# Usa nslookup per ricerche test (suffissi DNS)

## Sommario



## Introduzione

In questo documento viene descritto come utilizzare nslookup per le ricerche di test.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Panoramica

L'utilizzo di nslookup per controllare le risposte alle query DNS viene in genere utilizzato nella risoluzione dei problemi DNS. In alcuni scenari, le query possono restituire un livello aggiuntivo di un dominio. Ad esempio, se si cerca sub.domain.com si ottiene una query e una risposta per sub.domain.com.domain.com.

### nslookup: Differenze negli algoritmi di risoluzione

Quando si esegue una query su DNS, un'utilità è onnipresente in tutti i sistemi operativi moderni:

nslookup Sebbene gli utenti di Windows siano meno esperti di dig, per impostazione predefinita è limitato a nslookup. È importante notare che nslookup gestisce il DNS in modo diverso rispetto a dig o al sistema locale.

Per una query pubblica senza caratteri jolly pubblici

nslookup:

1. Query eseguita per domain.com (nslookup domain.com).

2. nslookup invia "domain.com.suffix" e verifica la presenza di una risposta - NXDOMAIN.

3. nslookup invia "domain.com.secondsuffix" e verifica la presenza di una risposta - NXDOMAIN.

4. nslookup invia "domain.com" e restituisce la risposta.

DNS o diagnostica di sistema

1. Query eseguita per domain.com (dig domain.com).

2. dig o il sistema invia un pacchetto DNS di ricerca in "domain.com" e restituisce la risposta

3. Se le informazioni precedenti non esistono, è possibile generare un pacchetto DNS per "domain.com.suffix"

4.  Se le informazioni precedenti non esistono, è possibile generare un pacchetto DNS per "domain.com.secondsuffix"

In uno scenario in cui non esiste una risposta locale ed esiste solo una risposta pubblica, questo agisce esattamente allo stesso modo. L'unica differenza nello scenario precedente è che, se i pacchetti vengono acquisiti, lo scenario nslookup può inviare query aggiunte con suffisso dall'aspetto strano.

Per una query pubblica in cui un suffisso DNS ha un carattere jolly pubblico

nslookup:

1. Query eseguita per domain.com (nslookup domain.com)

2. nslookup invia "domain.com.suffix" e verifica la presenza di una risposta. Viene restituita una risposta (il suffisso è un dominio pubblico con caratteri jolly). Trovata una risposta per domain.com.suffix, non vengono eseguite ulteriori query.

DNS o diagnostica di sistema

1. Query eseguita per domain.com (dig domain.com).

2. dig o il sistema invia un pacchetto DNS di ricerca in "domain.com" e restituisce la risposta per domain.com.

Di conseguenza, nslookup può restituire una risposta DNS completamente diversa rispetto agli utenti che utilizzano il browser Web di un computer e può portare a risposte DNS percepite come errate. Ciò può inoltre causare un "doppio" aspetto dei domini se il record DNS sottoposto a query corrisponde all'elenco di suffissi del computer.

## Soluzione di lavoro per l'utilizzo di nslookup per il dominio del suffisso di ricerca DNS pubblico con caratteri jolly

Quando si esegue una query su DNS, applicare un "." alla fine della query, a meno che non si utilizzi nslookup per eseguire una query su un nome host. È possibile cercare la query esatta richiesta. "nslookup domain.com." è possibile richiedere solo domain.com senza prima suffissi.

## Comparsa in Umbrella Reporting

In alcuni scenari, questo comportamento può essere osservato nei report Umbrella. In questo caso, è possibile che vengano visualizzate voci quali "facebook.com.domain.local" o "google.com.domain.local". Nella maggior parte dei casi, si tratta di nslookup che esegue prima queste query locali. Se i suffissi non sono autorevoli nella zona DNS, possono essere inoltrati a Umbrella anziché essere restituiti a NXDOMAIN dal server DNS locale in rete.

## Caso speciale: Umbrella Roaming Client

Se il dominio del suffisso di ricerca DNS applicato è un carattere jolly pubblico e viene utilizzato anche internamente, è inoltre possibile osservare il comportamento del suffisso raddoppiato descritto in precedenza. Le query per host.domain.com possono essere visualizzate come host.domain.com.domain.com nei report, nonostante siano presenti nell'elenco dei domini interni. Se domain.com è un carattere jolly pubblico, aggiungere "domain.com.domain.com" all'elenco dei domini interni per risolvere l'impatto osservato sugli utenti.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).