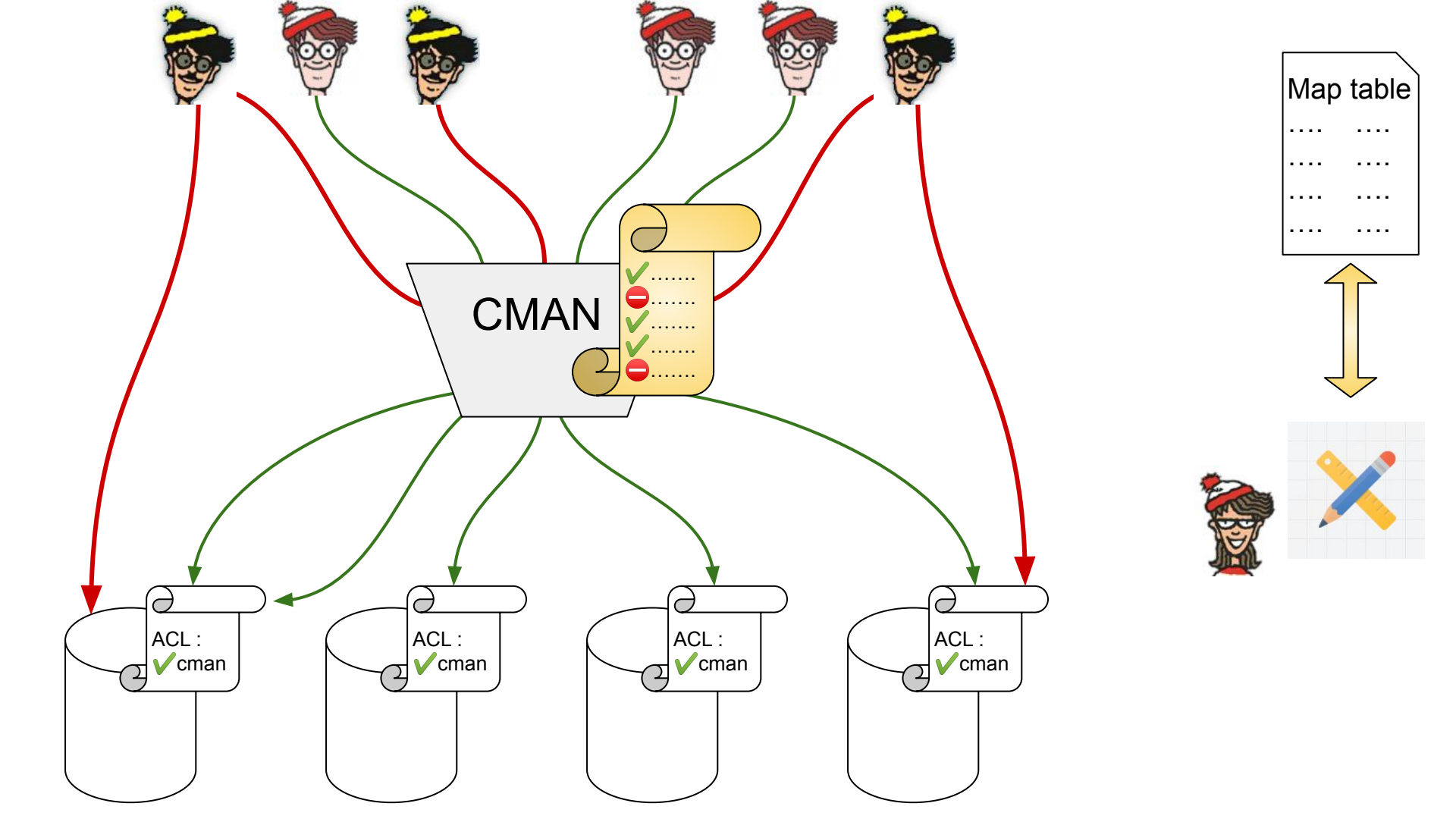
… but who takes decision about security policies ?

