テクニカル レポート

ONTAPでのDNSロードバランシング

構成とベストプラクティス

NetApp
Justin Parisi
2021年2月| TR-4523

概要

本ドキュメントでは、DNSロードバランシング方式で使用するNetApp ONTAP®管理ソフトウェアを搭載したNetApp®ストレージシステムの設定方法について説明します。このドキュメントでは、ONTAPで使用できる内蔵DNS機能、さまざまな設定方法、およびベストプラクティスについて説明します。

目次

表一覧

図一覧

ベストプラクティス一覧

ONTAPノドメインネームシステム

ONTAPを使用すると、ストレージ管理者は、NASアクセス用に、複数のノードにまたがるStorage Virtual Machine（SVM）ごとに複数の論理インターフェイス（データLIF）をクライアントに提供できます。NAS環境では、クラスタに最大24ノードを含めることができるため、1つのクラスタには大量のデータLIFが存在する可能性があります。このような規模になると、クライアントがIPアドレスを介したマウントに依存している場合、クライアントのアクセスが混乱する可能性があります。これは、ストレージシステム内のIPアドレスがどこにあるかをエンドユーザが理解する必要がないためです。クライアントが同じデータLIFを継続的にマウントし、特定のIPアドレスを覚えようとすると、ノードに要求が大量に発生する可能性があります。

これらのIPアドレスの管理も困難な場合があります。クライアントが既知のIPアドレスによってアクセスしている場合、管理者はクライアントがデータLIFを追加または削除したときに変更を明示的に認識できるようにする必要があります。

これらのデータLIFへのクライアントアクセスを簡易化し、NASネットワークコンポーネントをストレージ側から管理するために、多くの場合、Domain Name System（DNS；ドメインネームシステム）が実装され、1つのホスト名で複数のデータLIFを保護します。

ONTAPでのネームサービスの一般的なベストプラクティスについては、TR-4668：『ネームサービスベストプラクティスガイド』を参照してください。

次のRequest for Comments（RFC）は、DNS標準をカバーし、DNSに関する一般的な情報を提供します。

- RFC 1035-ドメイン名
- RFC 1123-インターネットホストの要件
- RFC 2181-DNS仕様の説明

DNSとは

DNSは、ネットワーク上のデバイスの階層的な命名システムであり、IPアドレスやサービスレコードなど、記憶が容易ではない項目に、判読可能な名前を関連付ける方法を提供します。DNSは、これらのレコードの発行を、ネットワーク上の信頼できるソースとして機能する1つ以上のサーバに解放します。

DNSの用語

次のセクションでは、内蔵DNSで使用されるさまざまな種類のDNS用語について説明します。

A/AAAAレコード

A/AAAAレコード（RFC-1101）は、ホスト名をIPアドレスにマッピングします。Aレコードは、ホスト名をIPv4アドレスにマッピングします。AAAAレコードは、ホスト名をIPv6アドレスにマッピングします。これらのマップは、フォワードDNSルックアップに使用されます。

正規名

正規名（CNAME）は、ホスト名のエイリアスです。

サービスレコード

サービス（SRV）レコード（RFC-2782）は、特定のドメインサービス（LDAP、CIFS、NFS、Exchangeなど）のDNSレコードを定義します。 など。これらのレコードは、複数のA/AAAAレコードをポイントして、ラウンドロビンによるロードバランシングとハイアベイラビリティを提供できます。

ポインタレコード

ポインタ(PTR)レコードは、IPアドレスを正規名にマップします。このマッピングは、DNSリバースルックアップに使用されます。

ネームサーバレコード

ネームサーバ（NS）NSレコードは、サブドメインをネームサーバのセットに委任するために使用されます。これらのレコードは、権限のあるレコードでも、権限のないレコードでもかまいません。

権限レコードの開始

このタイプのレコードは、どのネームサーバがDNS要求の信頼できる回答であるかを定義します。State of Authority（SOA；権限状態）レコードがないネームサーバがDNS要求に対する応答を発行した場合、その応答は「権限のない」応答としてクライアントに返されます。

SOAレコードには、次の情報が含まれています。

- DNSドメインからのプライマリネームサーバDNSドメインカラノプライマリネームサーバ
- 更新のタイムスタンプ
- ゾーンの更新時間
- 失敗した更新の再試行回数
- SOAレコードタイムアウト
- 負の存続可能時間（TTL）（障害が発生したリゾルバが障害キャッシュに存在する期間）

DNSフォワーダ

DNSフォワーダは、外部DNS名のDNSクエリをそのネットワーク外のDNSサーバに転送するネットワーク上のDNSサーバです。また、条件付きフォワーダを使用して、特定のドメイン名に従ってクエリを転送することもできます。このフォワーダは、通常のDNSフォワーダよりも優先されます。

条件付きフォワーダ

条件付きフォワーダは、クエリー内のDNSドメイン名に従ってDNSクエリーを転送するネットワーク上のDNSサーバです。たとえば、で終わる名前のすべてのクエリーを `example.newname.com` 特定のDNSサーバのIPアドレスまたは複数のDNSサーバのIPアドレスに転送するようにDNSサーバを設定できます。条件付きフォワーダは、DNSサーバのドメインが目的のDNSドメイン名と異なる場合に使用されます。

例：

```
example.newname.com → netapp.com
```

条件付きフォワーダでは、データLIFをネームサーバとしてDNSに追加し、SOAレコードを格納する必要があります。さらに、前方参照ゾーンと後方参照エントリを作成する必要があります。Windows 2008以降では、SOAレコードが必要になる場合があります。Windows 2003 DNSにはSOAレコードは必要ありません。

スタブゾーン

スタブゾーンに関するMicrosoftの記事から、次の手順を実行します。

スタブゾーンは、そのゾーンの権限のあるDomain Name System（DNS;ドメインネームシステム）サーバを識別するために必要なリソースレコードだけを含むゾーンのコピーです。スタブゾーンは、個別のDNSネームスペース間で名前を解決するために使用されます。このタイプの解決は、企業の合併で、2つの別々のDNS名前空間のDNSサーバーが両方の名前空間のクライアントの名前を解決する必要がある場合に必要になることがあります。

スタブゾーンは次の要素で構成されます。

- SOAリソースレコード、ネームサーバ（NS）リソースレコード、および委任されたゾーンのリソースレコードを接着します。
- スタブゾーンの更新に使用できる1つ以上のマスターサーバのIPアドレス。

スタブゾーンのマスターサーバは、子ゾーンの権限を持つ1つ以上のDNSサーバです。通常は、委任されたドメイン名のプライマリゾーンをホストするDNSサーバです。

ネームサーバがSOAサーバではなく、作成されたDNSゾーンがスタブゾーンではないため、条件付き転送が機能しない場合は、スタブゾーンが必要です。

スタブゾーンと条件付きフォワーダの比較については、Microsoftの記事「スタブゾーンと条件付きフォワーダの対照」を参照してください。

プライマリゾーン

プライマリゾーンは、ゾーンの情報のプライマリソースであり、ゾーンデータのマスターコピーをローカルファイルまたはデータベースに格納するDNSゾーンです。スタブゾーンとは異なり、プライマリゾーンではレコード（A、AAAA、SRVなど）を作成できます。

DNSイジョウ

DNS委任は、同じドメイン内の要求を委任ゾーンで指定されたDNSサーバーに委任します。たとえば `cdot.netapp.com`、のDNSドメインでの委任を使用します `netapp.com`。

ゾーンの委任の詳細については、Microsoftの「ゾーンの委任とゾーンの委任について」を参照してください。

サブドメイン

サブドメインは、プライマリDNSドメインの一部であるDNSドメインです。たとえば、`dns.domain.com` はのサブドメイン `domain.com`です。

ONTAPのDNSオプション

NetApp ONTAPには、次のようなDNS設定を制御するためのさまざまなオプションが用意されています。

- 動的DNS（IPv4およびIPv6）
- 組み込みのDNSロードバランシング
- データLIFをネームサーバやネームレコードとして使用する機能

ONTAP 9.7以降のadvanced権限で使用できるDNS設定オプションは次のとおりです。

```
cluster::*> dns ?
  check                       Display validation status of a DNS configuration
  create                      Create a new DNS table entry
  delete                      Remove a DNS table entry
  dynamic-update>             Manage Dynamic DNS Updates
  hosts>                      Manage local mapping for host names
  modify                      Change a DNS table entry
  show                        Display DNS configuration
```

ONTAPでのDNSルックアップのテスト

ONTAPには、DNSサーバに対して転送およびSRVレコード検索を実行するためのadvanced権限がコマンドに含まれています。これにより、ストレージ管理者はDNSが正常に機能しているかどうかを確認できます。

前方検索をテストするには、次のコマンドを実行します。

```
cluster::*> access-check dns forward-lookup -vserver SVM -hostname {hostname|fqdn}
```

SRV検索をテストするには、次のコマンドを実行します。

```
cluster::*> access-check dns srv-lookup -vserver SVM -lookup-string {_ldap._tcp.ntap.local}
```

ネットグループを使用している場合は `getXXbyYY netgrpcheck` 、advanced権限でコマンドを実行してDNSを確認することもできます。

```
cluster::*> getxxbyyy netgrpcheck -node node1 -vserver DEMO -netgroup netgroup1 -clientIP
10.193.67.225

Client 10.193.67.225 is not a member of netgroup netgroup1
Searched using NETGROUP_BYHOST
```

ONTAPでのDNSキャッシュ

ONTAPは、DNSホスト名とIPアドレスのキャッシュを提供します。これにより、DNSサーバへの負荷を軽減し、名前解決要求を高速化できます。これらのキャッシュは、`name-service cache hosts` advanced権限でコマンドを使用して管理します。

次の表に、キャッシュ設定のデフォルト値を示します。

表1）ONTAPのDNSキャッシュ設定

設定	Value
DNSキャッシュが有効	True
ネガティブキャッシュ有効	True
Time-To-Live（TTL）	24時間
負の存続可能時間（TTL）	1 分
DNSから取得されたTime-To-Live（TTL）	True

注: ネガティブキャッシュエントリは、失敗したDNS試行の長期的なキャッシュを防ぐために、より早く期限切れになります。

DNSホストキャッシュの表示と管理

`name-service cache hosts` advanced権限を持つコマンドセットと同じコマンドセットを使用すると、ホストエントリのキャッシュを表示して手動でクリアできます。キャッシュには、エクスポートアクセス、ネットグループチェック、および `access-check dns` コマンドからデータが格納されます。

DNSキャッシュエントリを表示するには、次のコマンドを実行します。

```
cluster::*> name-service cache hosts forward-lookup show -vserver DEMO -host centos7 -instance

                    IP       Address IP                    Create
Vserver   Host      Protocol Family Address          Source Time         TTL(sec)
----------- ----------- ---------- --------- ------------------- ---------- ------------- -----------
DEMO      centos7 Any       Any     10.193.67.225 dns       4/29/2020 3600
                                                              11:15:49

cluster::*> name-service cache hosts reverse-lookup show -vserver DEMO -ip 10.193.67.225
------------- -------------------- -------------------------- -------- -------------------- -----------
Vserver    IP Address      Host                  Source Create Time     TTL(sec)

DEMO       10.193.67.225   centos7.ntap.local    dns    4/29/2020 11:25:58 3600
```

