Cisco Prime Network Registrar を使用した DNS エニーキャスト

エニーキャストは、同じサービスを提供する多くのサーバーに1つのクライアントからパケットを送信できるようにするネットワークとルーティングのメカニズムです。エニーキャストグループ内のすべてのサーバーは同じエニーキャスト IP アドレスを使用して設定されます。パケットはルーティング アルゴリズムに基づいて判断されたベスト パスでクライアントから最も近いサーバーにルーティングされます。エニーキャスト ルーティングで複数のサーバーを1つのサービスとしてグループ化することにより、シームレスな冗長性、ロードバランシング、水平スケーリングといった重要な機能を利用できます。エニーキャスト DNS は DNS サービスのエニーキャストの実装です。エニーキャストは、サービスの可用性を隣接ルータにアドバタイズするために BGP（Border Gateway Protocol）などのルーティングプロトコルと併用されます。これにより、エニーキャスト DNS が有効に機能します。

この章では、エニーキャストを使用して Cisco Prime Network Registrar DNS サービスを設定するための情報とツールについて説明します。

DNS エニーキャストの基本要件

次のリストは、エニーキャスト DNS をサポートするための要件と推奨事項です。

- キャッシング DNS サーバーのエニーキャストアドレスを介して DNS クエリを解決するようにクライアントを設定する必要があります。
- ネームサーバーは、NS と A RR でエニーキャストアドレスをアドバタイズする必要があります。
- ネームサーバーは、エニーキャスト IP アドレスの DNS クエリをリッスンする必要があります。
- ループバック インターフェイスの少なくとも 1 つのエニーキャスト IP アドレスを使用してネームサーバーを設定する必要があります。
- また、管理 IP（物理または追加のループバック インターフェイスのいずれか）を使用してサーバーを設定する必要があります。
- ルーティング情報の交換と、エニーキャスト IP アドレスへのルートが存在しない場合のシステムアクセスとメンテナンスのために、DNS サーバーに少なくとも 1 つの物理 IP を定義する必要があります。
- ゾーン転送、ゾーン更新、または query-source に物理 IP または管理 IP のアドレスを使用し、意図したサーバーに更新が送信されるように、ネームサーバーを設定する必要があります。
- ネームサーバーは、RIP、OSPF、BGP などのルーティング プロトコルを使用して、ルーテッド ネットワークにエニーキャスト IP アドレスを挿入する必要があります。

エニーキャストルーティング

エニーキャストは手動で設定できますが、エニーキャスト宛先アドレスをゲートウェイルータに通知する BGP や OSPF などのルーティングプロトコルを使用して設定することを推奨します。ルーティングプロトコルを使用して DNS サービスの可用性を通知することにより、サービスが停止した場合にルータが DNS クエリをブラックホールに送信しないようにします。Cisco Prime Network Registrar DNS アプリケーションにはルーティング機能がないため、DNS アプリケーションの外部にあるコードを DNS 環境（物理サーバーまたは仮想マシン）に追加する必要があります。主要なオープンソース製品は、RHEL/CentOS 8.x 用の FRRouting（FRR）と RHEL/CentOS 7.x 用の Quagga です。

FRRouting

（注） RHEL/CentOS 8.x では、FRR を使用します。

FRR は、Linux および Unix プラットフォーム用の IP ルーティング プロトコル スイートで、BGP、IS-IS、LDP、OSPF、PIM、および RIP のプロトコルデーモンが含まれています。

FRR は、Linux 用の別のルーティング プロトコル スイートである Quagga から分岐されます。FRR には、Quagga を広く普及させた基本的な機能と、その基盤を大幅に改善した多くの拡張機能が含まれています。

FRR は、Cisco Prime Network Registrar に同梱されていません。FRR の詳細については、FRR のマニュアルを参照してください。

Quagga

（注） RHEL/CentOS 7.x では、Quagga を使用します。

Quaggaはルーティング ソフトウェア スイートであり、Unixプラットフォーム、Linux、Solaris、およびNetBSD用のOSPFv2、OSPFv3、RIP v1およびv2、RIPng、ならびにBGP-4が実装されます。この章では、BGP を使用してこのソリューションを説明します。

