

# Comment créer une entrée DNS ponctuelle

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Aperçu ponctuel de DN](#)

[Configurez](#)

[Créez les enregistrements SRV de DN](#)

[Configurez le serveur DNS de Windows](#)

[Configurez le serveur DNS de GRIPPAGE](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment créer les entrées ponctuelles pour les états de service (SRV) sur le Serveur de noms interne (NS) afin de fonctionner autour du manque d'installations fendues de Système de noms de domaine (DNS).

Contribué par Zoltan Kelemen, édité par Joshua Alero et Lidiya Bogdanova, ingénieurs TAC Cisco.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base des DN
- Un domaine qui est correctement configuré sur le NS bien fondé public

### [Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows Server 2012
- Communication vidéo système) (VCS/autoroute

Remarque: Les informations dans ce document peuvent être utilisées avec le serveur DNS

de Microsoft, ou le GRIPPAGE. Vous devez seulement utiliser les étapes appropriées pour votre serveur DNS particulier. Des instructions pour d'autres types de serveurs DNS ne sont pas fournies, mais le concept peut être utilisé avec n'importe quel autre serveur DNS si le serveur prend en charge cette configuration.

Remarque: Le NS interne est utilisé par les utilisateurs internes, aussi bien que le système de communication vidéo (VCS)/autoroute-C de Cisco.

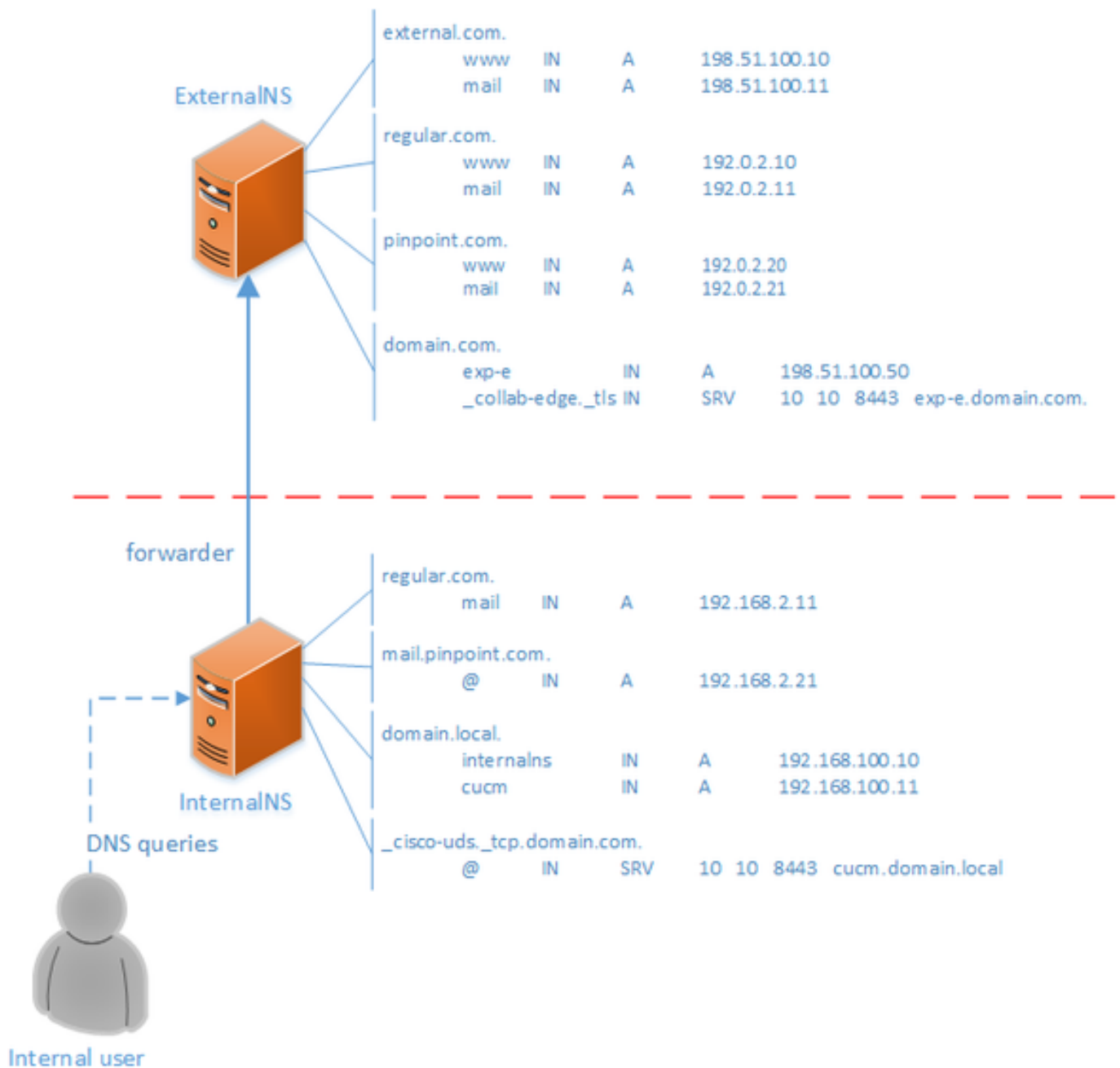
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

