Gebruik nslookup voor testopzoeken (DNS-achtervoegsels)

Inhoud

Inleiding

In dit document wordt beschreven hoe u nslookup kunt gebruiken voor het opzoeken van tests.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Het gebruik van nslookup om DNS-queryantwoorden te controleren wordt vaak gebruikt bij het oplossen van DNS-problemen. In sommige scenario's kunnen query's een extra niveau van een domein weergeven. Als u bijvoorbeeld sub.domain.com opzoekt, krijgt u een vraag en antwoord voor sub.domain.com.domain.com.

nslookup: verschillen in resolutiealgoritme

Bij het bevragen van DNS is één hulpprogramma alomtegenwoordig in alle moderne besturingssystemen: nslookup. Hoewel ouder en minder geschikt dan graven, zijn Windows-gebruikers standaard beperkt tot nslookup. Het is belangrijk op te merken dat nslookup DNS anders behandelt dan graven of het lokale systeem.

Voor een openbare zoekopdracht zonder openbare wildcard

nslookup:

1. Query gemaakt voor domain.com (nslookup domain.com).

2. nslookup verzendt "domain.com.suffix" en controleert op een reactie - NXDOMAIN.

3. nslookup verzendt "domain.com.secondsuffix" en controleert op een reactie - NXDOMAIN.

4. nslookup verzendt "domain.com" en geeft het antwoord terug.

System DNS of Dig

1. Query gemaakt voor domain.com (dig domain.com).

2. dig of het systeem verzendt een DNS-pakketopzoeking "domain.com" en geeft het antwoord terug

3. Als de eerdere informatie niet bestaat, kan een DNS-pakket worden gegenereerd voor "domain.com.suffix"

4. Als de eerdere informatie niet bestaat, kan een DNS-pakket worden gegenereerd voor "domain.com.secondsuffix"

In een scenario waarin er geen lokaal antwoord is en alleen een publiek antwoord bestaat, werkt dit precies hetzelfde. Het enige verschil in het eerdere scenario is dat als pakketten worden vastgelegd, het nslookup-scenario vreemd uitziende achtervoegsel met toegevoegde query's kan verzenden.

Voor een openbare zoekopdracht waarbij een DNS-achtervoegsel een openbare wildcard heeft

nslookup:

1. Zoekopdracht gemaakt voor domain.com (nslookup domain.com)

2. nslookup verzendt "domain.com.suffix" en controleert op een reactie. De respons wordt teruggegeven (suffix is een publiek wildcard domein). Er is een antwoord gevonden voor domain.com.suffix, er worden geen verdere vragen gesteld.

System DNS of Dig

1. Query gemaakt voor domain.com (dig domain.com).

2. dig of het systeem verzendt een DNS-pakketopzoeking "domain.com" en geeft het antwoord voor domain.com.

Als gevolg hiervan kan nslookup een heel ander DNS-antwoord retourneren dan gebruikers die de webbrowser van een computer gebruiken en kan dit leiden tot waargenomen onjuiste DNS-reacties. Dit kan ook leiden tot "dubbele" verschijningsvormen van domeinen als het opgevraagde DNS-record overeenkomt met de suffix-lijst van de computer.

Werkende oplossing om nslookup te gebruiken voor Public Wildcard DNS Search Suffix Domain

Wanneer u DNS opvraagt, past u een "." toe aan het einde van de query, tenzij u nslookup gebruikt om een hostnaam op te vragen. Dit kan de exacte gevraagde zoekopdracht opzoeken. "nslookup domain.com." kan alleen domain.com aanvragen zonder voorvoegsels.

Verschijnen in Umbrella Reporting

In bepaalde scenario's kan dit gedrag waarneembaar zijn in overkoepelende rapporten. Inzendingen kunnen verschijnen zoals "facebook.com.domain.local" of "google.com.domain.local" wanneer dit zich voordoet. In de meeste gevallen is dit het eerst uitvoeren van die lokale zoekopdrachten. Als uw achtervoegsels niet gezaghebbend zijn in de DNS-zone, kunnen ze worden doorgestuurd naar Umbrella in plaats van te worden geretourneerd NXDOMAIN door de lokale DNS-server op het netwerk.

Speciaal geval: Umbrella Roaming Client

Als uw toegepaste DNS-zoekachtervoegseldomein een openbare joker is en ook intern wordt gebruikt, kunt u ook het eerder vermelde gedrag van het achtervoegsel verdubbelen observeren. Query's voor host.domain.com kunnen in uw rapporten worden weergegeven als host.domain.com.domain.com (ondanks dat ze in de lijst met interne domeinen staan). Als domain.com een openbare jokerkaart is, voegt u "domain.com.domain.com" toe aan uw lijst met interne domeinen om eventuele waargenomen gevolgen voor de gebruiker op te lossen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.