DNSキャッシュエントリをクリアするには、次のコマンドを実行します。

```
cluster::*> name-service cache hosts forward-lookup

  delete                      *Delete an entry
  delete-all                  *Delete all the entries for the vserver
```

DNSロード バランシング

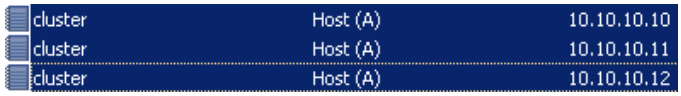
DNSホスト名を使用して複数のIPアドレスを参照するもう1つの利点は、DNSサーバでさまざまなロードバランシングメカニズムを利用できることです。DNSロードバランシングは、クライアントの操作を必要とせずに、ホスト名に対するクライアント要求を複数のIPアドレスに分散する方法です。一般に、DNSロードバランシングはラウンドロビンによって実行されます。ロードバランシングは、サードパーティのロードバランサや、内蔵DNSロードバランシングと呼ばれるONTAP機能を使用して実行することもできます。

オフボックスラウンドロビンDNS

ラウンドロビンDNSは、DNSロードバランシングの最も一般的な形式です。これは、DNSサーバでデフォルトで提供され、要求しているクライアントにIPアドレスを提供する簡単な方法です。

ラウンドロビンA/AAAAレコードを作成するには、元のレコードと同じ名前で別のA/AAAAレコードを作成します。

図1）レコードを使用したオフボックスDNSラウンドロビン方式の例



- Windowsでのラウンドロビン DNSの詳細については、「Windowsでのラウンドロビン DNSの設定」を参照してください。
- BINDのラウンドロビンDNSの詳細については、「ラウンドロビン負荷分散」を参照してください。

ラウンドロビンDNSの制限事項

ラウンドロビンバランシングでは、サーバの負荷やネットワーク接続などは考慮されません。要求を受信した順にIPアドレスを提供するだけです。サーバーまたはクライアントのIPアドレスにラウンドロビン構成で問題が発生した場合でも、DNSサーバーは問題のあるサーバーのIPアドレスを問題する可能性があり、クライアントに問題が発生する可能性があります。このような可能性があるため、ラウンドロビンDNSはエンタープライズNAS環境には理想的な方法ではない可能性があります。これらの環境では、より明確なロードバランシング方式が必要になる場合があります。幸いなことに、ONTAPは、DNS用の統合されたシンプルでインテリジェントなロードバランシング解決策を無料で提供しています。ライセンスは必要ありません。

組み込みのDNSロードバランシング

ONTAPを使用すると、各ノードでDNSサービスを使用して、クライアントからのDNS要求を処理できます。ONTAPでは、ノードのCPU負荷とポートスループットを評価するアルゴリズムに基づいてデータLIFのIPアドレスを問題することもできます。このプロセスでは、マウント要求に対してクラスタ全体で適切な負荷分散が行われるように、使用率が最も低いデータLIFが提供されます。マウントまたはマップが成功すると、クライアントは再マウントするまでその接続を使用し続けます。

このアプローチはラウンドロビンDNSとは異なり、外部DNSサーバがすべての要求を処理し、クラスタ内のノードのビジー率を把握できないためです。

内蔵DNSに関する考慮事項

NFSv4.xリファーラルまたはSMB自動配置を使用する場合は、DNSロードバランシングを使用する必要はありません。最初に接続が確立されるのは、DNSから返されたIPアドレスに関係なく、アクセス対象のボリュームに対してローカルなノードです。

FlexGroupで組み込みのDNSを使用すると、ボリュームがクラスタ内の複数のノードにまたがる場合でも、確立されるTCP接続が複数のノードに分散されるため、いくつかの利点があります。

また、ラウンドロビンDNSは、Time-To-Live（TTL）値が設定されたIPアドレスを発行します。デフォルトでは、TTLはWindowsでDNS要求を24時間キャッシュします。内蔵DNSはTTL値を0で発行します。つまり、DNSがクライアントにキャッシュされることはなく、新しいIPは常に負荷に基づいて発行されます。クライアントはTTLを設定せず、DNSサーバがTTLを定義します。この場合、ONTAPはDNSサーバとして機能します。

Windows DNSキャッシュの内容を確認するには、ipconfig /displaydnsを使用します。

オンボックスDNSとpNFSの連携

内蔵DNSはpNFSデータトラフィックには適用されません。pNFSデータトラフィックでは、マウント時にI/Oのトラフィックが一貫してリダイレクトされます。ただし、組み込みのDNSは、クラスタ内のメタデータサーバ（MDS）へのロードバランシング接続に役立ちます。pNFSの詳細については、TR-4067：『NFS Best Practices and Implementation Guide』およびTR-4063：『Parallel Network File System Configuration and Best Practices for Clustered Data ONTAP』を参照してください。

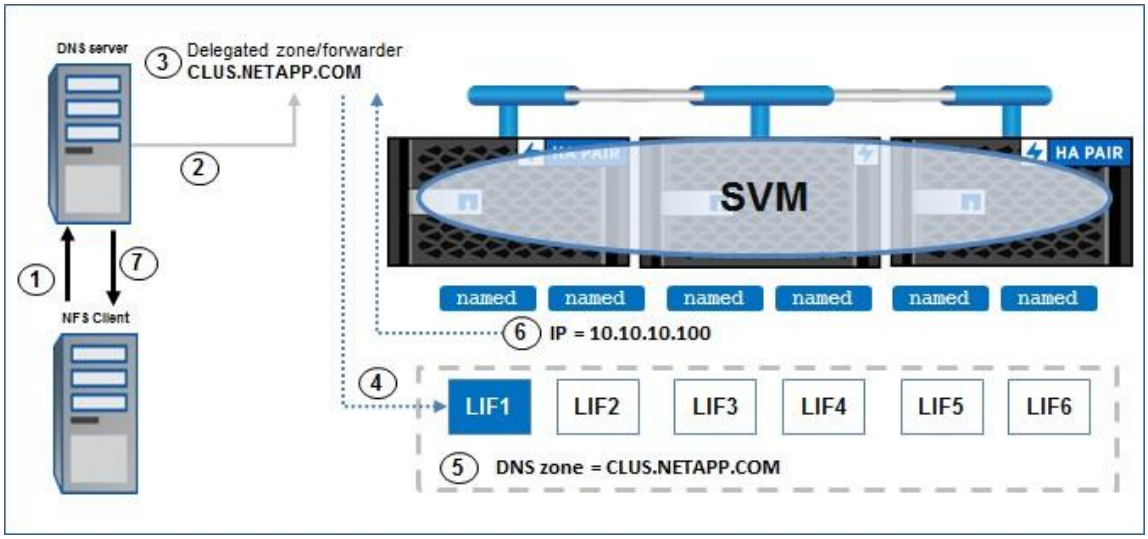
ベストプラクティス1：推奨されるONTAPバージョン：内蔵DNS

内蔵DNSを使用する場合は、最新のパッチが適用されたONTAPリリースを使用して最適な結果を得てください。

オンボックスDNSロードバランシングの仕組み

クラスタ内の各ノードには、クライアントからの受信DNS要求を処理するサービス（named）があります。また、CPU利用率とノードスループットに基づくアルゴリズムで決定された重みの計算に基づいてIPアドレスが発行されます。

図2）内蔵DNSロードバランシングの例



クライアントがDNSホスト名を使用してクラスタにアクセスしようとすると、次のプロセスが実行されます。

1. クライアントはDNS要求を発行し、その構成で指定されたDNSサーバを使用します。
2. DNSサーバは要求でホスト名を検索します。
3. 内蔵DNSを使用する場合、ホスト名はDNS委任または条件付きフォワーダです。このレコードには、DNS要求に使用するデータLIFのIPアドレス（NSレコードとして提供）のリストが含まれます。
4. 要求は、ラウンドロビンベースでいずれかのデータLIF IPアドレスに転送または委譲されます。
5. LIFにDNSゾーンが設定されていて、DNSクエリをリスンするように設定されている（LIFのポート53が開く）場合、データLIFは要求を受信します。
6. 要求を受信したノードは、各ノードのDNS重みを確認し、計算された負荷に基づいてIPアドレスを発行します。

7. IPアドレスがDNSサーバに返され、DNSサーバはそのIPアドレスをクライアントに返します。

注： ONTAP 8.2より前のバージョンでは、組み込みのDNSロードバランシングはifgrpまたはVLANでは機能しません。これらの設定がある実装では、外部ラウンドロビンDNSを使用します。ONTAPバージョン8.2以降では、ifgrpおよびVLANでDNSロードバランシングが搭載されています。

内蔵DNSアルゴリズム

ONTAP内蔵DNSアルゴリズムは特許番号US8271652でカバーされている。詳細については、特許リンクをご覧ください。その特許から以下の要約を参照してください。

「DNSの名前解決は、ネットワークストレージクラスタ内の各ノードに統合されており、重み付きランダム分散を使用してDNS要求を解決し、ネットワークアドレスのロードバランシングを可能にします。クラスタ内のノードは、クラスタ内のノード上のリソース利用率（CPU利用率やスループットなど）に関する統計を収集し、それらの統計を他のすべてのノードに分散します。各ノードでは、同じアルゴリズムを使用して、クラスタに分散された統計に基づいてクラスタのさまざまなIPアドレスの重みが生成されます。重みは、使用可能なネットワークアドレスの重み付きリストを生成するために使用されます。DNS要求に応答して、特定のノード内のDNSが重み付きアドレスリストにランダムにインデックスを作成し、ネットワークアドレスへの要求を解決します。重みは、DNSが負荷の低いIPアドレスを選択する可能性が高いため、時間の経過とともにポートとノードの使用量が分散されるように選択されます。」

このアルゴリズムには、DNSロードバランシンググループに含まれるデータLIFに割り当てられた一連の重みが組み込まれています。これらの重みは毎分更新され、CPUの重みとスループットの重みを使用して最終的な重みが計算されます。内蔵DNSアルゴリズムの計算は次のとおりです。

- **CPUノオモミ**

  cpu_weight = 100.0 -（CPU使用率）/ IPアドレスが存在するノードのIPアドレスの数）
- **スループットの重み**

  thpt_weight = 100.0−（使用されているポートスループットの割合）/ IPアドレスが存在するポート上のIPアドレスの数
- **最終重量**

  final_weight =（thpt_weight + cpu_weight）/ 2

幾何平均と算術平均

バグ619247の修正前のONTAPバージョンでは、DNSロードバランスアルゴリズムが幾何平均ではなく算術平均を使用していました。スループットが低くCPU利用率が100%のノードのIPアドレスを返すことがわかっていたため、この値が変更されました。現在のバージョンのONTAPでは、デフォルトで形状平均が使用されます。NetAppでは、このオプションを変更することを推奨していません。

ベストプラクティス2：幾何平均構成

NetAppテクニカルサポートから指示がないかぎり、ロードバランシングの幾何平均を変更しないでください。

この動作は、advanced権限モードのCLIオプションを使用して制御します。

```
cluster::*> network options load-balancing show
Geometric Mean Algorithm for load balancing: true
```