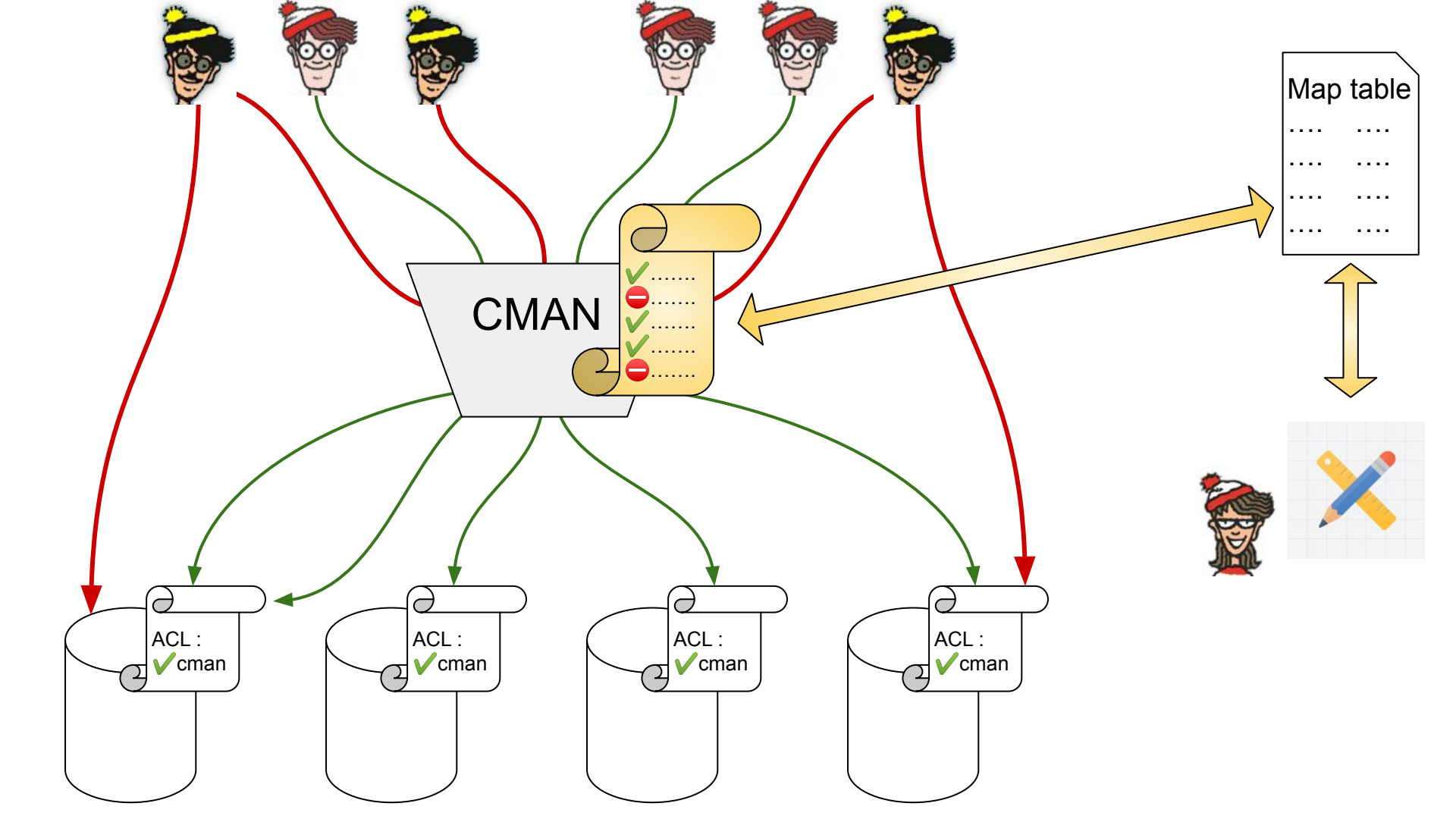
- DBAs ?

Security policies management

- Give the responsibility back to the security team
  - Example with :


CMAN
ACL :
cman
ACL :
cman
ACL :
cman
ACL :
cman


CMAN
ACL :
cman
ACL :
cman
ACL :
cman
ACL :
cman
Map table


Map table
CMAN
ACL :
cman
ACL :
cman
ACL :
cman
ACL :
cman

Map table example

- From this ...

```
(rule_list=
    (rule=(src=1.2.3.4/16)(dst=destinationHost1)(srv=cool_svc)(act=accept))
    (rule=(src=5.6.7.8/16)(dst=destinationHost2)(srv=nice_svc)(act=accept))
    (rule=(src=privilegedServer)(dst=destinationHost3)(srv=*)(act=accept))
    [...]
    (rule=(src=*)(dst=*)(srv=*)(act=reject))
)
```

Map table example

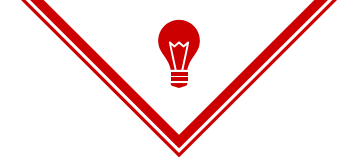
- To this ...

CMAN_RULES	
ID	NUMBER
SOURCE	VARCHAR2 (255 CHAR)
DESTINATION	VARCHAR2 (255 CHAR)
SERVICE	VARCHAR2 (500 CHAR)
ACTION	VARCHAR2 (10 CHAR)
RULE_ORDER	NUMBER
DESCRIPTION	VARCHAR2 (500 CHAR)
UPDATE_DATE	DATE

ID	SOURCE	DESTINATION	SERVICE	ACTION	RULE_ORDER	DESCRIPTION	UPDATE_DATE
1	x.x.x.x/16	destinationHost1	cool_svc	accept	1	Subnet x.x.x.x/16 can access service cool_svc on host destinationHost1	2019-05-06...
2	y.y.y.y/16	destinationHost2	nice_svc	accept	2	Subnet y.y.y.y/16 can access service nice_svc on host destinationHost2	2019-03-26...
3	privilegedServer	destinationHost3	*	accept	3	privilegedServer can access all services on destinationHost3	2019-04-06...
5	*	*	*	reject	999	Reject all other connections	2019-03-19...

Remember …

- Centralised deployment on CMANs only
- Simple config on all DB servers
- Know your environment before implementing
- Keep your solution(s) as simple as possible
- There is not one solution “to rule them all”
- Techies … must juggle a lot of non-tech problems



Thanks!

Any thoughts?

Martin Berger
martin.a.berger@gmail.com

Flora Barriele
flora.barriele@gmail.com