## Aperçu ponctuel de DN

L'entrée DNS ponctuelle est une zone créée pour un seul hôte seulement. Cette entrée peut être définie en tant que bien fondé sur un Serveur de noms, qui n'est pas bien fondé pour le domaine de parent. Ceci permet d'autres requêtes DNS pour que ce domaine soit expédié au bien fondé divisent.

La zone ponctuelle contient habituellement un enregistrement simple sans compter que le début exigé des enregistrements de l'autorité (SOA) et du Serveur de noms. Cet enregistrement est une autoréférence, identique au nom de la zone et apparaît en tant que **mêmes que le dossier parent** dans des **DN de Microsoft**, ou est mentionné par **@ un** symbole dans le fichier de **zone de GRIPPAGE**. L'enregistrement peut être de n'importe quel type pris en charge par les DN. **@ le** symbole est également utilisé dans des outils de l'interface de ligne de commande Windows (CLI), et fonctionne la même manière que dans le GRIPPAGE.

L'image suivante fournit un exemple de ces enregistrements :



C'est une caractéristique du système DNS et ne se fonde pas sur n'importe quel mécanisme dans le Cisco Jabber ou les applications d'autoroute de Cisco. C'est également une solution prise en charge pour le déploiement de Cisco Jabber si les DN séparés n'est pas disponible.

Si un Serveur de noms est configuré en tant que bien fondé ou principal pour un domaine, alors des requêtes ne sont pas expédiées pour des noms dans ce domaine à ses expéditeurs, même si il peut ne pouvoir pas résoudre un nom spécifique. Ainsi, afin de fournir la résolution de noms différente dans le même domaine à interne et aux utilisateurs externes du domaine normalement, des DN fendus seraient utilisés. En configuration DNS fendue, un serveur DNS interne met à jour une copie de la zone avec des entrées d'interne-particularité et un serveur DNS externe met à jour une copie de la zone avec des entrées d'externe-particularité. Les entrées actuelles dans la zone externe, mais pas dans la zone interne doivent pour les résoudre pour des requêtes internes.

Puisque ceci peut mener au temps système de Gestion, quelques administrateurs réseau préfèrent éviter des configurations DNS fendues. Les entrées DNS ponctuelles offrent une alternative dans des ces cas.

# Configurez

## Créez les enregistrements SRV de DN

Pour l'approvisionnement automatique de Cisco Jabber, aussi bien que le service de mobile et d'Accès à distance (MRA), deux enregistrements SRV sont impliqués pour chaque domaine (utilisant **domain.com** comme exemple) :

- **\_collab-edge.\_tls.domain.com**
- **\_cisco-uds.\_tcp.domain.com**

Vous pouvez avoir des plusieurs entrées pour ces enregistrements si l'autoroute et/ou le Cisco Unified Communications Manager (CUCM) est groupée.

Quand le fichier authoritative de zone pour **domain.com** existe seulement sur le NS externe, une entrée DNS ponctuelle pour le **\_tcp de \_cisco-uds.** est exigée sur le NS interne. D'abord la zone DNS ponctuelle doit être créée, puis le SRV dans la zone.

L'enregistrement SRV de **\_tcp de \_cisco-uds.** doit être seulement résoluble sur le réseau interne, pas de l'externe, et doit le résoudre au nom de domaine complet (FQDN) des noeuds CUCM avec les services de données d'utilisateur (UDS).

L'enregistrement SRV de **\_tls de \_collab-edge.** doit être résoluble du réseau externe, et des résolutions au nom de domaine complet (FQDN) du serveur d'autoroute-e.

## Configurez le serveur DNS de Windows

L'entrée DNS ponctuelle est créée pendant que n'importe quelle autre zone, et son nom doivent contenir le nom entier SRV (par exemple, **\_cisco-uds.\_tcp.domain.com**). Cette étape peut être aussi bien exécutée par l'interface utilisateur graphique (GUI), bien que l'exemple ci-dessous suppose que l'entrée DNS ponctuelle n'a pas été déjà créée.