DNSでテスト済みの制限事項を搭載

搭載DNSの最近の負荷テストでは、ONTAPで処理できるノードあたりの同時DNS要求数を確認するために、搭載DNSの最近の負荷テストが実行されました。

表2）ノードあたりの1秒あたりの最大DNS要求数-ONTAP 9.7

TCP経由のDNS	UDP経由のDNS
4、000~5、000	1、000~1、500

注： テストの詳細については、内部バグ1285445を参照してください。

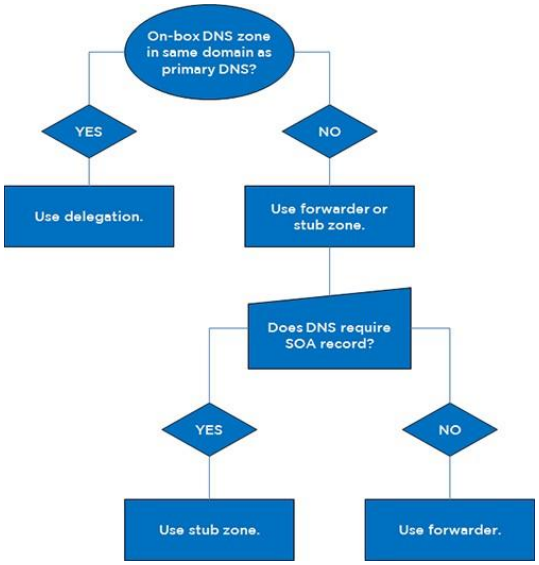
オンボックスDNSゾーンの設定方法の決定

このセクションでは、オンボックスDNSロードバランシングの設定に使用するDNSゾーン方式を決定する方法について説明します。

注: Windows以外のDNSサーバー(BINDなど)にも同じ概念が適用されます。DNSは、RFC 1035で規定されているインターネット標準です。

Windows DNSで使用する設定の決定

図3）On-BOの設定で考慮すべき要素Windows DNSサーバ上のX DNSロードバランシング。



内蔵DNSロードバランシングを設定する場合は、条件付き転送、スタブゾーン、DNSゾーン委任のいずれを使用するかを設計上決定する必要があります。このブログでは、どのタイプの転送ゾーンを使用するかのユースケースシナリオについて説明します。

左側の図に示すように、設計の決定はさまざまな要因に基づいています。

場合によっては、DNSリスナーとして機能するデータLIFをネームサーバとして直接参照するようにクライアントを設定した方が理にかなっていることがあります。その方法については、「ONTAPデータLIFをDNSとして使用するクライアントの設定」を参照してください 。

ベストプラクティス3：Windows DNS構成に関する推奨事項

次のガイダンスに従って、Windows DNSサーバで使用するDNSゾーンのタイプを決定します。

- プライマリDNSサーバと同じドメイン内にあるDNSゾーンを含む名前のデータLIFには、DNS委譲を使用します。
- プライマリDNSサーバとは別のDNSドメインにあるDNSゾーンで名前を付けたデータLIFには、SOAレコードが不要な場合を除き、スタブゾーンを使用します。そのような場合は、フォワーダを使用してください。

BIND DNSで使用する設定の決定

内蔵DNSロードバランシングを設定する場合は、転送、サブドメインゾーン、またはDNSゾーン委任のいずれを使用するかについて、設計上の決定を行う必要があります。

ベストプラクティス4：バインドDNSの設定に関する推奨事項

BINDで使用するDNSゾーンのタイプを決定するには、次のガイダンスを使用します。

- キャッシュネームサーバを使用せず、再帰要求を許可する場合は、フォワーダを使用します。

- DNSドメインが子ドメインでない場合は、ゾーン委任を使用するのが理想的です。委譲ではSOAレコードとNSレコードを指定できますが、フォワーダでは指定できません。さらに、バインドゾーンファイルを使用して委任をスレーブDNSサーバに自動的に複製し、フォワーダをに手動で追加することもできます `named.conf`。
- DNSドメインが子ドメインの場合は、サブドメインを使用します。

注: 内蔵DNSでBIND9 DNSサーバを使用している場合は、バグ892388のため、必ずONTAP 8.2.3以降を実行してください。

異なるサブネットおよびネットワークにあるデータLIFでの組み込みDNSの使用

ONTAPでは、DNSサーバを、クライアントが接続するデータLIFとは異なる物理ネットワークまたは仮想的に分割されたネットワークまたはIPスペースに配置することができます。この設定では、組み込みのDNSを使用して必要なデータLIFをクライアントに提供することもできます。

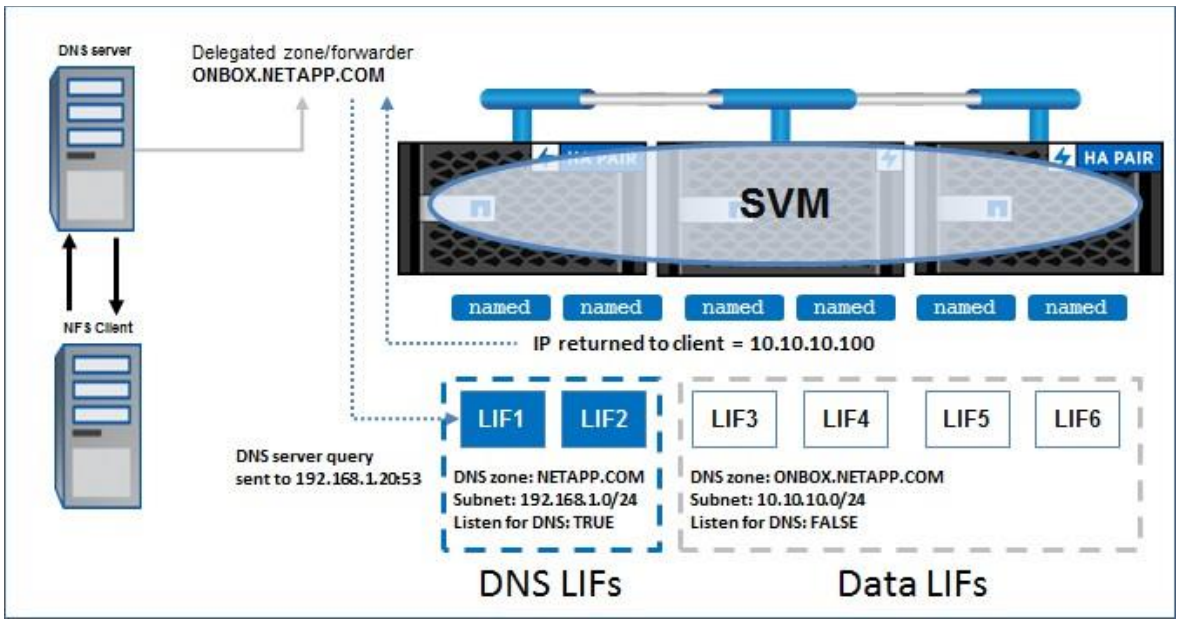
これを行うには、DNSサーバと通信できるLIFがDNSクエリをリスンするように設定します。DNSゾーンに参加するデータLIFは、DNSクエリをリスンしないで、目的のDNSゾーンを使用するように設定する必要があります（`-listen-for-dns-query false`）。

これにより、DNSサーバがDNS LIFを使用してSVMと通信できるようになります。また、サーバは通信できない可能性のあるクライアントにIPアドレスのリストを返すことができます。

注： `-listen-for-dns-query`「true」に設定したデータLIFにもを `-dns-zone` 指定する必要があります。そうしないと、クラスタでそのLIFがDNSクエリをリスンすることができません。

図4 に同様の構成を示します。

図4）同じSVMに複数のサブネットがある組み込みDNS



データLIFの設定は次の例のようになります。data1という名前のデータLIFはDNSサーバと通信できますが、dns-zoneという名前のデータLIFは次のことはできません。

```
cluster::*> net int show -vserver SVM -fields dns-zone,listen-for-dns-query,address
  (network interface show)
vserver lif      address       dns-zone                    listen-for-dns-query
------- -------- ------------- --------------------------- --------------------
SVM     data1    10.63.57.237 domain.netapp.com           true
SVM     dns-zone 10.10.10.200 onbox.domain.netapp.com    false
```

ONTAPノテエタLIFテノオンホトDNSノユウコウカ

データLIFでDNSクエリを処理するには、この `-listen-for-dns-query` オプションを「true」に設定する必要があります。 SVMがDNSクエリでデータLIFを返すためには、DNSゾーンに属する目的のデータLIFにを使用してDNSゾーンを割り当てる必要があります `-dns-zone`。DNSクエリのSOAとして機能するデータLIFは、クライアントがポイントするDNSサーバへのネットワーク接続が確立されている必要があります。この処理は無停止で実行できます。

ベストプラクティス5：DNSサーバとして機能するデータLIFに関する推奨事項

DNS要求の耐障害性とロードバランシングを確保するために、可能であれば複数のデータLIFをDNSサーバとして設定することを推奨します。また、 `lb-weight` DNS要求を処理するLIFのを0に設定して、データトラフィックにDNSゾーンで使用されないようにすることも理にかなっています。

組み込みのDNSロードバランシングの対象となるデータLIFは 、表3で説明したネットワークインターフェイスオプションの設定によって異なります。

表3）ONTAPに搭載されたDNSロードバランシング用のデータLIFオプション

ネットワークインターフェイスオプション	機能	権限レベル
`-dns-zone`	組み込みのDNSロードバランシング処理の対象となるデータLIFのDNSゾーンを指定します。1つのSVMに複数のDNSゾーンを指定できます。	admin
`-listen-for-dns-query`	データLIFがポート53でDNSクエリをリスンし、SOAとして機能するように指定します。	admin
`-lb-weight`	このパラメータを使用して、データLIFのロード バランシングの重みを変更します。ロードバランシングの重みは、1~100の任意の整数または「load」です。 DNSゾーン内のすべてのデータLIFでロードバランシングの重みを同じに指定すると、ラウンドロビンDNSと同様に、クライアント要求は均一に分散されます。ロード バランシングの重みが小さいデータLIFは、ロード バランシングの重みが大きいデータLIFと比べて、クライアント要求が割り当てられる回数が少なくなります。	上級

`listen-for-dns-query` オプションを使用すると、DNSゾーン内の特定のデータLIFのみをネームサーバとして指定し、他のデータLIFをDNSゾーンのデータトラフィックにのみ使用することができます。同じSVMに、組み込みのDNSロードバランシングゾーンには含まれておらず、データトラフィックの処理は可能なデータLIFを配置することもできます。

オンボックスDNSに参加しているデータLIFのlb-weightの手動変更

搭載されたDNSロードバランシングで複数のデータLIFが使用されている場合は `lb-weight` 、特定のデータLIFのをロードバランシングアルゴリズムのより早く機能させることができます。このユースケースの1つは、回転式ディスクを使用するノードや、RAMやCPUの多いノードを優先するのではなく、データLIFの重みでSSDまたはAll Flash FAS（AFF）システムを使用するクラスタ内のノードを優先することです。

