Usar nslookup para búsquedas de pruebas (sufijos DNS)

Contenido

Introducción

Este documento describe cómo utilizar nslookup para las búsquedas de prueba.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

El uso de nslookup para verificar las respuestas de consulta DNS se usa comúnmente en la resolución de problemas de DNS. En algunos escenarios, puede parecer que las consultas devuelven un nivel adicional de un dominio. Por ejemplo, si busca sub.domain.com, obtendrá una consulta y una respuesta para sub.domain.com.domain.com.

nslookup: Diferencias de algoritmos de resolución

Al consultar DNS, una utilidad está presente en todos los sistemas operativos modernos: nslookup. Aunque son más antiguos y tienen menos capacidad que dig, los usuarios de Windows están limitados de forma predeterminada a nslookup. Es importante tener en cuenta que nslookup maneja DNS de manera diferente que dig o el sistema local.

Para una consulta pública sin comodín público

nslookup:

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

2. nslookup envía "domain.com.suffix" y verifica una respuesta: NXDOMAIN.

3. nslookup envía "domain.com.secondsuffix" y verifica una respuesta: NXDOMAIN.

4. nslookup envía "domain.com" y devuelve la respuesta.

DNS del sistema o Dig

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

2. dig o el sistema envía una búsqueda de paquetes DNS hasta "domain.com" y devuelve la respuesta

3. Si la información anterior no existe, se puede generar un paquete DNS para "domain.com.suffix"

4. Si la información anterior no existe, se puede generar un paquete DNS para "domain.com.secondsuffix"

En un escenario donde no hay respuesta local y solo existe una respuesta pública, esto actúa exactamente igual. La única diferencia en el escenario anterior es que si se capturan los paquetes, el escenario nslookup puede estar enviando consultas añadidas de sufijos de aspecto extraño.

Para una consulta pública donde un sufijo DNS tiene un comodín público

nslookup:

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

2. nslookup envía "domain.com.suffix" y busca una respuesta. Se devuelve una respuesta (el sufijo es un dominio comodín público). Se encuentra una respuesta para domain.com.suffix, no se realizan más consultas.

DNS del sistema o Dig

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

2. dig o el sistema envía una búsqueda de paquetes DNS hasta "domain.com" y devuelve la respuesta para domain.com.

Como resultado, nslookup puede devolver una respuesta DNS completamente diferente a la de los usuarios que utilizan el navegador web de un equipo y puede dar lugar a respuestas DNS incorrectas percibidas. Esto también puede dar lugar a apariciones "dobles" de dominios si el registro DNS consultado coincide con la lista de sufijos del equipo.

Solución de trabajo para utilizar nslookup para dominio de sufijo de búsqueda de DNS comodín público

Al consultar DNS, aplique un carácter "." al final de la consulta, a menos que se utilice nslookup para consultar un nombre de host. Esto puede buscar la consulta exacta solicitada. "nslookup domain.com." sólo puede solicitar domain.com sin sufijos primero.

Aparición en Umbrella Reporting

En determinados escenarios, este comportamiento puede observarse en los informes generales. Las entradas pueden aparecer como "facebook.com.domain.local" o "google.com.domain.local" cuando esto ocurra. En la mayoría de los casos, se trata de nslookup realizando primero esas consultas locales. Si los sufijos no son autoritativos en la zona DNS, se pueden reenviar a Umbrella en lugar de que el servidor DNS local de la red devuelva NXDOMAIN.

Caso especial: Cliente de roaming de Umbrella

Si el dominio de sufijos de búsqueda de DNS aplicado es un comodín público y también se utiliza internamente, también puede observar el comportamiento de sufijo duplicado mencionado anteriormente. Las consultas para host.domain.com pueden aparecer como host.domain.com.domain.com en sus informes (a pesar de estar en la lista de dominios internos). Si domain.com es un comodín público, agregue "domain.com.domain.com" a su lista de dominios internos para resolver cualquier impacto observado en el usuario.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).