Utiliser nslookup pour les recherches de test (suffixes DNS)

Table des matières

Introduction

Ce document décrit comment utiliser nslookup pour les recherches de test.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

L'utilisation de la commande nslookup pour vérifier les réponses aux requêtes DNS est couramment utilisée pour résoudre les problèmes DNS. Dans certains scénarios, les requêtes peuvent sembler renvoyer un niveau supplémentaire d'un domaine. Par exemple, si vous recherchez sub.domain.com, vous obtenez une requête et une réponse pour sub.domain.com.domain.com.

nslookup : Différences des algorithmes de résolution

Lors de l'interrogation de DNS, un utilitaire est omniprésent dans tous les systèmes d'exploitation modernes : nslookup. Bien qu'ils soient plus anciens et moins performants que dig, les utilisateurs Windows sont limités par défaut à nslookup. Il est important de noter que nslookup gère le DNS différemment de dig ou du système local.

Pour une requête publique sans caractère générique public

nslookup :

1. Requête effectuée pour domain.com (nslookup domain.com).

2. nslookup envoie « domain.com.suffix » et recherche une réponse - NXDOMAIN.

3. nslookup envoie « domain.com.secondsuffix » et recherche une réponse - NXDOMAIN.

4. nslookup envoie « domain.com » et renvoie la réponse.

DNS système ou recherche

1. Requête effectuée pour domain.com (dig domain.com).

2. ou le système envoie une recherche de paquet DNS « domain.com » et renvoie la réponse

3. Si les informations précédentes sont inexistantes, un paquet DNS peut être généré pour « domain.com.suffix »

4. Si les informations précédentes sont inexistantes, un paquet DNS peut être généré pour « domain.com.secondsuffix »

Dans un scénario où il n'y a pas de réponse locale et où il n'existe qu'une réponse publique, cela agit exactement de la même manière. La seule différence dans le scénario précédent est que si des paquets sont capturés, le scénario nslookup peut envoyer des requêtes avec un suffixe étrange.

Pour une requête publique dans laquelle un suffixe DNS possède un caractère générique public

nslookup :

1. Requête effectuée pour domain.com (nslookup domain.com)

2. nslookup envoie « domain.com.suffix » et recherche une réponse. Réponse renvoyée (le suffixe est un domaine générique public). Une réponse est trouvée pour domain.com.suffix, aucune autre requête n'est faite.

DNS système ou recherche

1. Requête effectuée pour domain.com (dig domain.com).

2. ou le système envoie une recherche de paquet DNS « domain.com » et retourne la réponse

pour domain.com.

Par conséquent, nslookup peut renvoyer une réponse DNS complètement différente de celle des utilisateurs utilisant le navigateur Web d'un ordinateur et peut entraîner des réponses DNS incorrectes perçues. Cela peut également entraîner une « double » apparition des domaines si l'enregistrement DNS demandé correspond à la liste de suffixes de l'ordinateur.

Solution de travail pour utiliser nslookup pour le domaine de suffixe de recherche DNS générique public

Lors de l'interrogation du DNS, appliquez un "." à la fin de la requête, sauf si vous utilisez nslookup pour interroger un nom d'hôte. Cela permet de rechercher la requête exacte demandée. "nslookup domain.com." ne peut demander que domain.com sans suffixe au préalable.

Apparition dans Umbrella Reporting

Dans certains scénarios, ce comportement peut être observé dans les rapports Umbrella. Les entrées peuvent apparaître, par exemple « facebook.com.domain.local » ou « google.com.domain.local ». Dans la plupart des cas, il s'agit de nslookup qui exécute d'abord ces requêtes locales. Si vos suffixes ne font pas autorité sur la zone DNS, ils peuvent être transférés à Umbrella plutôt que d'être retournés à NXDOMAIN par le serveur DNS local sur le réseau.

Cas particulier : Client d'itinérance Umbrella

Si votre domaine de suffixe de recherche DNS appliqué est un masque générique public et est également utilisé en interne, vous pouvez également observer le comportement de doublure de suffixe noté précédemment. Les requêtes pour host.domain.com peuvent apparaître sous la forme host.domain.com.domain.com dans vos rapports (bien qu'elles figurent dans la liste des domaines internes). Si domain.com est un masque générique public, ajoutez « domain.com.domain.com » à votre liste de domaines internes pour résoudre tout impact observé sur l'utilisateur.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.