たとえば、4ノードクラスタにA800sのHAペアがあり、2つのノードがSASシェルフを使用するFAS9xxxのノードである場合は、AFFノードが所有するデータLIFの重みがSASシェルフを使用するノードよりも大きいように設定することを推奨します。そうすることで、AFFシステムの強化されたパフォーマンス機能を活用できます。

LIFの重みを設定する際は、次のガイドラインを考慮してください。

- LIFの重みを100に設定すると、ほとんどの場合、データLIFがDNS要求で使用されます。
- LIFの重みを1に設定すると、そのデータLIFがDNS要求で使用されることはほとんどありません。
- すべて `lb-weights` 同じ場合は、ラウンドロビンDNSが使用されます。

- `lb-weights` データLIFのを手動で設定するかどうかを決定する際には、組み込みのDNSロードバランシングアルゴリズムがどのように機能するかに注意してください。

SOAレコードの送信を有効または無効にするためのONTAPの設定

Windows以外のDNSサーバなどでは、複数のサブネットで動作するオンボックスDNSゾーンを取得するために、クラスタからのSOAレコードの送信を無効にする必要がある場合があります。これらのレコードは、次のadvanced権限のコマンドで無効にできます。

```
cluster::> set advanced
cluster::*> network options send-soa modify -enable true
```

注： 同じクラスタでマルチプロトコルNAS（CIFS / SMBおよびNFS）を使用していて、を無効にする場合 `send-soa`は、両方の環境が正常に機能し、SOAレコードの送信が無効になっていることを確認してください。

SOAレコードの送信をディセーブルにすると、オンボックスDNSゾーンがDNS要求に対する非権限応答者としてレンダリングされます。

クライアントの信頼できるネームサーバとしてのデータLIFの使用

データLIFは、ポート53でDNS要求をリスンしてSOAサーバとして機能するように設定できるため、クライアントのネームサーバとしても使用でき、独立したDNSサーバとしても機能します。この設定は、DNSサーバを変更できない環境や、クライアントがドメイン内のDNSサーバにアクセスできない環境で役立ちます。

データLIFをネームサーバとして使用するには、クライアントのDNS設定を行うだけです（`resolv.conf` Linuxクライアントの場合は、Windowsクライアントの場合は[DNS]プロパティボックス）。詳細および例については、ONTAPデータLIFをDNSサーバとして使用するクライアントの設定を参照してください。

サードパーティ製ロードバランサ

DNSロードバランシングを実行するハードウェアまたはソフトウェアソリューション（F5ネットワークなど）は、DNSなどのロードバランシングトラフィック用にONTAPでサポートされています。サードパーティ製ロードバランサの設定およびサポート情報については、ベンダーにお問い合わせください。

オンボックスDNSによるアプリケーションへの影響

一部のアプリケーションは、内蔵DNSとうまく連携しない場合があります。たとえば、ネットワークの問題や中断（ストレージフェイルオーバーを含む）中にOracle dNFSが破損する可能性があります。これは、再接続中にアプリケーションが特定のホストの新しいIPを受信したことに気づかない可能性があるためです。詳細については、TR-3633：『Oracle Databases on ONTAP』を参照してください。

この種の問題は、すべてのアプリケーションに同じ影響を与えるわけではありません。オンボックスDNSを導入する前に、環境で適切にテストし、アプリケーションベンダーに確認してください。

組み込みのDNSロードバランシングの設定

このセクションでは、ONTAPでの内蔵DNSロードバランシングの設定について説明します。

SVMでの組み込みDNSの設定

クラスタに搭載されたDNSを設定するには、適切なデータLIFを選択して負荷分散に追加します。DNSクエリをリスンするDNSサーバとして機能するデータLIFを指定してください。

1. データLIFでDNSゾーンを有効にします。

```
::> net int modify -vserver [SVM] -lif [LIF] -dns-zone [cdot.domain.com]
```

2. DNSクエリをリスンするようにLIFを設定します（8.2以降のみ）。

```
::> net int modify -vserver [SVM] -lif [LIF] -listen-for-dns-query true
```

3. advanced権限モードで、データLIFのlb-weightを「load」または目的のlb-weightに設定します。

```
::*> net int modify -vserver [SVM] -lif [LIF] -lb-weight load
```

内蔵DNSと連携するようにWindows DNSサーバを設定する

次の設定手順を使用して、Windows DNSサーバに内蔵DNSを設定できます。このセクションでは、次のシナリオについて説明します。

- 委譲
- スタブゾーン
- 条件付きフォワーダ

Windows DNSでのDNS委任の設定

次の手順は、Windows DNSサーバでDNS委任を設定する方法を示しています。この例で使用しているサーバのバージョンはWindows 2008R2ですが、他のWindowsサーバにも同じ手順が適用されます。正式な手順については、Microsoft TechNetのドキュメントを参照してください。

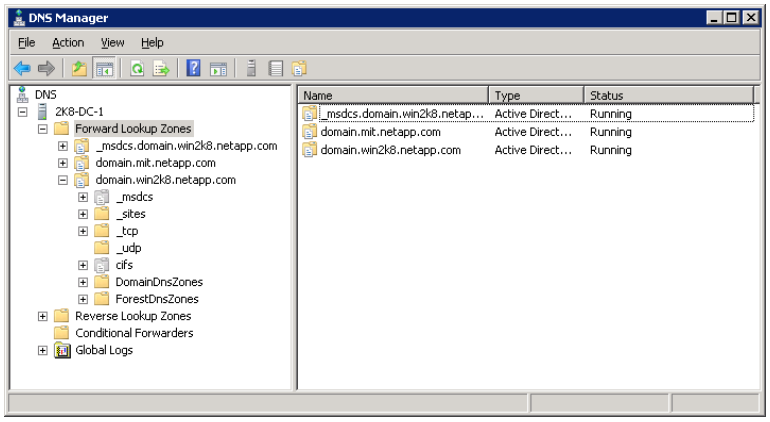
DNS委譲は、次の目的で使用されます。

- DNSネームスペースの管理を組織内の別の場所に委任する
- 大規模なゾーンを小さなゾーンに分割して、複数のサーバに負荷を分散したり、フォールトトレランスを向上させたりする
- サブドメインを追加するためのネームスペースの拡張

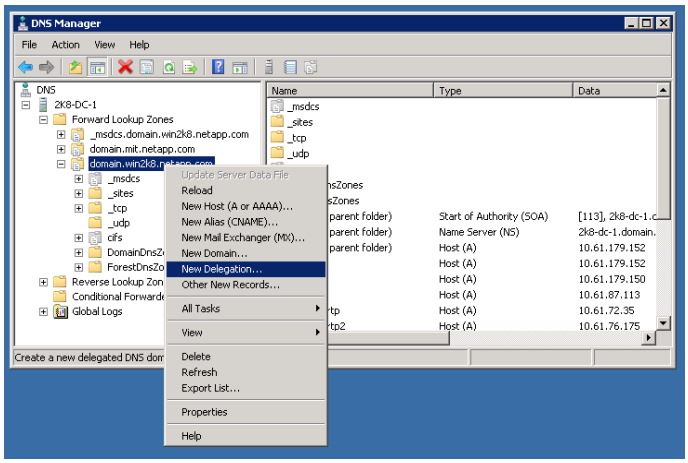
組み込みのDNSの場合、委譲を使用してDNSゾーントラフィックをSVM上のデータLIFにリダイレクトできます。一般に、データLIFのDNSゾーンがDNSサーバと同じDNSドメインにある場合は、委譲が使用されます。たとえば、データLIFがを使用し `cluster.domain.com`、DNSサーバのドメインがであるとします `domain.com`。

DNS委任を設定するには、次の手順を実行します。

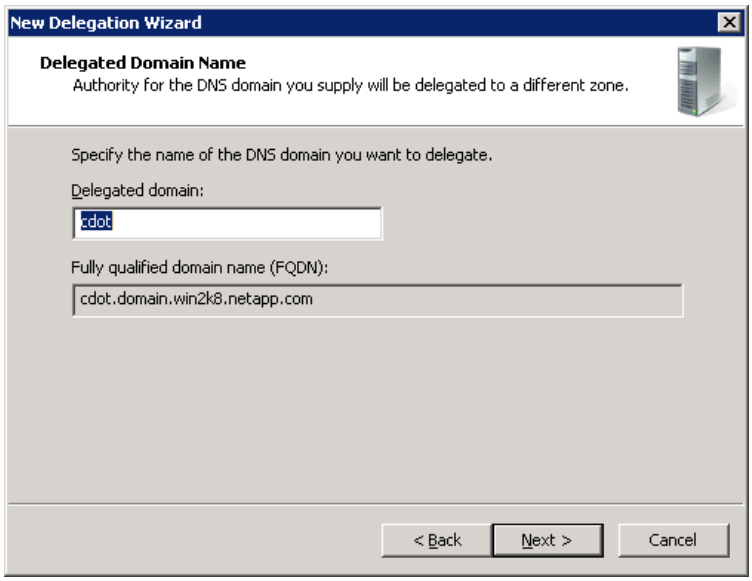
1. DNSマネージャコンソールを開きます。



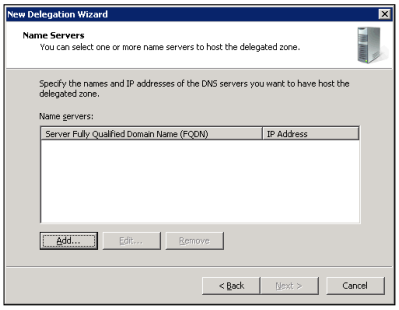
2. DNSドメインを右クリックし、[New Delegation]を選択します。

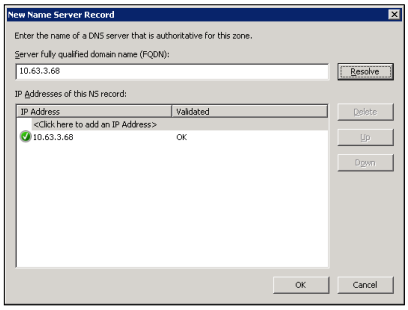


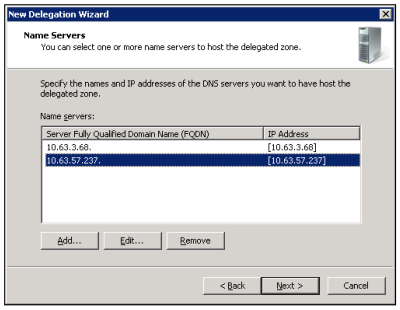
3. 委任されたドメインの名前を入力します。



4. ONTAP SVMデータLIFをネームサーバとして（一度に1つずつ）追加します。



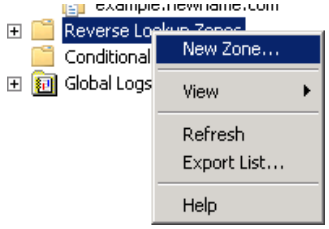




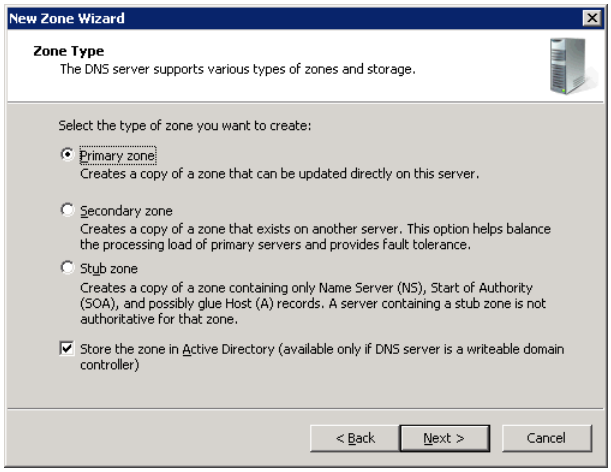
逆引き参照ゾーンとPTRレコードを設定するには、次の手順を実行します。

注： 内蔵DNSは、ONTAP 8.2より前のIPv4のリバースルックアップをサポートしていません。IPv6のサポートはONTAP 8.3で追加されました。Kerberosに対してのみホスト名を使用するようにクライアントを強制する場合は、PTRレコードを作成しないでください。これにより、IPを直接マウントすることがなくなり、ロードバランシングが確実に適用されます。ただし、Kerberos NFSが機能するためにPTRレコードが必要な場合もあります。

