

TAFORA

ORACLE au quotidien

White Papers
TAFORA
pour ORACLE
7,8,8i,9i

Accéder à une base derrière un firewall depuis le Web

DRAFT 2.10.502 - 03/01/2004 15:33

Préservez vos données! Où cassons l'os pour avoir la moelle!

1 Table de matières

1	TABLE DE MATIERES.....	2
2	ACCEDER A UNE BASE DERRIERE UN FIREWALL DEPUIS LE WEB	3
2.1	PROBLEMATIQUE	3
2.2	PERIMETRE DE LA SOLUTION.....	3
2.3	CADRE GLOBAL TECHNIQUE	3
2.4	EXEMPLE PRATIQUE	4
2.4.1	<i>Installer CMAN</i>	<i>4</i>
2.4.2	<i>CMAN.ORA.....</i>	<i>4</i>
2.4.3	<i>Tnsnames.ora.....</i>	<i>5</i>
2.4.4	<i>Administrer le demon cman.....</i>	<i>5</i>

2 Accéder à une base derrière un firewall depuis le Web

2.1 Problématique

Il est parfois nécessaire d'accéder à une base Oracle située derrière un firewall. Bien que les connexions standards (1521, 1526, etc) puissent être permises en libérant ces ports, les réponses des process serveurs Oracle s'effectuent sur d'autres ports, se trouvant bloquées par le firewall. Pour permettre l'utilisation d'un port ou ensemble de ports prédéfinis pour les réponses, une solution est d'utiliser CMAN (Connexion Manager).

2.2 Périmètre de la solution

CMAN est un process intermédiaire qui aiguille les tentatives de connexions ainsi que les réponses des process serveurs vers un même port prédéfini. Il a un comportement de routeur. CMAN est servi par deux process,

- CMGW (Connection Manager GateWay) qui reçoit les connexions clientes et détermine si l'accès est autorisé, suivant les règles définies dans le fichier de configuration cman.ora. Ce processus initialise les connexions au Listener pour le client et assure le relais entre le client et le serveur. CMGW s'enregistre auprès du processus administratif CMADMIN.
- CMADMIN gère les fonctions administratives de CMAN.