Quagga アーキテクチャにはコアデーモンとして zebra が含まれています。zebra は基盤となる Linux カーネルの抽象化レイヤとして機能し、Unix または TCP ストリームを介した Quagga クライアントへの Zserv API を提供します。これらの Zserv クライアントは、通常ではルーティング プロトコルを実装し、zebra デーモンにルーティングの更新を伝達します。

Quagga デーモンは、ネットワークアクセス可能な CLI（**vty** という）を使用して設定できます。CLI は、他のルーティング ソフトウェアと同様のスタイルに従います。Quagga には **vtysh** と呼ばれる別のツールがあります。vtysh はすべてのデーモンに対する単一の統合されたフロントエンドとして機能するため、さまざまな Quagga デーモンのほぼすべての側面を 1 か所で管理できます。

Quagga は、Cisco Prime Network Registrar に同梱されていません。Quagga の詳細については、Quagga のマニュアルを参照してください。

Script

サンプルの Python スクリプトは Cisco Prime Network Registrar のインストールに含まれており、次の場所にあります。

- FRR

  /opt/nwreg2/local/examples/dns/python/dns_anycast_bgp_frr.py

- Quagga

  /opt/nwreg2/local/examples/dns/python/dns_anycast_bgp.py

スクリプトは FRR/Quagga を開始および停止し、DNS クエリを送信して動作を確認します。FRR/Quagga が開始されると、FRR/Quagga デーモンが接続ルータにエニーキャストのアドバタイズメントを送信し、エニーキャストアドレスによる DNS サービスが使用可能になります。DNS サーバーがスクリプトからのクエリに応答しない場合、スクリプトは FRR/Quagga デーモンを停止します。FRR/Quagga の停止によって TCP 接続が切断され、ルータは BGP キープア

ライブメッセージの受信を停止します。その後で、ルータはそのエニーキャストグループからDNSサービスを削除し、次に最も近い、使用可能なDNSサービスへのDNSクエリの送信を開始します。DNS サーバーがスクリプトからのクエリに応答すると、スクリプトはFRR/Quaggaデーモンが実行されているかどうかを確認します。デーモンが実行されていない場合、スクリプトはデーモンを開始します。

サンプルスクリプトを別の場所にコピーし、定期的にスクリプトを実行してDNSサーバーのステータスを確認するようにcronジョブを設定し（推奨は5分間隔）、設定に応じてBGPデーモンを開始または停止することをお勧めします。cronジョブの例は、このソリューションの範囲外です。

ルータ設定

設定はネットワーク要件やアドレス方式のバリエーションによって異なる可能性があります。

BGP を使用したエニーキャスト設定の例

この項では、シスコのルータとFRR/Quaggaホストベースのルーティングソフトウェアで BGPを使用したエニーキャストの基本的なセットアップと設定について説明します。この章の目的は、ルータと BGP の設定について管理者に手順を示すことではなく、Cisco Prime Network Registrarラボで正常にテストされた設定を示すことです。ネットワーク要件は異なる場合がありますので注意してください。

BGP は、インターネットの自律システム（AS）間でルーティング情報と到達可能性情報を交換することを目的として標準化された外部ゲートウェイプロトコルです。この設定は単一のAS を使用します。この方法は、自律システム全体に展開されるソリューションではありません。

次の手順をホスト DNS-1 と DNS-2 で実行する必要があります。

FRR

FRR ルーティングソフトウェアのインストール

Cisco Prime Network Registrarを実行している同じシステムにFRRをインストールします。これにより、次のようなFRRパッケージがインストールされます。

frr-7.0-5.el8.x86_64

Quagga

Quagga ルーティング ソフトウェアのインストール

Cisco Prime Network Registrar を実行している同じシステムに Quagga をインストールします。これにより、次のような Quagga パッケージがインストールされます。

quagga-0.99.15-7.el6_3.2.x86_64

ループバック インターフェイスの作成

システムでループバック インターフェイスのエイリアスを作成します。このループバック インターフェイスのエニーキャスト IP アドレスを設定します。

RHEL の場合、インターフェイス コンフィギュレーション ファイルは、**/etc/sysconfig/network-scripts** にあります。**ifcfg-lo:0** という名前のディレクトリに次の内容のファイルを作成します。

```
DEVICE=lo:0
IPADDR=10.10.10.1
NETMASK=255.255.255.255
BOOTPROTO=none
ONBOOT=yes
```

