



権威 DNS のキャパシティとパフォーマンスのガイドライン

この章では、64 ビットの Cisco Prime Network Registrar 8.3.5.4 以降のシステムサイジングに役立つ、権威 DNS のキャパシティとパフォーマンスのガイドラインについて説明します。

- [DNS システムのデプロイメント上の制限 \(1 ページ\)](#)
- [DNS データベースアーキテクチャ \(2 ページ\)](#)
- [DNS システムのサイジング \(3 ページ\)](#)

DNS システムのデプロイメント上の制限

Cisco Prime Network Registrar では、権限 DNS システムの最大構成サイズについて次の推奨事項があります。次の推奨事項は、Cisco Prime Network Registrar の権威 DNS サーバ（プライマリサーバ、プライマリ HA サーバ、またはセカンダリサーバ）に基づいています。冗長 DNS アーキテクチャには、すべて同じデータを処理するこれらのタイプのサーバが複数含まれます。したがって、新しいサーバのセットを導入することで、キャパシティを水平方向に拡張できます。これらの推奨事項は、DNS 展開が適切に機能するためのガイドラインです。



(注) DNSSEC 対応ゾーン（Cisco Prime Network Registrar 9.1 以降のバージョン）には、ゾーン内の RR の数を大幅に増やす自動生成 RR が含まれます。

- 権威 DNS サーバ（プライマリサーバ、HA ペアサーバ、またはセカンダリサーバ）あたり最大 2,500 万 RR、理想的にはゾーンあたり 200 万 RR を超えないようにします。複数の DNS プライマリサーバは、より多くの RR を必要とする展開に使用できます。
- 権威 DNS サーバ（プライマリサーバ、HA ペアサーバ、またはセカンダリサーバ）あたり最大 10000 ゾーン。複数の DNS プライマリサーバは、より多くのゾーンを必要とする展開に使用できます。
- プライマリサーバまたは HA ペアサーバあたり最大 4 台のセカンダリサーバ。

- 最大 2 階層のセカンダリサーバ（第 1 階層のセカンダリサーバと第 2 階層のセカンダリサーバ）。
- 第 1 階層のセカンダリサーバあたり最大 2 台の第 2 階層のセカンダリサーバ。

DNS データベースアーキテクチャ

権威 DNS サーバは、インメモリキャッシュとオンディスクデータベースの組み合わせを使用して、権威 RR データを保存および維持します。サイジングを目的として、各 RR には RR キャッシュ用に 300 バイトのメモリ、RR DB 用に 300 バイトのディスク容量が必要であると想定しています。CSET DB は RR セットへの変更を記録するため、各 RR のディスク容量の要件が高くなりますが、これらの変更はゾーンごとに保持される変更履歴の数に制限されます。

RR DB

- DNS サーバで設定されたゾーンのすべての RR（保護および非保護）を保存するデータベース。
- プライマリ DNS サーバでは、RR データの編集は、管理操作（つまり、RR の追加）、または DNS の更新とゾーンのスカベンジングによって RR DB に書き込まれます。セカンダリでは、RR DB はゾーン転送によって書き込まれます。
- RR DB はすべての ADNS サーバ（プライマリ/セカンダリ）に必要です。

RR キャッシュ

- RR DB データのサブセットを保存する（名前セット全体を保存する）ことで、クエリのパフォーマンスが向上します。
- 最もアクティブな RR データは、DNS クエリ処理によって生成された RR DB ルックアップの一部として、RR キャッシュに動的に保存されます。
- RR キャッシュのメモリフットプリントは、設定可能な DNS サーバ属性（*mem-cache-size*）によって制限されます。最大キャッシュサイズに達すると、DNS サーバは古いエントリをキャッシュから削除して、新しいエントリ用のスペースを確保します。各 RR では、約 300 バイトのメモリが必要です。
- DNS サーバのリロードや再起動により、RR キャッシュが削除されます。サーバが再起動すると、クエリトラフィックに基づいて再構築されます。
- RR キャッシュは、すべての ADNS サーバ（プライマリ/セカンダリ）に必要です。

CSET DB

- 増分ゾーン転送要求（IXFR）に応答するために必要な RR 変更（追加、削除、保護の変更、および更新）を保存するデータベース。
- RR 変更は最初に RR DB に保存され、次に CSET DB に保持されます。

- 増分ゾーン転送を処理する必要がない DNS サーバ（つまり、アウトバウンド IXFR を送信しないセカンダリサーバ）の場合は、永続的な変更セット（*csetdb-persist-csets*）を無効にすることで、サーバのパフォーマンスを向上させることができます。デフォルトでは、変更は CSET DB に自動的に保持されます。
- DNS は、制限された設定可能な変更数（*csetdb-htrim-max-cset-kept*）のみを維持し、最大数に達すると自動的にエントリをトリミングします。トリミングは、データベースサイズの制限に役立ちます。DNS アップデートを使用する環境では、フルゾーン転送を回避するために、保持する変更の数を増やすことを推奨します。
- CSET DB が削除されると、DNS サーバは空のデータベースを作成し、新しいゾーンの履歴データがデータベースに入力されるまでフルゾーン転送（AXFR）で応答します。

