【Linux】Dns 動態解析

若想實現同一個 DNS Server 根據不同來源 IP 返回不同的結果，這在 DNS 中稱為**視圖（View）或基於來源的策略解析**，以下是詳細實現方式。

使用 Bind 實現（最佳選擇）

Bind 支持基於來源 IP 的視圖配置，可以為不同來源的請求返回不同的 DNS 記錄。

配置步驟

1. **安裝 Bind** 安裝 Bind DNS Server：

   ```
   sudo apt install bind9
   ```

2. **配置視圖（View）** 編輯 Bind 的主配置文件 `/etc/bind/named.conf`，添加基於來源 IP 的視圖。
   範例配置：

   ```
   acl "internal-network" {
      192.168.1.0/24;
   };

   acl "external-network" {
      any;
   };

   view "internal" {
      match-clients { "internal-network"; };
      zone "example.com" {
         type master;
         file "/etc/bind/db.internal.example.com";
      };
   };

   view "external" {
      match-clients { "external-network"; };
      zone "example.com" {
         type master;
         file "/etc/bind/db.external.example.com";
      };
   };
   ```

3. **創建區域文件** 根據來源 IP 創建不同的區域文件。例如：
   - **內部網絡的區域文件** **`/etc/bind/db.internal.example.com`**：

     ```
     $TTL 604800
     @   IN  SOA example.com. admin.example.com. (
           1   ; Serial
           604800 ; Refresh
           86400 ; Retry
           2419200 ; Expire
           604800 ) ; Negative Cache TTL
     ;
     @   IN  NS  ns.example.com.
     @   IN  A   192.168.1.1
     ```

   - **外部網絡的區域文件** **`/etc/bind/db.external.example.com`**：

     ```
     $TTL 604800
     @   IN  SOA example.com. admin.example.com. (
           1   ; Serial
           604800 ; Refresh
           86400 ; Retry
           2419200 ; Expire
           604800 ) ; Negative Cache TTL
     ;
     @   IN  NS  ns.example.com.
     @   IN  A   203.0.113.1
     ```

4. **重啟 Bind** 重啟 Bind 服務：

```
sudo systemctl restart bind9
```

使用 dnsmasq 實現（輕量級）

配置步驟

1. **安裝 dnsmasq**

```
sudo apt install dnsmasq
```

2. **配置條件解析** 編輯 `/etc/dnsmasq.conf`，添加基於來源 IP 的條件解析規則：

```
# 為內部網絡配置
dhcp-range=set:internal,192.168.1.0,192.168.1.255
address=/example.com/192.168.1.1

# 為外部網絡配置
dhcp-range=set:external,0.0.0.0,255.255.255.255
address=/example.com/203.0.113.1
```

3. **重啟 dnsmasq**

```
sudo systemctl restart dnsmasq
```

使用 PowerDNS（動態解析）

- https://wiki.freedomstu.com/books/%E9%96%8B%E6%BA%90%E8%BB%9F%E9%AB%94%E5%AE%89%E8%A3%9D debian
- https://doc.powerdns.com/authoritative/indexTOC.html
- https://blog.csdn.net/sdhzdtwhm/article/details/135910057
- https://lantian.pub/article/modify-website/powerdns-lua-diy-geodns.lantian/
- https://github.com/PowerDNS/pdns/blob/master/docker-compose.yml

配置 PowerDNS + Lua 脚本

PowerDNS 支持使用 Lua 腳本進行動態解析。

1. **安裝 PowerDNS 和相關組件**

```
sudo apt install pdns-server pdns-backend-sqlite3
```

2. **啟用 Lua 腳本支持** 在 `/etc/powerdns/pdns.conf` 中啟用 Lua Backend：

```
launch=gsqlite3,lua
lua-dns-script=/etc/powerdns/dns.lua
```

3. **編寫 Lua 腳本** 創建 `/etc/powerdns/dns.lua`，根據來源 IP 返回不同的結果：

```
function postresolve(remoteip, domain, qtype)
    if string.match(remoteip, "^192%.168%.1%.") then
        return {{qtype="A", content="192.168.1.1", ttl=60}}
    else
        return {{qtype="A", content="203.0.113.1", ttl=60}}
    end
end
```

4. **重啟 PowerDNS**

```
sudo systemctl restart pdns
```

測試

使用 `dig` 測試

針對不同的來源 IP 測試返回的解析結果。

- 從內部網絡：

  ```
  dig @<DNS_SERVER_IP> example.com
  ```

  返回內部地址（例如 `192.168.1.1`）。
- 從外部網絡：

  ```
  dig @<DNS_SERVER_IP> example.com
  ```

  返回外部地址（例如 `203.0.113.1`）。

注意事項

1. **來源 IP 檢測**：
   - 檢查網絡路由，確保 DNS 伺服器能正確檢測請求的來源 IP。
   - 若有 NAT 設置，需配置正確的來源地址。
2. **DNS 緩存**：
   - 若存在 DNS 緩存伺服器，可能會干擾條件解析結果。
3. **性能**：
   - `Bind` 和 `PowerDNS` 適合高流量環境。
   - `dnsmasq` 適合輕量級應用場景。

這些方案可以靈活地根據來源 IP 實現不同的 DNS 解析結果。

修訂版本 #5
★由 treeman 建立於 22 ﷿Q﷿@﷿﷿ 2024 10:48:37
由 treeman 更新於 6 ﷿Q﷿G﷿﷿ 2024 16:19:40