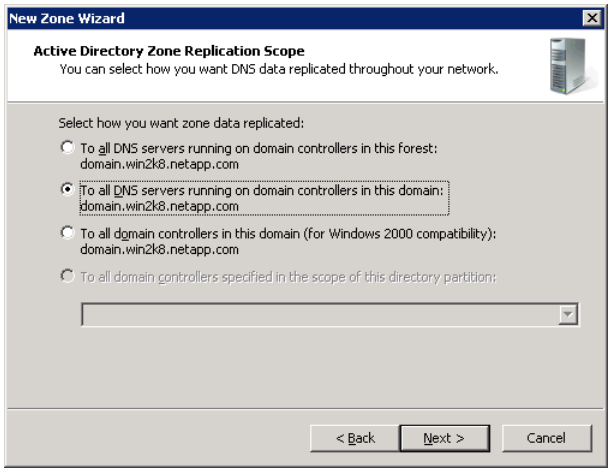
1. データLIFの逆引き参照ゾーンを作成します。



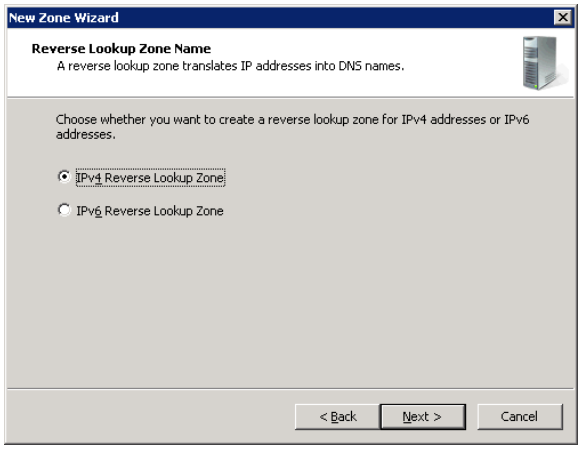
2. ONTAPのDNSでは逆引き参照を処理できないため、[プライマリゾーン]を選択します。



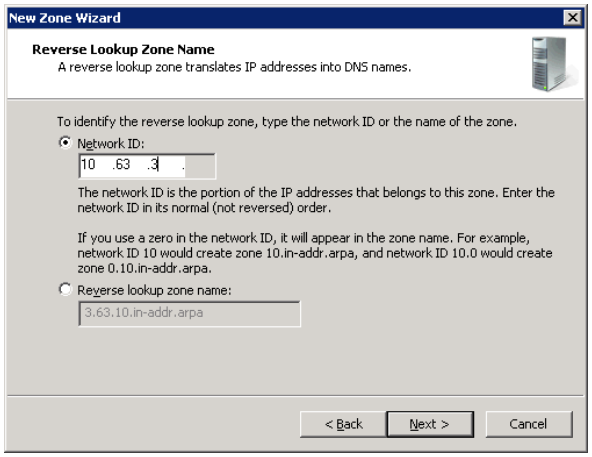
3. 使用するゾーンレプリケーションポリシーを選択します。



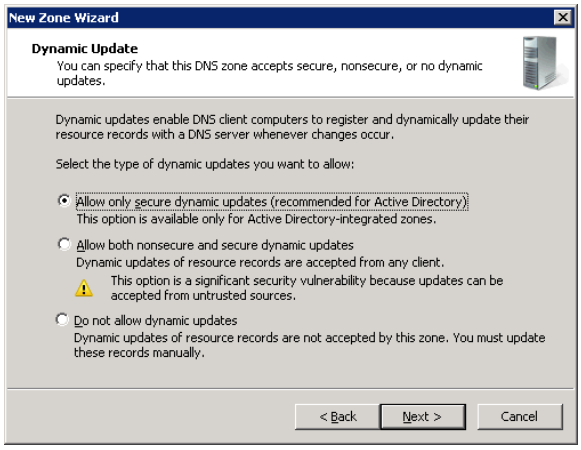
4. ONTAPのバージョンでサポートされる内容とデータLIFで使用される内容に応じて、検索ゾーンとしてIPv4またはIPv6を選択します。

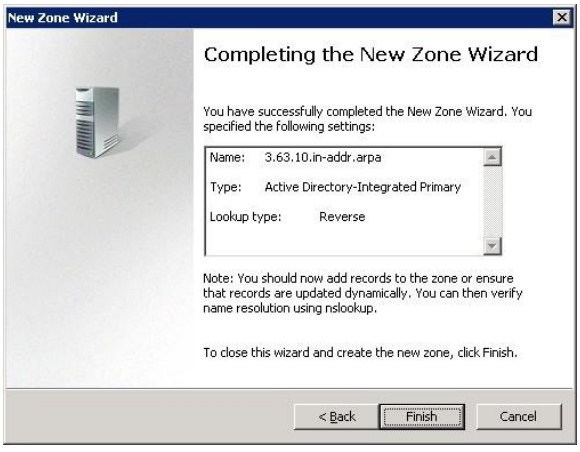


5. ネットワークID /サブネット（IPアドレスの最初の3オクテット）を入力します。



6. 動的更新ポリシーを選択します。





7. 他のサブネットについて、手順6～11を繰り返します。
8. `nslookup` またはを使用して、新しいゾーンのDNSルックアップをテストします `dig`。

```
C:\>nslookup cdot
Server: UnKnown
Address: ::1
```

```
Non-authoritative answer:
Name:    cdot.domain.win2k8.netapp.com
Address: 10.63.57.237

C:\>nslookup cdot
Server: UnKnown
Address: ::1

Non-authoritative answer:
Name:    cdot.domain.win2k8.netapp.com
Address: 10.63.3.68
```

Windows DNSでのDNSスタブゾーンの設定

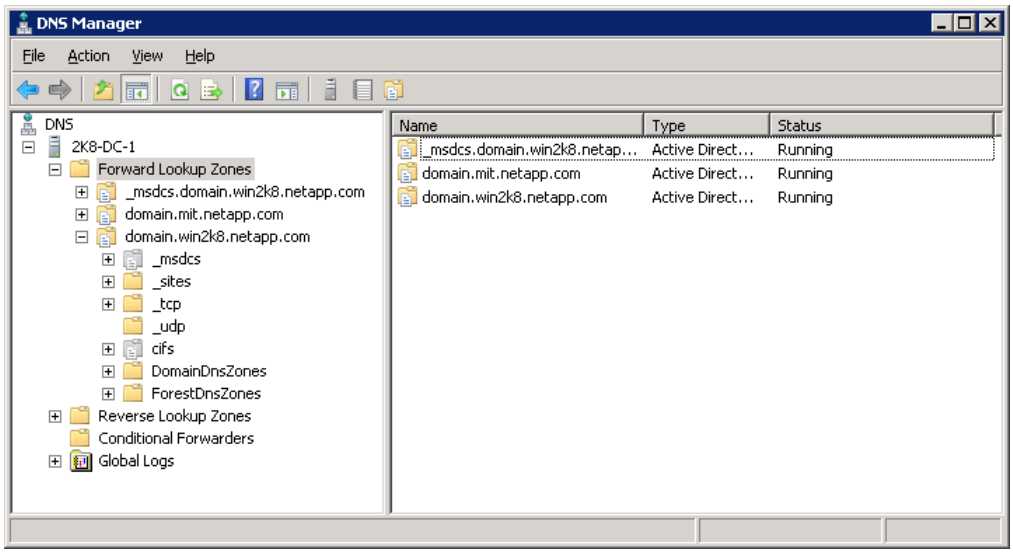
次の手順は、Windows DNSサーバでDNSスタブゾーンを設定する方法を示しています。この例で使用しているサーバのバージョンはWindows 2008R2ですが、他のWindowsサーバにも同じ手順が適用されます。公式な手順については、Microsoft TechNetのドキュメントを参照してください。

スタブゾーンは、DNSゾーンをActive Directoryと統合する必要がある場合や、ゾーンにSOAレコードが必要な場合に使用されます。内蔵DNSを使用すると、DNSサーバとしてリスンするデータLIFをスタブゾーンのSOAレコードとしてリストできるため、これは理想的なセットアップです。

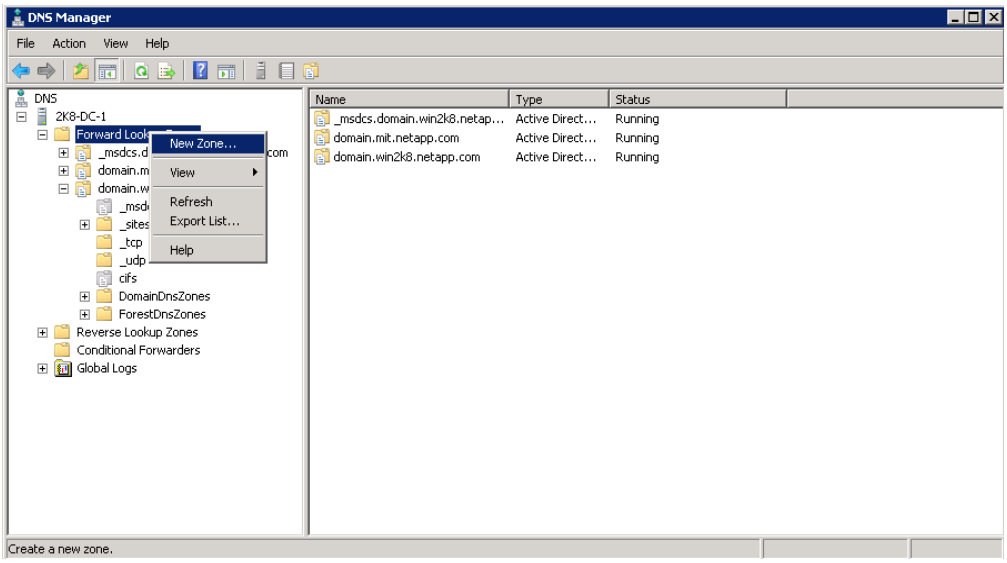
注: ONTAP内蔵DNSは SOAレコードのみを送信します。グルーレコードはONTAPから送信されません。