Ifup lo: 0コマンドを使用して、新しいループバックインターフェイスを起動します。

ネットワーク ルータ設定

このルータ設定は、このDNSエニーキャストソリューションの検証で使用されます。これは、DNS エニーキャスト ソリューションの開発を補助するための参考資料として提供されています。この特定のソリューションの完全な設定ですが、ソリューション開発のための参考用でしかありません。

```
csr1000v# sh run
Building configuration...
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet1
 ip address 10.78.29.77 255.255.255.0 (Router)
 negotiation auto
!
interface GigabitEthernet2
 ip address 10.0.2.1 255.255.255.0 (Client)
 negotiation auto
!
interface GigabitEthernet4 (DNS-2)
 platform ring rx 256
 ip address 10.0.3.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet5 (DNS-3)
 platform ring rx 256
 ip address 10.0.5.1 255.255.255.0
 negotiation auto
!
router ospf 1
 router-id 2.2.2.2(is the loopback IP address)
 redistribute bgp 65500 subnets
 network 2.2.2.2 0.0.0.0 area 1
 network 10.0.6.0 0.0.0.255 area 1
 network 10.0.0.0 0.0.255.255 area 1
!
router bgp 65500
 bgp log-neighbor-changes
 neighbor IBGP peer-group
 neighbor IBGP update-source Loopback0
 neighbor ANY peer-group
 neighbor 1.1.1.1 remote-as 65500
```

```
 neighbor 1.1.1.1 peer-group IBGP
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 10.0.3.2 remote-as65500
!(This should be the bgp AS in Quagga for DNS-2)
 neighbor 10.0.3.2 peer-group ANY
 neighbor 10.0.5.2 remote-as 65500
!(This should be the bgp AS in Quagga for DNS-3)
 neighbor 10.0.5.2 peer-group ANY
 !
 address-family ipv4
 redistribute ospf 1
 neighbor IBGP next-hop-self
 neighbor ANY next-hop-self
 neighbor 1.1.1.1 activate
 neighbor 10.0.3.2 activate
 neighbor 10.0.5.2 activate
 exit-address-family
!
virtual-service csr_mgmt
 ip shared host-interface GigabitEthernet1
 activate
!
ip default-gateway 10.78.28.1
ip forward-protocol nd
!
no ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.78.28.1
ip route 10.78.28.0 255.255.254.0 GigabitEthernet1 10.78.28.1
!
ip prefix-list anycast-ip seq 5 permit 10.10.10.1/32
!
control-plane
!
line con 0
 stopbits 1
line vty 0 4
 login local
!
!
end
```

DNS サーバーでの FRRouting の設定

両方のサーバーで FRR 構成ファイルを設定します。次は DNS-1 の例です。DNS-2 も同様に設定する必要があります。構成ファイルは **/etc/frr** にあります。

/etc/frr には構成ファイルの例が複数あります。（FRR がサポートする各ルーティングプロトコル用と、メインプロセスである zebra 用）。BGP を使用してエニーキャストを有効にするには、**zebra.conf**、**bgpd.conf**、**daemons** ファイルを設定する必要があります。

デーモンファイルで zebra と bgpd を有効にする

```
# cat /etc/frr/daemons
# This file tells the frr package which daemons to start.
watchfrr_enable=yes
watchfrr_options="-r '/usr/lib/frr/frr restart %s' -s '/usr/lib/frr/frr start %s' -k
'/usr/lib/frr/frr stop %s'"
```

```
#
zebra=yes
bgpd=yes
ospfd=no
```

FRR Zebra 設定

```
# cat /etc/frr/zebra.conf
hostname DNS-1
!
password zebra
enable password zebra
!
interface eth0
 ip address 10.0.3.2/24
!
interface lo
 ip address 10.10.10.1/32
!
line vty
!
```