HA DB

- DNS HA ペアに関するステート情報と、通信中断中またはパートナーダウンイベント時の RR 変更に関するデータを保存するデータベース。
- プライマリ HA DNS サーバ（メインおよびバックアップ）にのみ適用されます。
- HA DB が削除されると、HA 同期によってすべてのゾーンデータが HA メインから HA バックアップにプッシュされます。

DNS システムのサイジング

Cisco Prime Network Registrar の DNS 展開は、RR とゾーンの数、DNS 更新アクティビティ、および停止中または更新中のリカバリ時間に応じて、小規模、中規模、または大規模に分類できます。ゾーンの数は、展開のサイズに影響を与える可能性があります。主に RR の数が決定要因となります。また、DNS 展開に多数の RR やゾーンが必要な場合は、複数の DNS 展開を使用することを推奨します。理想的には、関連するゾーンと RR が一緒に設定されるようにデータを適切に分離します。



- (注) 権威 DNS システムを適切に機能させるには、システムのディスク容量とメモリを監視することが重要です。権限のある DNS サーバのメモリが不足すると、クラッシュします。ディスク容量が不足すると、要求を処理できなくなり、データベースが破損して使用できなくなる可能性があります。

DNS 展開のリージョン管理

リージョナルサーバは、すべての Cisco Prime Network Registrar ローカルクラスタのライセンス管理を提供し、Cisco Prime Network Registrar の DNS 展開の集中管理と複製を可能にします。リージョン DNS クラスタ管理を使用する場合は、次の推奨事項に従ってシステムのサイジングと構成を調整します。

- 4 CPU 以上
- 8 GB 以上の RAM
- ディスク容量は、少なくとも、すべての管理対象 DNS（メイン）のプライマリクラスタにおけるディスクサイズの合計である必要があります。
- 大規模な DNS 展開では、保護されていない RR の複製を無効にする必要があります (*poll-replica-rrs*)。

小規模な展開

- 1 ～ 1000 の RR と 1 ～ 100 のゾーン。
- 主に静的データ。ゾーンの編集は、主に管理者が行います。
- 通常、1つのプライマリサーバとセカンダリサーバで構成されます。
- DNS キャッシングサーバは不要であるか、ハイブリッドモードで処理できます。
- DNS は、実稼働環境にほとんど影響を与えずに、数分以内にシャドウバックアップから復旧できます。
- 2 CPU 以上
- 4 GB 以上の RAM
- 10 GB 以上のディスク容量

中規模な展開

- 1000 ～ 100,000 の RR および 100 ～ 1000 のゾーン。
- 静的データと動的データがかなり均等に混合しており、1秒あたり 100 回以下の更新が可能です。
- 通常、1つのプライマリと2つから4つのセカンダリで構成されます。
- 通常、2台から4台の DNS キャッシングサーバで構成されます。DNS キャッシングサーバは、別のマシンまたは VM に展開する必要があります。
- DNS は、実稼働環境への影響を最小限に抑えながら、1時間以内にシャドウバックアップから復旧できます。
- 4 CPU 以上
- 8 GB 以上の RAM
- 25 GB 以上のディスク容量。プライマリでは、変更セットの保持数 (*csetdb-htrim-max-cset-kept*) を増やす必要があります。この値は、システムで処理される DNS の更新回数によって異なりますが、1000 ～ 5000 の範囲で指定する必要があります。

大規模な展開

- 100,000 ～ 25,000,000 の RR と 1000 ～ 10,000 のゾーン
- 動的データは、データの大部分を占め、1 秒間に数千回の更新が行われます。
- 通常、2 つのプライマリ (DNS HA ペア) と 4 つのセカンダリで構成されます。
- 通常、4 台以上の DNS キャッシングサーバで構成されます。
- DNS リカバリは複雑で、メンテナンス期間中に行う必要があります。DNS サーバは、シャドウバックアップからの復旧に 1 時間以上かかることがあります。
- 8 CPU 以上
- 16 GB 以上の RAM。DNS RR キャッシュメモリのサイズ (*mem-cache-size*) を増やす必要があります (RR あたり約 300 バイト、ただし 2,000,000 KB を超えないようにする)。
- 100 GB 以上のディスク容量。プライマリでは、変更セットの保持数 (*csetdb-htrim-max-cset-kept*) を増やす必要があります。この値は、システムで処理される DNS の更新回数によって異なりますが、5000 ～ 10,000 の範囲で指定する必要があります。