スタブゾーンを設定するには、次の手順を実行します。

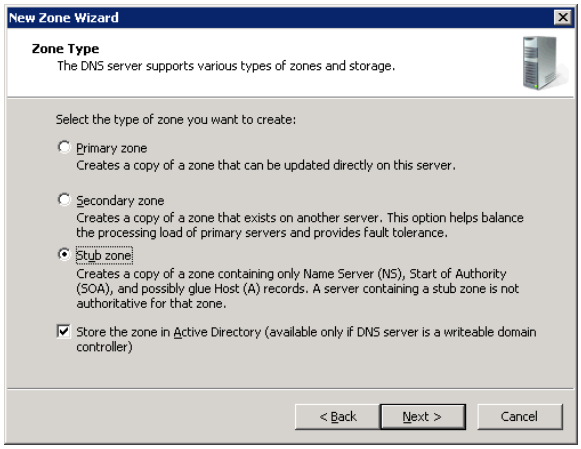
1. DNSマネージャコンソールを開きます。



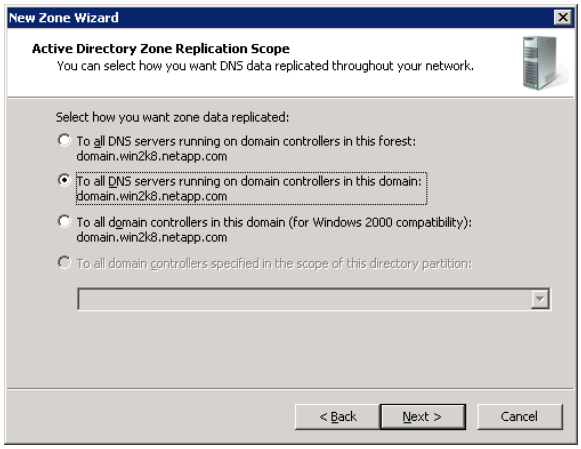
2. [Forward Lookup Zones]を右クリックし、[New Zone]を選択します。



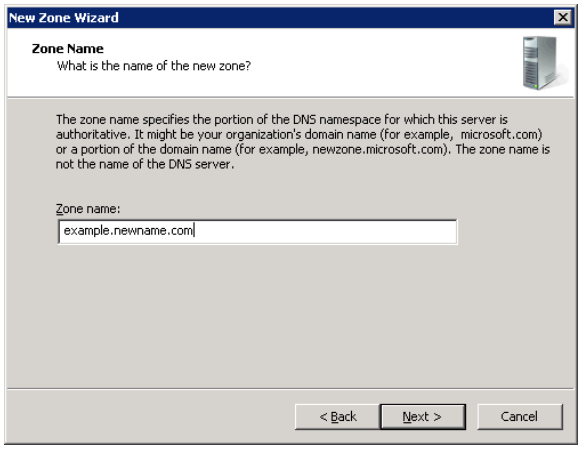
3. ゾーンとしてスタブゾーンを選択します。



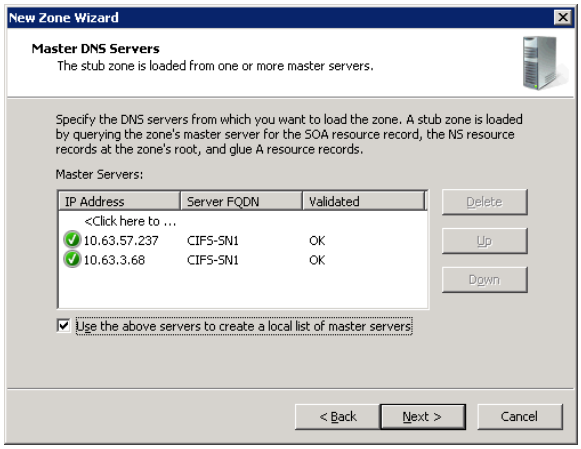
4. ゾーンレプリケーションがどのように機能するかを選択します。



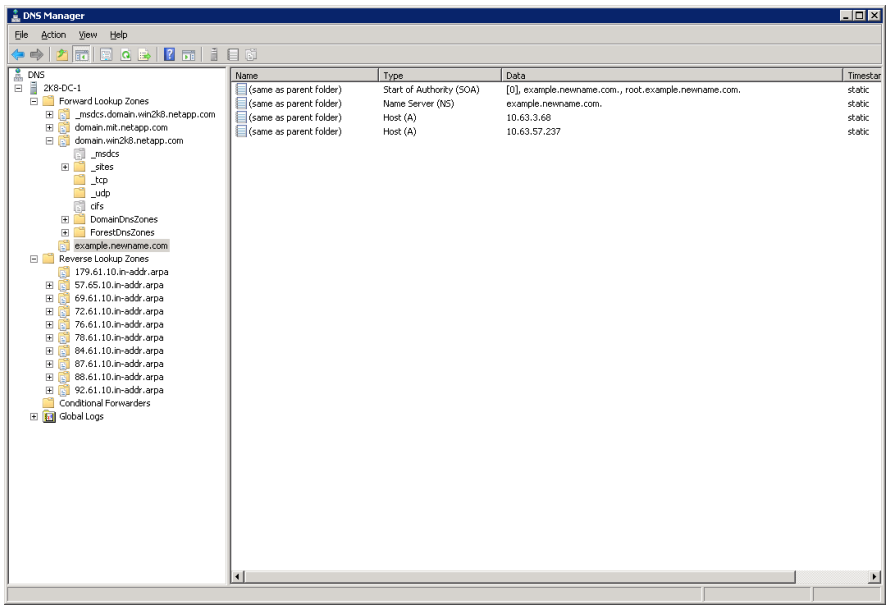
5. ゾーン名を指定します。



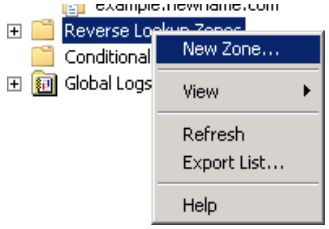
6. 組み込みのDNS用に設定されているすべてのデータLIFをマスターDNSサーバリストに追加します。[Use the Above Servers to Create a Local List of Master Servers]チェックボックスをオンにします。



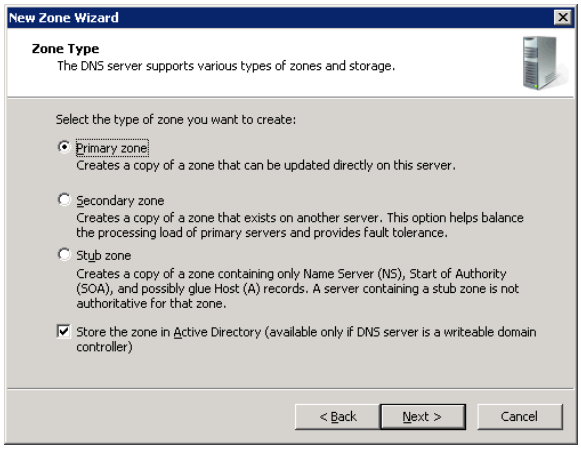
7. スタブゾーンにSOAレコードとNSレコードがあることを確認します。



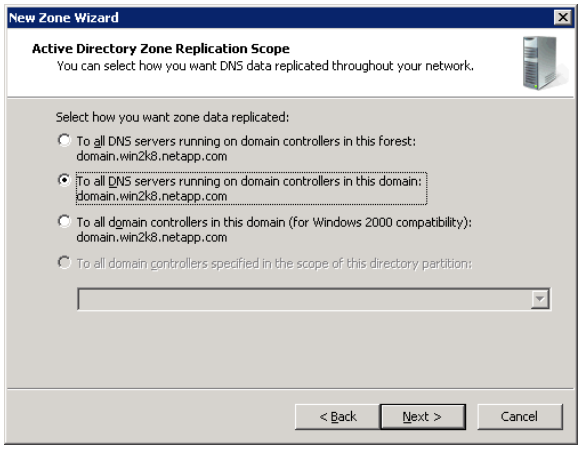
8. データLIFの逆引き参照ゾーンを作成します。



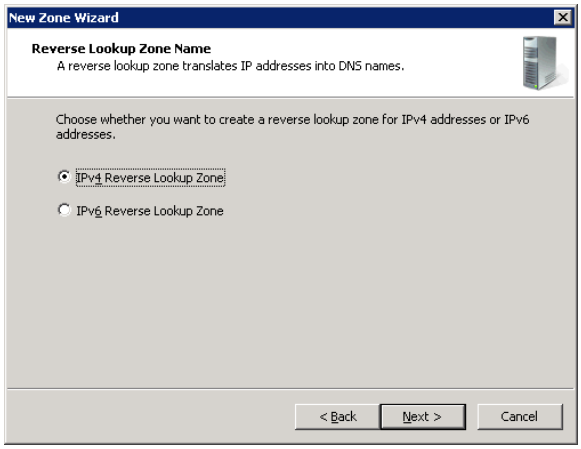
9. ONTAPのDNSでは逆引き参照を処理できないため、[プライマリゾーン]を選択します。



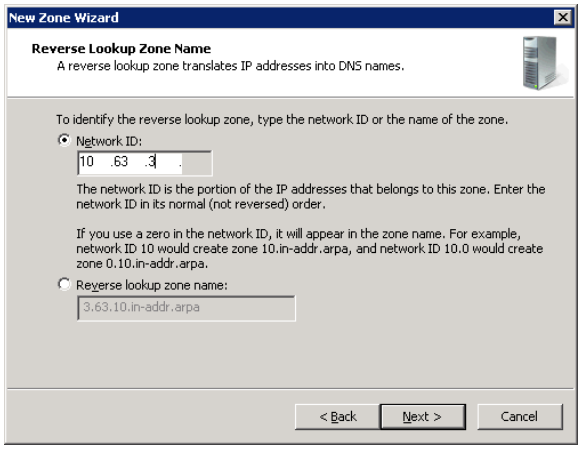
10. 使用するゾーンレプリケーションポリシーを選択します。



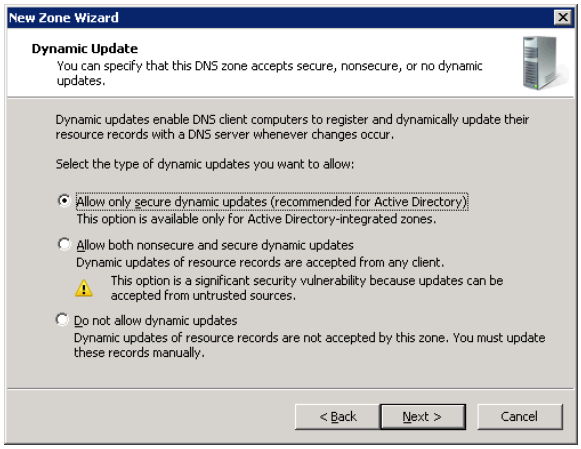
11. ONTAPのバージョンでサポートされる内容とデータLIFで使用される内容に応じて、検索ゾーンとしてIPv4またはIPv6を選択します。