（注） このグループに属する他のエニーキャスト サーバーに対して、この手順を繰り返します。

FRR BGP 設定

```
# cat /etc/frr/bgpd.conf
! -*- bgp -*-
!
! BGPd sample configuration file
!
!
hostname DNS-1
password zebra
log stdout
!
router bgp 65500
bgp router-id 10.78.29.79
bgp log-neighbor-changes
network 10.10.10.1/32
timers bgp 4 16
neighbor 10.0.3.1 remote-as 65500
neighbor 10.0.3.1 next-hop-self
neighbor 10.0.3.1 prefix-list DEFAULT in
neighbor 10.0.3.1 prefix-list ANYCAST out
!
address-family ipv4
network 10.0.3.1/24
neighbor 10.0.3.1 activate
exit-address-family
!
ip prefix-list ANYCAST seq 5 permit 10.10.10.1/32
ip prefix-list DEFAULT seq 5 permit 0.0.0.0/0
line vty
!
```

FRR サービスの開始

次のコマンドを使用して、FRR サービスを開始します。

```
systemctl start frr.service
```

ループバックインターフェイスで追加の IPアドレス を作成する

FRR を使用してエニーキャスト用のループバック インターフェイスに追加の IP アドレスを作成するには、Red Hat のマニュアルを参照してください。

FRR サービスの再起動

次のコマンドを使用して、FRR サービスを再起動します。

```
systemctl restart frr.service
```

DNS サーバーでの Quagga の設定

両方のサーバーで Quagga コンフィギュレーション ファイルを設定します。次は DNS-1 の例です。DNS-2 も同様に設定する必要があります。コンフィギュレーション ファイルは**/etc/Quagga** にあります。

/etc/Quagga にはコンフィギュレーション ファイルの例が複数あります（Quagga がサポートする各ルーティングプロトコル用と、メインプロセスである zebra 用）。BGP を使用してエニーキャストを有効にするには、**zebra.conf** と **bgpd.conf** を設定する必要があります。

Quagga Zebra の設定

```
# cat /etc/quagga/zebra.conf
hostname DNS-1
!
password zebra
enable password zebra
!
interface eth0
 ip address 10.0.3.2/24
!
interface lo
!
line vty
!
```

（注） このグループに属する他のエニーキャスト サーバーに対して、この手順を繰り返します。

Quagga BGP の設定

```
# cat /etc/quagga/bgpd.conf
! -*- bgp -*-
!
! BGPd sample configuration file
!
!
hostname DNS-1
password zebra
log stdout
!
router bgp 65500
bgp router-id 10.78.29.79
bgp log-neighbor-changes
network 10.10.10.1/32
timers bgp 4 16
neighbor 10.0.3.1 remote-as 65500
neighbor 10.0.3.1 next-hop-self
neighbor 10.0.3.1 prefix-list DEFAULT in
neighbor 10.0.3.1 prefix-list ANYCAST out
!
address-family ipv4
network 10.0.3.1/24
neighbor 10.0.3.1 activate
exit-address-family
!
ip prefix-list ANYCAST seq 5 permit 10.10.10.1/32
ip prefix-list DEFAULT seq 5 permit 0.0.0.0/0
line vty
!
```

BGP デーモンの開始

次のコマンドを使用して、BGP デーモンを開始します。

```
systemctl start bgpd
```

ルータでの診断の実行

ルータで診断を実行して、エニーキャストが正しく設定されていることを確認します。

sh ip bgp summary コマンドの出力は、router-1 が 2 つのネイバーとの BGP セッションを開始したことを示します。**State/PfxRcd** の値は、TCP セッションがアップしており、ルータとホストがルートを交換していることを示します。このフィールドは、リモート ネイバーから受信したルート プレフィックスの数を示す数値である必要があります。値の例は 1 です。この時点で、DNS サーバーとの BGP 接続が確立された状態になります。

sh ip bgp summary の概要：

```
BGP router identifier 2.2.2.2, local AS number 65500
BGP table version is 86, main routing table version 86
1 network entries using 248 bytes of memory
2 path entries using 240 bytes of memory
1/1 BGP path/bestpath attribute entries using 248 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
```

```
BGP using 736 total bytes of memory
BGP activity 16/15 prefixes, 61/59 paths, scan interval 60 secs
```

