ORACLE

Oracle Database Connection ManagerによるPROXYプロトコルのサポート

Oracle CMANによるPROXYプロトコルのサポートによって
アプリケーションIPアドレスをロードバランサ経由で渡すことで
アクセス制御ルールおよびロギングを有効化

2023年3月3日、バージョン1.1

ORACLE

Oracle CMANでのPROXYプロトコルの使用

本書では、Oracle Connection Manager（Oracle CMAN）がロードバランサのバックエンドとして指定されている場合に、PROXYプロトコルをサポートしてOracle CMANを構成する方法について説明します。

Oracle CMANは、接続リクエストをデータベースまたは他のプロキシ・サーバーへ転送するプロキシ・サーバーです。ロードバランサをOracle CMANとともに使用することにより、統一されたアドレスをクライアント・アプリケーションに公開する一方で、アプリケーション負荷を複数のOracle CMANインスタンス間で分散できます。このモデルを使用すると、ワークロードに基づくOracle CMANインスタンスの水平スケーリングも可能になります。

PROXYプロトコルによって、NATまたはTCPプロキシにおける複数のレイヤー間の接続情報を渡すための便利な方法が提供されます。また、Oracle CMANにクライアント・アプリケーションIPアドレスを渡すこともできるため、アクセス・ルールを強化できます。PROXYプロトコルがない場合、Oracle CMANではロードバランサのIPアドレスのみを使用できます。

PROXYプロトコル・サポートは、Oracle Database 21c以降、非Windowsプラットフォーム上のOracle CMANで使用可能です。PROXYプロトコル・サポートは、Oracle Cloudまたはオンプレミス・デプロイメントで使用できます。PPv1とPPv2の両方がサポートされます。

図1は、ロードバランサの背後にデプロイされ、PROXYプロトコルがポート1で有効化されているOracle CMANを示しています。

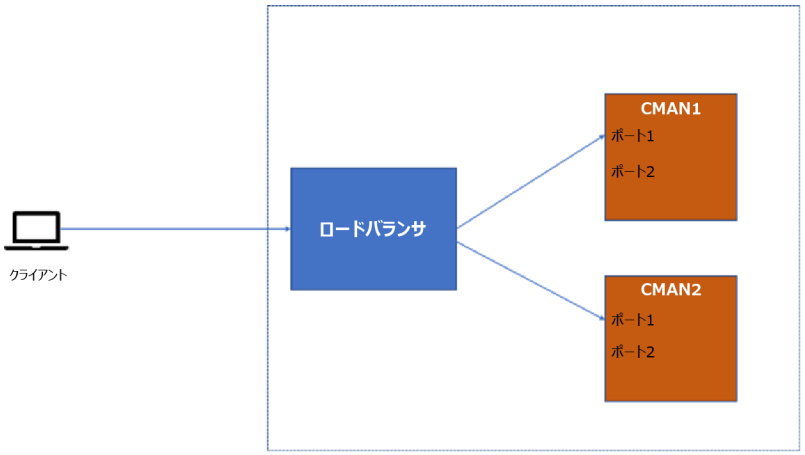

図1.ロードバランサの背後のOracle CMAN。PROXYプロトコルはポート1で有効化。

Oracle CMANでのPROXYプロトコルの有効化

PROXYプロトコルをOracle CMANで有効にするには、PROXYプロトコルを受信するポートのリスニング・アドレスにexpected_proxiesを追加します。expected_proxiesのIPには、ロードバランサがOracle CMANへの接続に使用するすべてのロードバランサのIPアドレスが含まれる必要があります。Oracle CMANはそれらのIPアドレスから発信されるプロキシ・プロトコルのビットを信頼するため、リストがロードバランサのノードのみに限定されるよう留意する必要があります。

Oracle CMANのコントロール操作では、expected_proxiesが指定されなかった別のリスニング・アドレスをcman.oraに追加する必要があります。このアドレスは、expected proxiesを含むアドレスの前に出現する必要があります。

動的な登録を使用する場合は、データベース層のremote_listenerをOracle CMANの非プロキシ・エンドポイントに設定する必要があります。これが必要な理由は、PROXYプロトコルが使用される際に登録がサポートされないためです。

以下は、PROXYプロトコルがポート5435で有効化されているcman.oraの例です。

```
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)
    )

)
```

Oracle CMANのログ・ファイルを検証することで、実際のクライアントIPアドレスが認識されていることを確認できます。以下は、接続でのOracle CMANログのサンプル・エントリです。

```
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
```

ここでは、10.85.86.210が実際のクライアント・アプリケーションIPアドレスです。ポート18025は実際のクライアント・ポートです。PEER_PROXY_IPはロードバランサのIPです。PEER_PROXY_PORTはロードバランサで使用されるポートです。

ロードバランサでのPROXYプロトコルの有効化

HAProxyやNginxなどのロードバランサは、Oracle CMANバックエンドへのPROXYプロトコルの送信を有効化するために固有の構成を必要とします。

F5などの一部のロードバランサでは、すでにクライアントIPアドレスの保持をサポートしています。このような場合、PROXYプロトコルは必要とされないでしょう。

以下に示す構成は、例を示すことのみを目的としています。詳細については、ロードバランサのドキュメントを確認してください。

HAProxy

HAProxyの場合、バックエンドを指定する際に構成にsend-proxyまたはsend-proxy-v2を含める必要があります。たとえば、次のとおりです。

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

NGinx

Nginxの場合、バックエンド・サーバー構成でproxy_passを指定できます。

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

ヘルス・チェックのログ・エントリの停止

一部のロードバランサでは、Oracle CMANへのソケット・レベルの接続を発行してから切断することによって、定期的にヘルス・チェックを実行する場合があります。これによって、Oracle CMANログ・ファイルにエラー・エントリが生成される可能性があります。以下の例のように、cman.oraにパラメータlog_suppress_nodesを設定することによってロギングを無効化できます。

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

Oracle DatabaseへのアプリケーションIPアドレスの転送

Oracle CMANによって認識されるおのおののアプリケーション接続のIPアドレスは、Oracle Databaseに転送することもできます。これは、監査ログ・レコードまたはサービス・ベースのACL（DBMS_SFW_ACL_ADMINによって設定）で必要とされる場合があります。

この機能はPROXYプロトコルから独立しており、ロードバランサなしにアプリケーションが直接Oracle CMANに接続する場合にも利用できます。これは、Oracle Database 19c以降の専用サーバーでのみサポートされます。

アプリケーションIPアドレスを転送するには、以下を実行します。

1. **Oracle CMANの構成**：cman.oraのパラメータ・セクションに(ENABLE_IP_FORWARDING = TRUE)を追加します。
2. **Oracle Databaseの構成**：データベースのsqlnet.oraファイルでTCP.ALLOWED_PROXIESパラメータを設定します。このパラメータは、クライアント・アプリケーション・アドレスを転送できるOracle CMANインスタンスのリストを指定します。以下にエントリのサンプルを示します。

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

cman.oraとsqlnet.oraが構成されると、以下のような問合せを用いて、転送されたクライアント・アプリケーションIPアドレスを参照できます。

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

参考資料

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