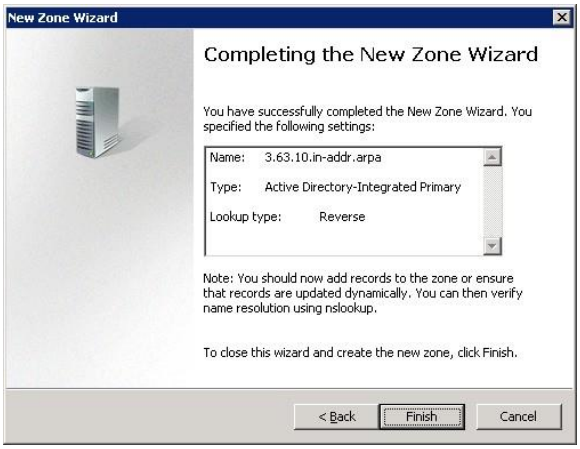


12. ネットワークID /サブネット（IPアドレスの最初の3オクテット）を入力します。

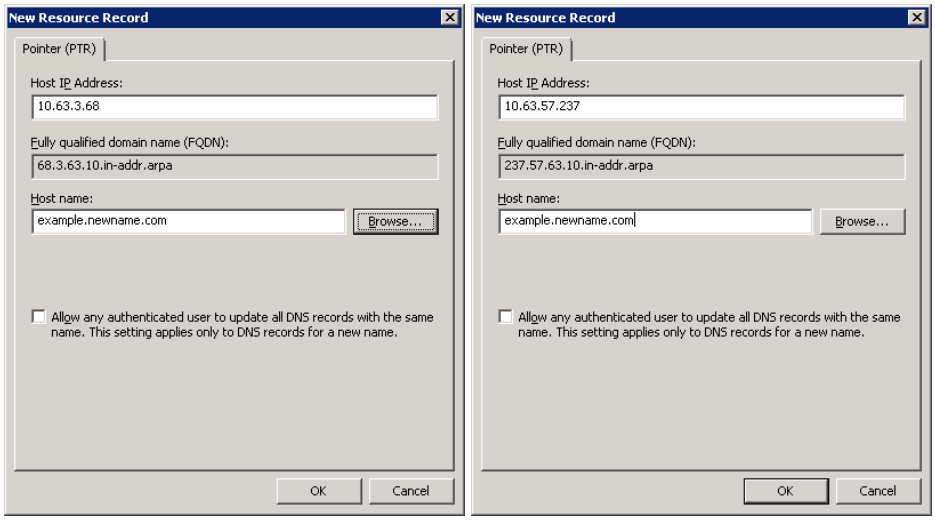


13. 動的更新ポリシーを選択します。





14. 他のサブネットについて、手順8～13を繰り返します。
15. ONTAPでは名前の逆引きがサポートされないため、データLIFのPTRレコードを追加します。



16. `nslookup` DNSでフォワードルックアップとリバースルックアップをテストするために使用します。

```
C:\>nslookup example.newname.com
Server: localhost
Address: ::1

Name:    example.newname.com
Addresses: 10.63.57.237
          10.63.3.68

C:\>nslookup 10.63.57.237
Server: localhost
Address: ::1

Name:    example.newname.com
Address: 10.63.57.237


C:\>nslookup 10.63.3.68
Server: localhost
Address: ::1
```

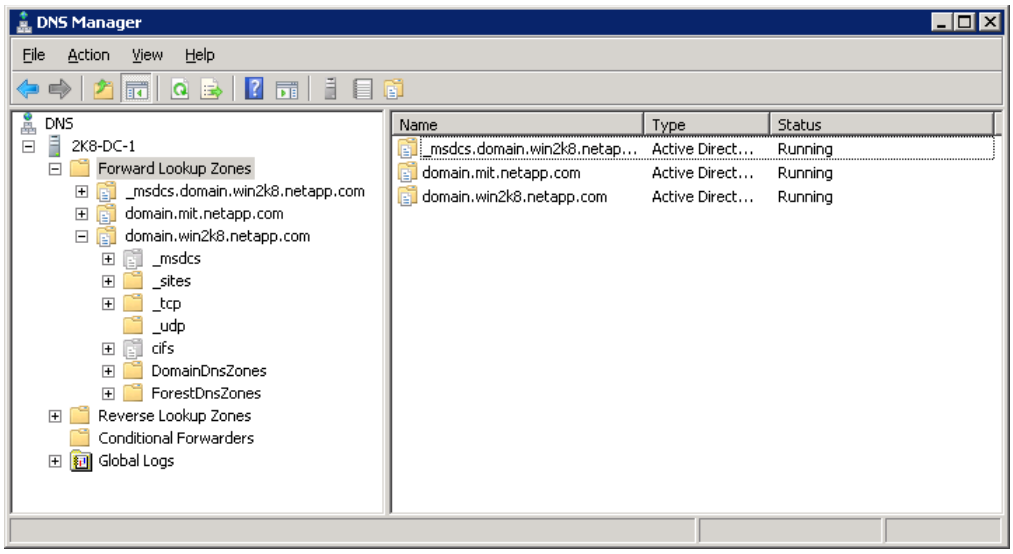
Windows DNSでの条件付きフォワーダの設定

次の手順は、Windows DNSサーバでDNS条件付きフォワーダを設定する方法を示しています。この例で使用しているサーバのバージョンはWindows 2008R2ですが、他のWindowsサーバにも同じ手順が適用されます。正式な手順については、Microsoft TechNetのドキュメントを参照してください。

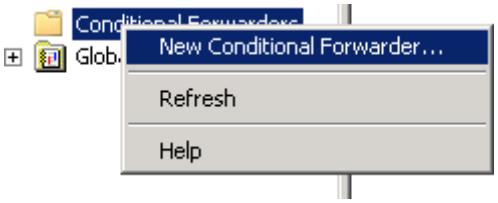
条件付きフォワーダは、クエリ内のDNSドメイン名に従って、DNSドメイン内のDNSサーバにDNSクエリを転送するために使用されます。ほとんどの場合、条件付きフォワーダは、転送されるデータLIFのDNSドメイン名がメインのDNSサーバのDNSドメインとは異なるドメインにある場合に、内蔵DNSで使用するのが適切です。たとえば、へのクエリが、`example.different.com` DNSドメインで設定された条件付きフォワーダで転送される場合など `domain.com`です。

Windows 2008で条件付きフォワーダを設定するには、次の手順を実行します。

1. DNSマネージャコンソールを開きます。

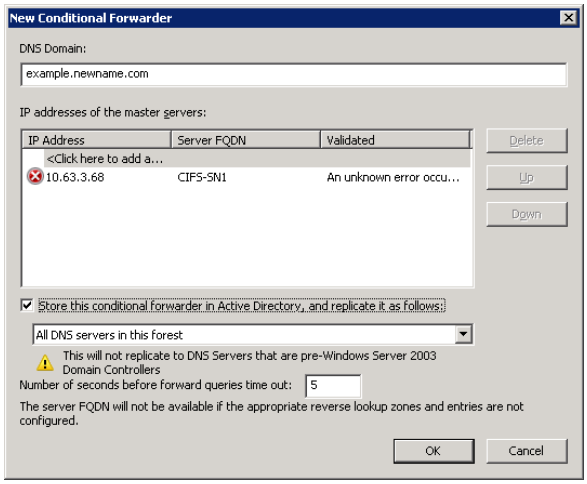


2. 条件付きフォワーダ（Conditional Forwarders）を右クリックし、新規条件付きフォワーダ（New



Conditional Forwarder）を選択します。

3. DNSドメインとデータLIFを入力します。エラーが発生した場合は、サーバがSOAレコード要求を送信していない可能性があります。問題を修正するか、スタブゾーンを使用してください。



4. [OK]をクリックし、を使用して `nslookup` 転送ゾーンをテストします。

```
C:\>nslookup example.newname.com
Server: localhost
Address: ::1

Name:    example.newname.com
Addresses: 10.63.57.237
          10.63.3.68
```

```
C:\>nslookup 10.63.57.237
Server: localhost
Address: ::1

Name:    example.newname.com
Address: 10.63.57.237


C:\>nslookup 10.63.3.68
Server: localhost
Address: ::1
```

オンボックスDNSと連携するためのバインド形式のDNSサーバの設定

多くの場合、特にActive Directoryが環境に存在する場合は、DNS解決にWindowsサーバが使用されます。これは、Active Directoryの機能にはDNSが必要であるだけでなく、Windowsが提供するシンプルな統合とGUIが必要であるためです。

ただし、BINDやBIND9などのLinuxベースのDNSサーバを使用する環境もあります。これらの構成では、「BIND DNSで使用する構成の決定」セクションで説明されているように、オンボックスDNSの設計を検討する場合にも同じ概念が適用されます。

次の例では、BINDをDNSサーバとして使用するCentOS / RHEL 7ボックスを使用しています。次の構成について説明します。

- プライマリDNSサーバと同じドメインにDNSゾーンがあるデータLIF
- プライマリDNSサーバとは別のドメインにDNSゾーンがあるデータLIF

組み込みのDNS設定：バインドサーバと同じドメインのデータLIF

バインドサーバの親ドメインと同じドメインのデータLIFを使用するには、ゾーンファイルでサブドメインエントリを使用します。サブドメインを使用すると、DNSサーバは、ゾーン転送を通じて特定のゾーンに対する要求を適切なサーバに渡すことができ、フォールトトレランスを実現できます。サブドメインが使用されていない場合、DNSサーバは要求がA/AAAAレコード要求であると判断し、NXDOMAIN（ドメインが存在しない）でルックアップが失敗する可能性があります。

BINDサーバーでゾーンを追加するのは、構成ファイルを変更するのと同じくらい簡単です。サブドメインを追加するには、次の手順を実行します。

1. オンボックスDNSサブドメインのゾーン設定をマスターゾーンファイルに追加します。
2. DNSクエリをリスンするデータLIFのNSレコードとA（GLUE）レコードを追加します。
3. 親DNSサーバのNSレコードを追加します。

次に、親DNSサーバと同じDNSドメイン内のゾーンにサブドメインを設定する例を示します。これは、SVMに搭載されているDNS設定です。

```
cluster::> net int show-zones -vserver SVM
  (network interface show-zones)
                                                              Listen For
Vserver          Interface Name DNS Zone                     DNS Query
---------------  -------------- ---------------------------  ----------
SVM
                 data           onbox.bind.SVM.com
                                                              true
                 data2          onbox.bind.SVM.com
                                                              false
2 entries were displayed.
```

これはDNSサーバのドメイン/ホスト名です。

```
# hostname
dns.bind.SVM.com
```

次のサンプルサブドメインゾーンがマスターゾーンファイルに追加されました。

```
$ORIGIN onbox.bind.SVM.com.
@                         IN      NS      onbox.bind.SVM.com.
                          IN      NS      dns.bind.SVM.com.
onbox.bind.SVM.com.    IN      A       10.193.67.226
```

次の手順を実行すると、そのゾーンのオンボックスDNS要求がクラスタから返されます。

```
[root@centos7 ~]# nslookup onbox
Server:         10.193.67.227
Address:        10.193.67.227#53

Non-authoritative answer:
Name:   onbox.bind.SVM.com
Address: 10.193.67.226

[root@centos7 ~]# nslookup onbox
Server:         10.193.67.227
Address:        10.193.67.227#53

Non-authoritative answer:
Name:   onbox.bind.SVM.com
Address: 10.193.67.229
```