Afin d'ajouter l'enregistrement SRV lui-même, un outil CLI doit être utilisé. Vous ne devez pas ajouter un enregistrement SRV à une entrée DNS ponctuelle par le GUI, car ceci ne fonctionne pas. Une fois ajouté par l'intermédiaire du CLI, ces enregistrements SRV sont maniables avec les outils réguliers juste comme n'importe quelle autre entrée. Windows CLI présente deux méthodes - **dnscmd** ou commandes de **PowerShell**. Chacun des deux exemples qui suivent créent les deux entrées DNS ponctuelles et ajoutent un enregistrement SRV pour le **\_tcp de \_cisco-uds.**

Seulement un de ces deux méthodes à la fois peut être utilisé :

- exemple 1 - utilisant le **dnscmd**

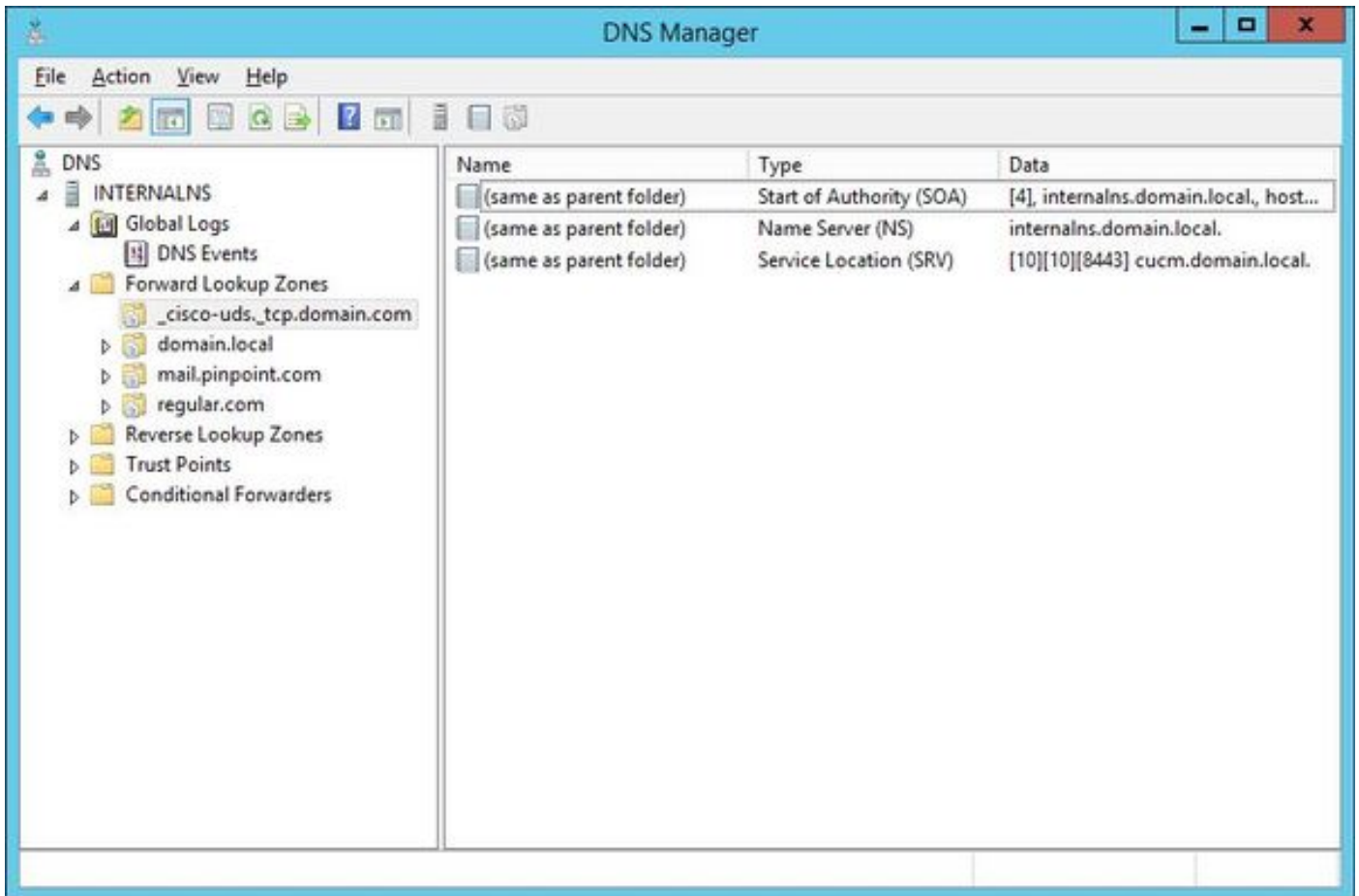
```
dnscmd . /zoneadd _cisco-uds._tcp.domain.com. /dsprimary
dnscmd . /recordadd _cisco-uds._tcp.domain.com. "@" SRV 10 10 8443 cucm.domain.local
```