ネイバー	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
1.1.1.1	4	65500	0	0	1	0	0	4w0d	Idle
10.0.3.2	4	65500	137919	129519	86	0	0	1w0d	1
10.0.5.2	4	65500	137923	129519	86	0	0	1w0d	1

show ip bgp neighbors コマンドは、ネイバーに関する情報を詳細に示します。

show ip route コマンドには、エニーキャストアドレスと現在ルーティングされているホストのエントリが含まれている必要があります。

```
#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 a - application route
 + - replicated route, % - next hop override, p - overrides from PfR
B 10.10.10.1/32 [200/0] via 10.0.3.2, 00:00:10
```

BGP トラフィック ログのモニター

ホスト DNS-1 と DNS-2 の BGP トラフィックログをモニターするには、 **telnet localhost bgpd** コマンドを使用します。

FRR

```
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Hello, this is FRRouting (version 7.0).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


User Access Verification

Password:
dns-anycast-1> enable
dns-anycast-1# terminal monitor
dns-anycast-1# conf t
dns-anycast-1(config)# debug bgp keepalives
dns-anycast-1(config)# 2020/10/27 02:56:22 BGP: : 10.0.3.1 KEEPALIVE rcvd

dns-anycast-1(config)# 2020/10/27 02:56:23 BGP: : 10.0.3.1 sending KEEPALIVE
2020/10/27 02:56:27 BGP: : 10.0.3.1 KEEPALIVE rcvd
2020/10/27 02:56:28 BGP: : 10.0.3.1 sending KEEPALIVE
2020/10/27 02:56:32 BGP: : 10.0.3.1 KEEPALIVE rcvd
2020/10/27 02:56:33 BGP: : 10.0.3.1 sending KEEPALIVE
```

```
2020/10/27 02:56:37 BGP: : 10.0.3.1 KEEPALIVE rcvd
2020/10/27 02:56:38 BGP: : 10.0.3.1 sending KEEPALIVE
2020/10/27 02:56:42 BGP: : 10.0.3.1 KEEPALIVE rcvd
2020/10/27 02:56:43 BGP: : 10.0.3.1 sending KEEPALIVE
2020/10/27 02:56:47 BGP: : 10.0.3.1 KEEPALIVE rcvd
2020/10/27 02:56:48 BGP: : 10.0.3.1 sending KEEPALIVE
```

Quagga

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Hello, this is Quagga (version 0.99.15).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
User Access Verification
Password:
DNS-1> enable
DNS-1# terminal monitor
DNS-1# 2016/07/13 15:49:20 BGP: 10.0.5.1 send message type 4, length (incl. header) 19
2016/07/13 15:49:21 BGP: 10.0.5.1 rcv message type 4, length (excl. header) 0
2016/07/13 15:49:25 BGP: 10.0.5.1 send message type 4, length (incl. header) 19
2016/07/13 15:49:27 BGP: 10.0.5.1 rcv message type 4, length (excl. header) 0
```

DNS ゾーンの設定

これでエニーキャスト機能の設定は終わりますが、管理者は DNS サーバーの設定を完了する必要があります。ゾーンの管理を参照してください。

詳細については、次のリンクを参照してください。

- http://www.pacnog.org/pacnog6/IXP/Anycast-v10.pdf
- http://www.nongnu.org/Quagga
- https://frrouting.org/
- https://cumulusnetworks.com/learn/frrouting/
- https://bgpgeek.com/installing-frr/
- https://access.redhat.com/solutions/4967711
- https://access.redhat.com/solutions/4538371
- http://www.linuxjournal.com/magazine/ipv4-anycast-linux-and-Quagga
- http://ddiguru.com/blog/125-anycast-dns-part-5-using-bgp

（注） 上記のリンクは外部 Web サイトを参照しており、シスコはそれらを最新の状態に保つ責任を負いません。これらは参照のためだけに提供されています。コンテンツが古い場合やリンクにアクセスできない場合は、Web サイトの所有者に連絡して最新情報を入手してください。