DNSサーバをバインドするためのPTRレコードの追加

場合によっては、DNSゾーンに参加しているSVMのデータLIFに対してリバースルックアップが機能するように、DNSサーバをバインドするためにPTRレコードを追加する必要があります。特に、Kerberosが関係している場合、PTRレコードの追加が有効になります。

PTRレコードの追加は、他のPTRレコードの追加と同じ方法で行われます。目的の逆引き参照ゾーンに必要なエントリをゾーンファイルに追加します。

次の例を参照してください。

```
[root@dns named]# cat 67.193.10.in-addr.arpa.zone
$TTL 86400
@   IN SOA      bind.SVM.com.        root.SVM.bind.com.
        ( 2013042202 ;Serial
        3600        ;Refresh
        1800        ;Retry
        604800      ;Expire
        86400       ;Minimum TTL
)

67.193.10.in-addr.arpa.                IN      NS      dns.bind.SVM.com.

225     IN      PTR     centos7.bind.SVM.com
227     IN      PTR     dns.bind.SVM.com
226     IN      PTR     onbox.cluster.com
229     IN      PTR     onbox.cluster.com
```

リバースルックアップの作業例を次に示します。

```
[root@centos7 ~]# dig PTR 10.193.67.226

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <<>> PTR 10.193.67.226
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 44516
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;10.193.67.226.                 IN      PTR
```

```
;; AUTHORITY SECTION:
.                       10793   IN      SOA     a.root-servers.net. nstld.verisign-grs.com.
2016062700 1800 900 604800 86400
```

Bind9構成とその他のサードパーティDNSサーバ

Bind9 DNSサーバは同じ一般設定を使用しますが、ファイルの場所が異なります。たとえば、named.conf for BIND9は /etc/bind ではなくに格納され /etc/namedます。詳細については、DNSアプリケーションの製品ドキュメントとマニュアルページを確認してください。

GUIを実装するサードパーティのDNSサーバーなど、他のサードパーティのDNSサーバーの場合、設計の背後にある概念は同じです。

- サブドメインは、親と同じDNSドメイン内のオンボックスDNS設定に使用します。
- 異なるDNSドメインのオンボックスDNS設定には、フォワーダを使用します。

追加情報の場合は、サードパーティ製GUIのプロバイダにお問い合わせください。

組み込みのDNS設定：バインドサーバとは別のドメインにあるデータLIF

バインドサーバの親ドメインとは異なるドメインのデータLIFを使用するには、に転送ゾーンエントリを追加します named.conf。転送ゾーンが他のDNSサーバにレプリケートされない可能性があるため、それに応じて計画してください。

転送エントリには、次の情報が必要です。

- DNSゾーンの名前
- 転送のタイプ
- DNSサーバとして使用するデータLIFのIPアドレスにエントリを転送する
- 複数のDNSサーバを使用している場合は named.conf 、が他のサーバにレプリケートするように設定されていない可能性があるため、これらのサーバにもゾーンを追加します。

これは、SVMに搭載されているDNS設定です。

```
cluster::> net int show-zones -vserver SVM
  (network interface show-zones)
                                                    Listen For
Vserver          Interface Name DNS Zone            DNS Query
---------------  ---------------  ----------------- -------------
SVM
                 data             onbox.cluster.com
                                                    true
                 data2            onbox.cluster.com
                                                    false
2 entries were displayed.
```

これはDNSサーバのドメイン/ホスト名です。

```
# hostname
dns.bind.SVM.com
```

次の例では、bindのnamed.confにある転送ゾーンの設定例を参照してください。

```
zone "onbox.cluster.com" IN
        { type forward;
        forwarders {10.193.67.226;};
};
```

これらの手順を実行すると、そのゾーンのnslookupの結果は次のようになります。

```
[root@centos7 ~]# nslookup onbox.cluster.com
Server:         10.193.67.227
```

```
Address:        10.193.67.227#53

Non-authoritative answer:
Name:   onbox.cluster.com
Address: 10.193.67.229

[root@centos7 ~]# nslookup onbox.cluster.com
Server:         10.193.67.227
Address:        10.193.67.227#53

Non-authoritative answer:
Name:   onbox.cluster.com
Address: 10.193.67.226
```

ONTAPのデータLIFをDNSサーバとして使用するためのクライアントの設定

場合によっては、クラスタのデータLIFをDNSサーバとして使用するようにクライアントの設定が必要になることがあります。これが必要になる可能性がある場合は、次のような場合があります。

- クライアントはプライマリDNSサーバにネットワークアクセスできません。
- プライマリDNSサーバは、ゾーン、委任、またはフォワーダを使用するように変更できません。
- 一般設定。

クライアントはホスト名の解決時に複数のネームサーバおよびゾーンを使用できるため、クライアントはプライマリDNSドメインとクラスタで設定されているデータLIFドメインの両方を使用できます。データLIFをローカルDNSサーバとして使用したり、組み込みのDNSと一般的なDNSゾーン設定を同じSVMで使用したりすることもできます。

組み込みのDNSをクライアントのDNSネームサーバとして設定するには、まずSVMに組み込みのDNSを設定し、少なくとも1つのデータLIFがDNSクエリをリスンできるようにします。また、クラスタがSOAレコードを送信していることを確認する必要があります。

```
cluster::> net int modify -vserver SVM -lif data -dns-zone cluster.local -listen-for-dns-query
true

cluster::> net int show -vserver SVM1 -lif data -fields dns-zone,listen-for-dns-query,address
  (network interface show)
vserver lif address        dns-zone      listen-for-dns-query
---------- ----- ----------------- ----------------- --------------------------
SVM1    data 10.193.67.220 cluster.local true

cluster::> set advanced
cluster::*> network options send-soa show
Enable sending SOA: true
```

次に、このデータLIFをDNSネームサーバとして使用するようにクライアントを設定し、データLIFに設定されている検索ドメインを追加します。

resolv.confを使用したLinuxクライアントの設定

Linuxクライアントでは、このような設定は `resolv.conf` ファイルを使用して行われます。次のクライアントは、設定前に `resolv.conf`DNSドメインを `cluster.local` 解決できなかったことを示しています。

```
```

そのDNSゾーンのデータLIFを使用するようにクライアントが設定されていれば、適切に解決できます。

次の例は、組み込みのデータLIFをLinuxクライアント用のDNSサーバとして設定する方法を示しています。

```
# cat /etc/resolv.conf
```

```
# Generated by NetworkManager
search cluster.local
nameserver 10.193.67.220

# dig cluster.local

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <<>> cluster.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15220
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cluster.local.                 IN      A

;; ANSWER SECTION:
cluster.local.          0       IN      A       10.193.67.220

;; AUTHORITY SECTION:
cluster.local.          86400   IN      NS      cluster.local.

;; Query time: 24 msec
;; SERVER: 10.193.67.220#53(10.193.67.220)
;; WHEN: Tue Jun 21 13:02:44 EDT 2016
;; MSG SIZE rcvd: 72
```

リバースルックアップも機能します。

```
# dig 10.193.67.220

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <<>> 10.193.67.220
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 60475
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;10.193.67.220.                 IN      A

;; Query time: 12 msec
;; SERVER: 10.193.67.220#53(10.193.67.220)
;; WHEN: Tue Jun 21 13:03:18 EDT 2016
;; MSG SIZE rcvd: 42
```

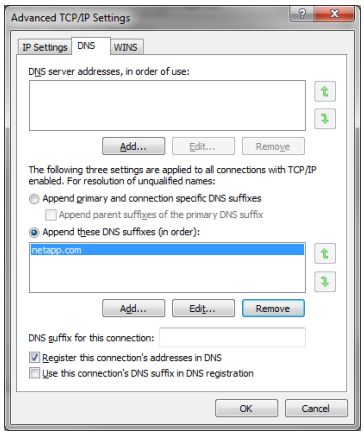
他のDNSサーバを設定に追加して、名前を適切に解決できます。たとえば、Google DNSサーバを追加すると、google.comを解決できます。

```
# cat /etc/resolv.conf
# Generated by NetworkManager
search cluster.local
nameserver 10.193.67.220
nameserver 8.8.8.8

# nslookup google.com
;; Got recursion not available from 10.193.67.220, trying next server
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.219.206
```

On-Cox DNSを独立したDNSサーバとして使用するためのWindowsクライアントの設定

Windowsクライアントは、SVM上のデータアクセス用のDNSサーバとしてONTAPデータLIFを使用することもできます。Windows構成では一般にGUIを使用しますが、PowerShellなどのCLIユーティリティも使用できます。この例ではGUIの設定について説明します。この例では、既存のDNS設定に加えて、データLIFをDNSサーバとして使用しています。

これは、Windowsクライアントの既存のDNS設定です。

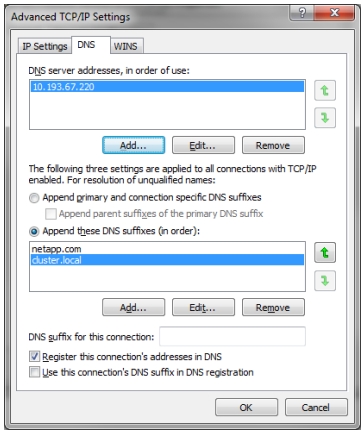


DNSサーバはDHCPを介してプルされています。DNSサフィックスが手動で設定されている。

現在のところ、データLIFのゾーン（`cluster.local`）に対するnslookup要求は失敗します。

```
C:\>nslookup cluster.local
Server: dns.netapp.com
Address: 10.193.67.200

*** dns.netapp.com can't find cluster.local: Non-existent domain
```

`cluster.local` が照会されたときにクラスタのデータLIFをDNSサーバとして使用してクラスタのデータLIFを返す場合の設定は次のようになります。



ここでは、DNSサーバとして搭載されたロードバランシングの対象となるデータLIFのみを追加しました。他のDNSサーバも追加する必要があります。

新しいサーバが追加されたら、DNSキャッシュをフラッシュし（Windowsはデフォルトで24時間DNSをキャッシュ）、クラスタゾーンのnslookupを試します。

```
C:\> nslookup cluster.local
Server: cluster.local
Address: 10.193.67.220

Name:    cluster.local
Address: 10.193.67.220
```

まとめ

内蔵DNSロードバランシングは、ラウンドロビンDNSロードバランシングなどの外部ソリューションを使用する代わりに使用できます。負荷に基づいてDNS要求の負荷を分散できることは、スケールアウトクラスタへの全体的な影響を軽減し、エンタープライズ環境でNAS接続を提供するインテリジェントな方法を提供します。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを確認してください。

- ONTAPドキュメント センター
  https://docs.netapp.com/ontap-9/index.jsp
- ONTAPとONTAP System Managerのドキュメント リソース
  https://www.netapp.com/data-management/oncommand-system-documentation/
- NetAppの製品ドキュメント
  https://www.netapp.com/support-and-training/documentation/

バージョン履歴

バージョン	日付	ドキュメント バージョン履歴
バージョン1.0	2016年7月	初版リリース
バージョン2.0	2016年10月	ONTAP 9.1用に更新
バージョン2.1	2020年5月	マイナーリビジョン
バージョン2.2	2021年2月	マイナーリビジョン

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4523-0221-JP

NetApp