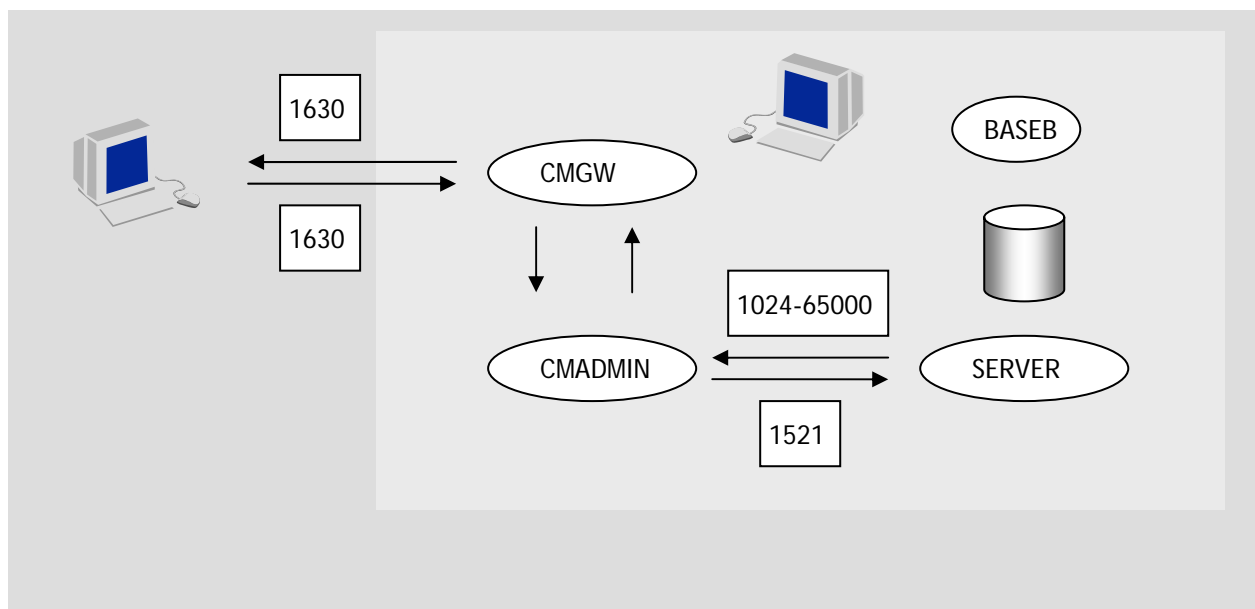


Figure 1 Routage des connexions CMAN

La configuration de CMAN est gérée par le fichier `$TNS_ADMIN/cman.ora` (généralement `$ORACLE_HOME/network/admin/cman.ora`).

2.3 Cadre global technique

- Livrer une adresse fixe pour que le client sache où se connecter. Le serveur en question a soit une adresse fixe, soit une adresse mobile, auquel cas utiliser un redirecteur quelconque (dyndns, par exemple)
- Ouvrir un port dans le firewall (le mien est un firewall incorporé dans mon routeur, un Netgear)
- Faire en sorte que la réponse du processus serveur se fasse entendre par le client (qu'elle ne soit pas bloquée, vu qu'elle arrive sur un autre port, fermé par le routeur)
- Bloquer les accès indésirables sur le serveur Oracle

