Usar nslookup para Pesquisas de Teste (Sufixos DNS)

Contents

Introdução

Este documento descreve como usar o nslookup para pesquisas de teste.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

O uso do nslookup para verificar respostas de consultas DNS é comumente usado na solução de problemas de DNS. Em alguns cenários, as consultas podem parecer retornar um nível extra de um domínio. Por exemplo, pesquisar sub.domain.com resulta em uma consulta e uma resposta para sub.domain.com.domain.com.

nslookup: Diferenças do Algoritmo de Resolução

Ao consultar o DNS, um utilitário é onipresente em todos os sistemas operacionais modernos: nslookup. Embora mais antigos e menos capazes do que o dig, os usuários do Windows são limitados por padrão ao nslookup. É importante observar que o nslookup trata o DNS de forma diferente do dig ou do sistema local.

Para uma Consulta Pública sem Caracteres Curinga Públicos

nslookup:

1. Consulta feita para domain.com (nslookup domain.com).

2. nslookup envia "domain.com.suffix" e verifica se há uma resposta - NXDOMAIN.

3. nslookup envia "domain.com.secondsuffix" e verifica se há uma resposta - NXDOMAIN.

4. nslookup envia "domain.com" e retorna a resposta.

DNS ou Dig do sistema

1. Consulta feita para domain.com (dig domain.com).

2. dig ou o sistema envia uma pesquisa de pacote DNS "domain.com" e retorna a resposta

3. Se as informações anteriores não existirem, um pacote DNS poderá ser gerado para "domain.com.suffix"

4. Se as informações anteriores não existirem, um pacote DNS poderá ser gerado para "domain.com.secondsuffix"

Em um cenário em que não há resposta local e existe apenas uma resposta pública, isso age exatamente da mesma forma. A única diferença no cenário anterior é que, se os pacotes forem capturados, o cenário nslookup poderá estar enviando consultas anexadas a sufixos estranhos.

Para uma consulta pública em que um sufixo DNS tem um curinga público

nslookup:

1. Consulta feita para domain.com (nslookup domain.com)

2. o nslookup envia "domain.com.suffix" e verifica se há uma resposta. A resposta é retornada (o sufixo é um domínio curinga público). Uma resposta foi encontrada para domain.com.suffix, nenhuma outra consulta foi feita.

DNS ou Dig do sistema

1. Consulta feita para domain.com (dig domain.com).

2. dig ou o sistema envia uma pesquisa de pacote DNS "domain.com" e retorna a resposta para domain.com.

Como resultado, o nslookup pode retornar uma resposta DNS completamente diferente dos usuários que utilizam o navegador da Web de um computador e pode levar a respostas DNS incorretas percebidas. Isso também pode levar a aparências "duplas" de domínios se o registro DNS consultado corresponder à lista de sufixos do computador.

Solução em funcionamento para usar o nslookup para o domínio de sufixo de pesquisa DNS curinga público

Ao consultar DNS, aplique um "." no final da consulta, a menos que esteja usando nslookup para consultar um nome de host. Isso pode pesquisar a consulta exata solicitada. "nslookup domain.com." primeiro é possível solicitar somente domain.com sem sufixos.

Aparência no relatório do Umbrella

Em determinados cenários, esse comportamento pode ser observado em relatórios do Umbrella. As entradas podem ser exibidas como "facebook.com.domain.local" ou "google.com.domain.local" quando isso estiver ocorrendo. Na maioria dos casos, esse é o nslookup executando essas consultas locais primeiro. Se seus sufixos não forem autoritativos na zona DNS, eles poderão ser encaminhados para o Umbrella em vez de serem retornados NXDOMAIN pelo servidor DNS local na rede.

Caso especial: Cliente de roaming Umbrella

Se o domínio de sufixo de pesquisa DNS aplicado for um curinga público e também for usado internamente, você também poderá observar o comportamento do sufixo duplicado observado anteriormente. As consultas de host.domain.com podem aparecer como host.domain.com.domain.com em seus relatórios (apesar de estarem na lista de domínios internos). Se domain.com for um curinga público, adicione "domain.com.domain.com" à sua lista de domínios internos para resolver qualquer impacto de usuário observado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.