- exemple 2 - utilisant des commandes de **PowerShell** (car le **dnscmd** doit être désapprouvé dans les versions futures de la Microsoft Windows Server, **PowerShell** peut être utilisé pour le

même but). Les options de **portée de réplication** sont **domaine**, **forêt**, ou vous pouvez installer un fichier avec - le paramètre de **ZoneFile**, si la zone n'est pas Répertoire actif (AD) intégré

```
Import-Module DnsServer
Add-DnsServerPrimaryZone -Name "_cisco-uds._tcp.domain.com" -ReplicationScope "Domain"
Add-DnsServerResourceRecord -Srv -ZoneName "_cisco-uds._tcp.domain.com" -Name "@" -Priority 10 -
Weight 10 -Port 8443 -DomainName "cucm.domain.local"
```

L'image suivante fournit un exemple de la façon dont l'entrée DNS ponctuelle avec l'enregistrement SRV ressemble à dans le GUI :



## Configurez le serveur DNS de GRIPPAGE

Avec le serveur DNS de GRIPPAGE, l'entrée DNS ponctuelle est créée la même manière comme fichier régulier de zone.

L'entrée **\$ORIGIN** doit indiquer le FQDN de l'enregistrement SRV (par exemple, **\_cisco-uds.\_tcp.domain.com**) et des enregistrements SOA et NS sont ajoutés comme d'habitude. Le SRV est facultatif (si l'entrée DNS ponctuelle définit ou ignore l'enregistrement SRV) et le nom utilisé est **@** qui est équivalent au nom/à ORIGINE de la zone.

Voici un exemple d'un contenu du fichier **Ne de \_cisco-uds.\_tcp.domain.com.zo** :

```
$TTL 1h
$ORIGIN _cisco-uds._tcp.domain.com.
@      IN      SOA      internalns.domain.local. hostmaster.domain.local. (
                2016033000;
                12h;
```

```
        15m;  
        3w;  
        3h;  
    )  
    IN      NS      internalns.domain.local.  
@      IN      SRV    10 10 8443 cucm.domain.local.
```

Voici un exemple de la façon dont toAdd la définition de zone à **named.conf** :

```
zone "_cisco-uds._tcp.domain.com" IN {  
    type master;  
    file "_cisco-uds._tcp.domain.com.zone";  
};
```

## Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- Utilisez le **nslookup** de commande avec le serveur réglé au NS interne, afin de vérifier les entrées DNS ponctuelles.

Voici un exemple de comment à l'adresse Internet de la consultation une du domaine de parent et de comment à la consultation l'enregistrement SRV a créé sur le NS interne :

```
C:\>nslookup exp-e.domain.com internalNS.domain.local
```

Non-authoritative answer:

```
Name: exp-e.domain.com Address: 198.51.100.50 C:\>nslookup -type=srv _cisco-uds._tcp.domain.com  
internalNS.domain.local _cisco-uds._tcp.domain.com SRV service location: priority = 10 weight =  
10 port = 8443 svr hostname = cucm.domain.local cucm.domain.local internet address =  
192.168.100.11
```

Voici un exemple de la façon à l'adresse Internet de la consultation une qui n'est pas configurée sur le NS interne, afin de vérifier que les demandes sont expédiées comme prévues.

```
C:\>nslookup www.example.com internalNS.domain.local
```

Non-authoritative answer:

```
Name: www.example.com  
Addresses: 203.0.113.42
```

- Placez le serveur à un public NS, ou au NS externe, et répétez les mêmes étapes. La consultation SRV pour l'enregistrement SRV de **\_tcp** de **\_cisco-uds.** échoue.

## Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si la vérification de **nslookup** renvoie une adresse Internet avec les pièces en double (par exemple, **cucm.domain.local.domain.local**), alors les entrées DNS doivent être vérifiées pour être terminées par un signe de point, autrement l'origine de la zone serait ajoutée à l'adresse Internet résolue.

S'il y a des soucis avec les entrées créées, ils peuvent être simplement supprimés du serveur DNS. Bien que le CLI soit exigé pour ajouter les entrées aux DN de Microsoft, des entrées peuvent supprimer sans risque et simplement dans le GUI.

## Informations connexes

Pour un déploiement de multi-domaine (différents noms de domaine internes et externes) de MRA consultez ce document :

[Exemple de configuration : Mobile et Accès à distance par Expressway/VCS dans un déploiement de multi-domaine](#)