2.4 Exemple pratique

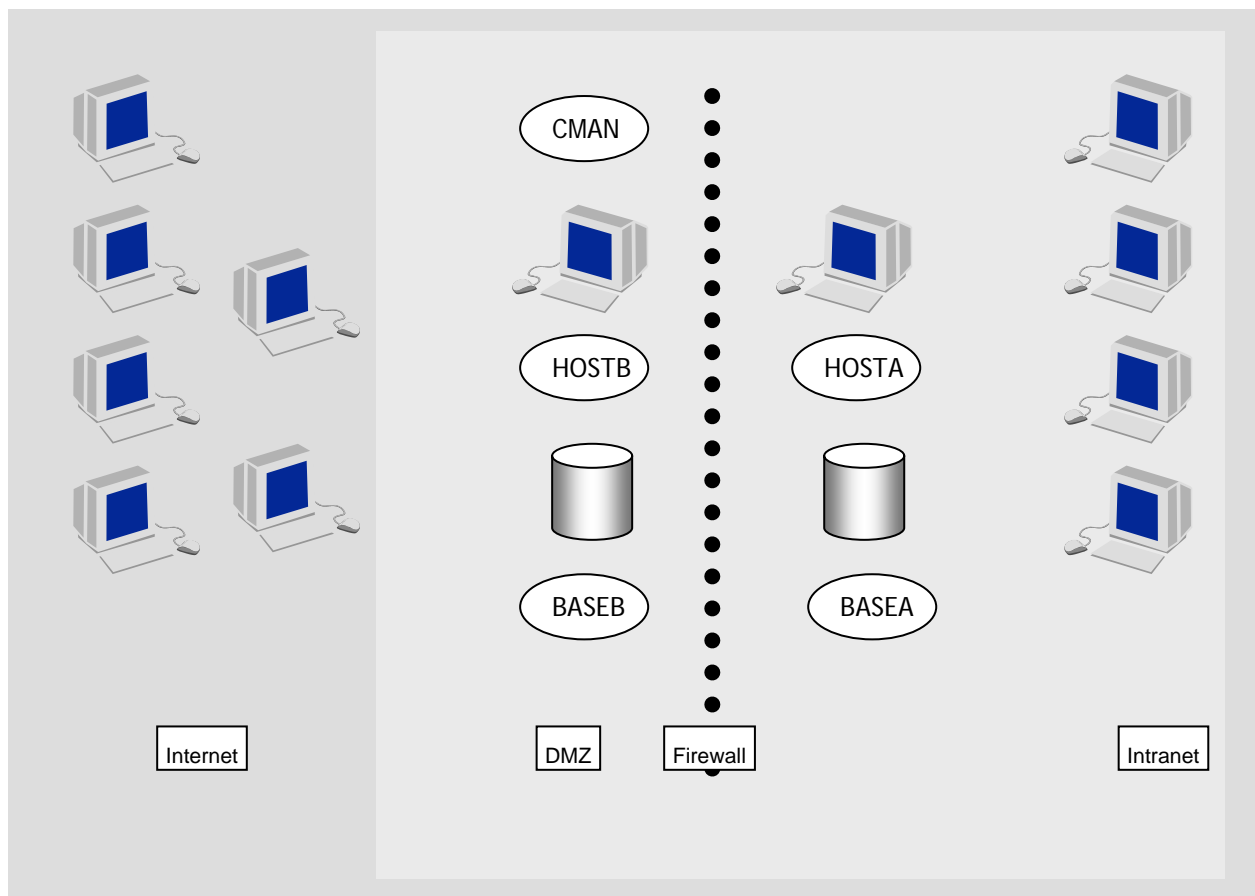


Figure 2 Une configuration Oracle derrière/devant un firewall

2.4.1 Installer CMAN

En fonction de la version d'Oracle, CMAN est installé ou pas ! Pour 9i, l'installation n'est pas effectuée par défaut lors de l'installation Oracle. Utiliser Oracle Universal Installer pour le récupérer (Installation de Oracle Database/Personnalisée/Composants/Oracle Net Services/Oracle Connection Manager). Après l'installation, patcher et exécuter catpatch.sql.

2.4.2 CMAN.ORA

```

cman =
  (ADDRESS_LIST=
    (ADDRESS=(PROTOCOL=tcp)(HOST=Nom_Local_Machine_Du_Serveur)
      (PORT=1630)(QUEUE_SIZE=32)
    )
  )
cman_admin = (ADDRESS=(PROTOCOL=tcp)(HOST=Nom_Local_Machine_Du_Serveur)
  (PORT=1830))
cman_profile =
  (parameter_list=
    (MAXIMUM_RELAYS=1024)LOG_LEVEL=0)(TRACING=no)(RELAY_STATISTICS=yes)
    (SHOW_TNS_INFO=yes)(USE_ASYNC_CALL=yes)AUTHENTICATION_LEVEL=0)
    (REMOTE_ADMIN=FALSE)(ANSWER_TIMEOUT=30)
  )
# firewall proxy TCP
cman_rules =
  (rule_list=
    (rule=(src=IPPermise)(dst=Nom_Local_Machine_Du_Serveur)
      (srv=Nom_Instance_Recherchee)(act=accept))
  )

```

Figure 3 Exemple de cman.ora

2.4.3 Tnsnames.ora

Le client qui désire se connecter à cette base, doit avoir renseigné les informations suivantes dans tnsnames.ora (dans cet exemple, la connexion à une même base est réalisée d'une manière classique et via cman). Le client pourra utiliser les deux, en sachant que la connexion via cman est ralentie :

```
Nom_Instance_Recherchee =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = Nom_Local_Machine_Du_Serveur)(PORT = 1521))
  )
(CONNECT_DATA =
  (SERVICE_NAME = Nom_Instance_Recherchee)
)
)
Cman.Nom_Instance_Recherchee =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = Nom_Public_Machine_Du_Serveur)(PORT = 1630))
    (ADDRESS = (PROTOCOL = TCP)(HOST = Nom_Local_Machine_Du_Serveur)(PORT = 1521))
  )
  (SOURCE_ROUTE = yes)
  (CONNECT_DATA =
    (SERVICE_NAME = Nom_Instance_Recherchee)
  )
)
)
```

Le nom public de la machine est nécessaire pour une connexion via Internet, par exemple, auquel cas le routeur devrait router les connexions au port 1630 vers la machine en question. A la place du *Nom_Public_Machine_Du_Serveur*, nous pouvons utiliser *Nom_Local_Machine_Du_Serveur*, si la connexion reste sur l'intranet. Le firewall ne verra pas les connexions 1521, enrôlées dans le port 1630.

2.4.4 Administrer le demon cman

L'arrêter

```
cmctl stop cman
```

Le demarrer

```
cmctl start cman
```

Son statut

```
cmctl status
```

Les statistiques

```
cmctl stats
```

Lors de la modification des paramètres cman, il est parfois nécessaire d'arrêter et redémarrer le listener.
