Oracle Database Connection Manager Support for the PROXY Protocol

CMAN support for the PROXY protocol lets application IP addresses be passed through load balancers to enable access control rules and logging

3 March 2023, Version 1.1

Public

Using the PROXY protocol with CMAN

This paper describes how to configure Oracle Connection Manager (CMAN) with PROXY protocol support when CMAN is specified as the backend of a load balancer.

CMAN is a proxy server that forwards connection requests to databases or other proxy servers. Using a load balancer with CMAN allows application load to be distributed across multiple CMAN instances while exposing a unified address to client applications. The model also allows for horizontal scaling of CMAN instances based on the workload.

The PROXY protocol provides a convenient way to pass connection information across multiple layers of NAT or TCP proxies. It allows client application IP addresses to be passed through to CMAN so access rules can be enforced. Without the PROXY protocol, only the load balancer IP address is available to CMAN.

PROXY protocol support is available with CMAN on non-Windows platforms from Oracle Database 21c onwards. It can be used in Oracle Cloud or with on-premise deployments. Both PPv1 and PPv2 are supported.

Figure 1 shows CMAN deployed behind a load balancer with the PROXY protocol enabled on port 1.

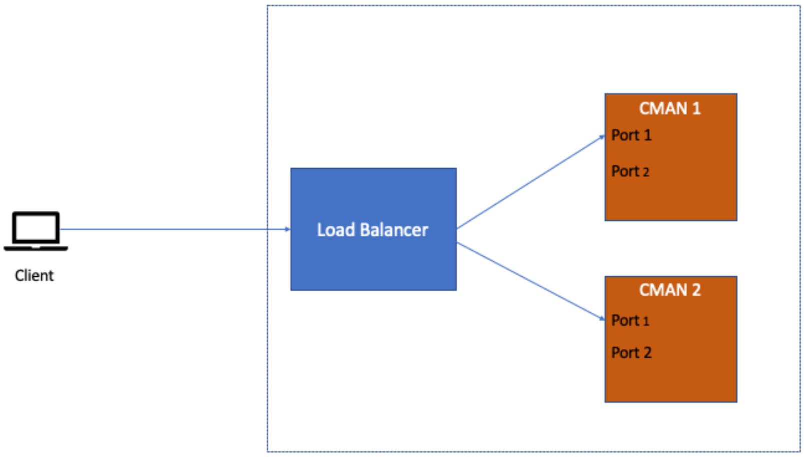

Figure 1. CMAN behind a load balancer. The PROXY protocol is enabled on port 1.

Enabling the PROXY protocol on CMAN

To enable the PROXY protocol in CMAN, add `expected_proxies` to the listen address for the port that receives the PROXY protocol. The IPs in `expected_proxies` should contain all load balancer IP addresses that the load balancers use to connect to CMAN. Care should be taken to restrict the list to only load balancers nodes because CMAN will trust the proxy protocol bits coming from these IP addresses.

For CMAN control operations, another listen address that does not have `expected`_proxies specified should be added to `cman`.ora. This address should appear before the address with `expected` proxies.

If Dynamic Registration is used, then `remote`_listener on the database tier should be set to a non-proxy endpoint of CMAN. This is needed because registration is not supported when the PROXY protocol is used.

A sample cman.ora with the PROXY protocol enabled on port 5435 is:

```
cman_1 =
  (CONFIGURATION =
    (ADDRESS_LIST =
      (ADDRESS=(HOST=host1)(PROTOCOL=tcp)(PORT=5433))
      (ADDRESS=(HOST=host1)(PROTOCOL=tcp)(PORT=5435)
(EXPECTED_PROXIES=10.250.220.139))
  )
  (RULE_LIST =
    (rule=(src=*)(dst=127.0.0.1)(srv=cmon)(act=accept)
(action_list=(mct=0)))
    (rule=(src=10.85.86.210)(dst=*)(srv=service1)
(act=accept)(action_list=(mct=0)))
  )
  (PARAMETER_LIST=
    (max_connections=512)
    (min_gateway_processes=5)
    (max_gateway_processes=20)
  )
)
```

The CMAN log file can be verified to see that the actual client IP address is seen. A sample entry in the CMAN log for a connection is:

```
03-JUN-2021 03:32:16 *
(connect_data=(service_name=service1)(CID=(PROGRAM=java)
(HOST= )(USER=john))) * (ADDRESS=(PROTOCOL=tcp)
(HOST=10.85.86.210)(PORT=18025)(PEER_PROXY_IP=10.0.0.8)
(PEER_PROXY_PORT=13768)) * establish * service1 * 0
```

Here, 10.85.86.210 is the actual client application IP address. The port 18025 is the actual client port. `PEER_PROXY_IP` is the IP of the load balancer. `PEER_PROXY_PORT` is the port used on the load balancer.

Enabling the PROXY protocol on a load balancer

Load balancers such as HAProxy and Nginx require their own specific configuration to enable sending the PROXY protocol to the CMAN backend.

Some load balancers like F5 already support client IP address preservation. In such cases the PROXY protocol may not be required.

The configurations shown below are only for illustration. Review your load balancer documentation for details.

HAProxy

For HAProxy the configuration needs to have `send-proxy` or `send-proxy-v2` when specifying the backend. For example:

```
server s1 backend.example.com:1523  send-proxy-v2  check
```

NGinx

For Nginx, `proxy_pass` can be specified in the backend server configuration:

```
server {
    listen *:1521
    proxy_pass backend.example.com:1523
    proxy_protocol_version 2
}
```

Switching off health check log entries

Some load balancers may periodically do a health check by issuing a socket level connect to CMAN followed by disconnect. This can generate an error entry in the CMAN log file. Logging can be disabled by setting the parameter `log_suppress_nodes` in cman.ora, for example:

```
log_suppress_nodes=(list of load balancer IPs)
```

Forwarding application IP addresses to Oracle Database

The IP address for each application connection seen by CMAN can additionally be forwarded to Oracle Database. This may be required for audit log records or service based ACLs (set through `DBMS_SFW_ACL_ADMIN`).

This feature is independent of the PROXY protocol and is also available when the application directly connects to CMAN without a load balancer. It is supported only for dedicated servers with Oracle Database 19c onwards.

To forward application IP addresses do:

1. **CMAN Configuration**: Add `(ENABLE_IP_FORWARDING = TRUE)` to the parameter section of cman.ora.
2. **Oracle Database Configuration**: Set the `TCP.ALLOWED_PROXIES` parameter in the database `sqlnet.ora` file. This parameter specifies a list of the CMAN instances that can forward client application addresses. A sample entry is:

```
TCP.ALLOWED_PROXIES=(10.1.1.1, cmanhost.example.com)
```

With `cman.ora` and `sqlnet.ora` configured, the forwarded client application IP address can be found using a query like:

```
SELECT SYS_CONTEXT ('USERENV','IP_ADDRESS') FROM DUAL
```

References

- The PROXY Protocol Versions 1 & 2
- Oracle Connection Manager Parameters
- Parameters for sqlnet.ora Files
- DBMS_SFW_ACL_ADMIN package reference