テスト検索にnslookupを使用する（DNSサフィックス）

内容

はじめに

このドキュメントでは、nslookupをテスト検索に使用する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

nslookupを使用したDNSクエリ応答の確認は、DNSの問題のトラブルシューティングによく使用されます。一部のシナリオでは、クエリがドメインの追加レベルを返すように見えることがあります。たとえば、sub.domain.comを検索すると、sub.domain.com.domain.comに対するクエリと応答が生成されます。

nslookup：解決アルゴリズムの違い

DNSのクエリーを実行する場合、現在のすべてのオペレーティング・システムで1つのユーティリティであるnslookupを使用できます。古く、digよりも機能が劣りますが、Windowsユーザはデフォルトでnslookupに制限されています。nslookupでは、digやローカルシステムとは異なる方法でDNSが処理されることに注意してください。

パブリックワイルドカードを使用しないパブリッククエリの場合

nslookup:

1. domain.com (nslookup domain.com)に対するクエリ。

2. nslookupは「domain.com.suffix」を送信し、応答(NXDOMAIN)を確認します。

3. nslookupは「domain.com.secondsuffix」を送信し、応答(NXDOMAIN)を確認します。

4. nslookupは「domain.com」を送信し、応答を返します。

システムDNSまたはDig

1. domain.comに対して行われたクエリ(domain.comを参照)。

2. digまたはシステムがDNSパケットルックアップを「domain.com」まで送信し、応答を返す

3. 以前の情報が存在しない場合は、「domain.com.suffix」のDNSパケットを生成できます

4. 以前の情報が存在しない場合、「domain.com.secondsuffix」に対してDNSパケットを生成できます。

ローカル応答がなく、パブリック応答のみが存在するシナリオでは、これは全く同じ動作をします。以前のシナリオの唯一の違いは、パケットがキャプチャされた場合、nslookupのシナリオでは追加されたクエリに奇妙な見た目のサフィックスを送信する可能性があることです。

DNSサフィックスにパブリックワイルドカードが含まれるパブリッククエリの場合

nslookup:

1. domain.comに対するクエリ(nslookup domain.com)

2. nslookupは「domain.com.suffix」を送信し、応答を確認します。応答が返されます（サフィックスはパブリックワイルドカードドメインです）。 domain.com.suffixに対する回答が見つかったため、それ以上のクエリは行われません。

システムDNSまたはDig

1. domain.comに対して行われたクエリ(domain.comを参照)。

2. digまたはシステムがDNSパケットルックアップを「domain.com」まで送信し、domain.comの応答を返す。

その結果、nslookupは、コンピュータのWebブラウザを使用するユーザとはまったく異なるDNS応答を返し、誤ったDNS応答が認識される可能性があります。また、問い合わせされたDNSレコードがコンピュータのサフィックスリストと一致する場合、ドメインが「二重」に見えることもあります。

パブリックワイルドカードDNS検索サフィックスドメインにnslookupを使用するための有効なソリューション

DNSのクエリーを実行する場合は、nslookupを使用してホスト名をクエリーする場合を除き、クエリーの最後に「。」を適用します。これにより、要求されたクエリを正確に検索できます。「nslookup domain.com.」は、最初にサフィックスなしでdomain.comのみを要求できます。

Umbrellaレポートでの表示

特定のシナリオでは、この動作はUmbrellaレポートで確認できます。この処理が実行されると、「facebook.com.domain.local」や「google.com.domain.local」などのエントリが表示されます。ほとんどの場合、これはnslookupが最初にこれらのローカル問い合わせを実行することです。サフィックスがDNSゾーンで権限を持たない場合は、ネットワーク上のローカルDNSサーバからNXDOMAINに返されるのではなく、Umbrellaに転送できます。

特殊なケース：Umbrellaローミングクライアント

適用したDNS検索サフィックスドメインがパブリックワイルドカードであり、内部でも使用されている場合は、前述したサフィックスを2倍にした動作も確認できます。host.domain.comに対するクエリは、レポートではhost.domain.com.domain.comとして表示できます（内部ドメインリストには含まれません）。 domain.comがパブリックワイルドカードの場合は、「domain.com.domain.com」を内部ドメインリストに追加して、ユーザに見られる影響を解決します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。