# Comment créer une entrée DNS Pinpoint

## Contenu



## Introduction

Ce document décrit comment créer des entrées de point d'identification pour les enregistrements de service (SRV) sur le serveur de noms interne (NS) afin de contourner l'absence de configuration DNS (Domain Name System) divisé.

Contribué par Zoltan Kelemen, sous la direction de Joshua Alero et Lidiya Bogdanova, ingénieurs du centre d'assistance technique de Cisco.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du DNS
- Domaine correctement configuré sur le NS faisant autorité publique

### Components Used

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

- Microsoft Windows Server 2012
- Système de communication vidéo (VCS) / Expressway

**Note**: Les informations de ce document peuvent être utilisées avec le serveur DNS Microsoft

ou BIND. Vous devez uniquement utiliser les étapes appropriées pour votre serveur DNS particulier. Les 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.

**Note**: Le NS interne est utilisé par les utilisateurs internes, ainsi que par le système de communication vidéo (VCS) / Cisco Expressway-C.

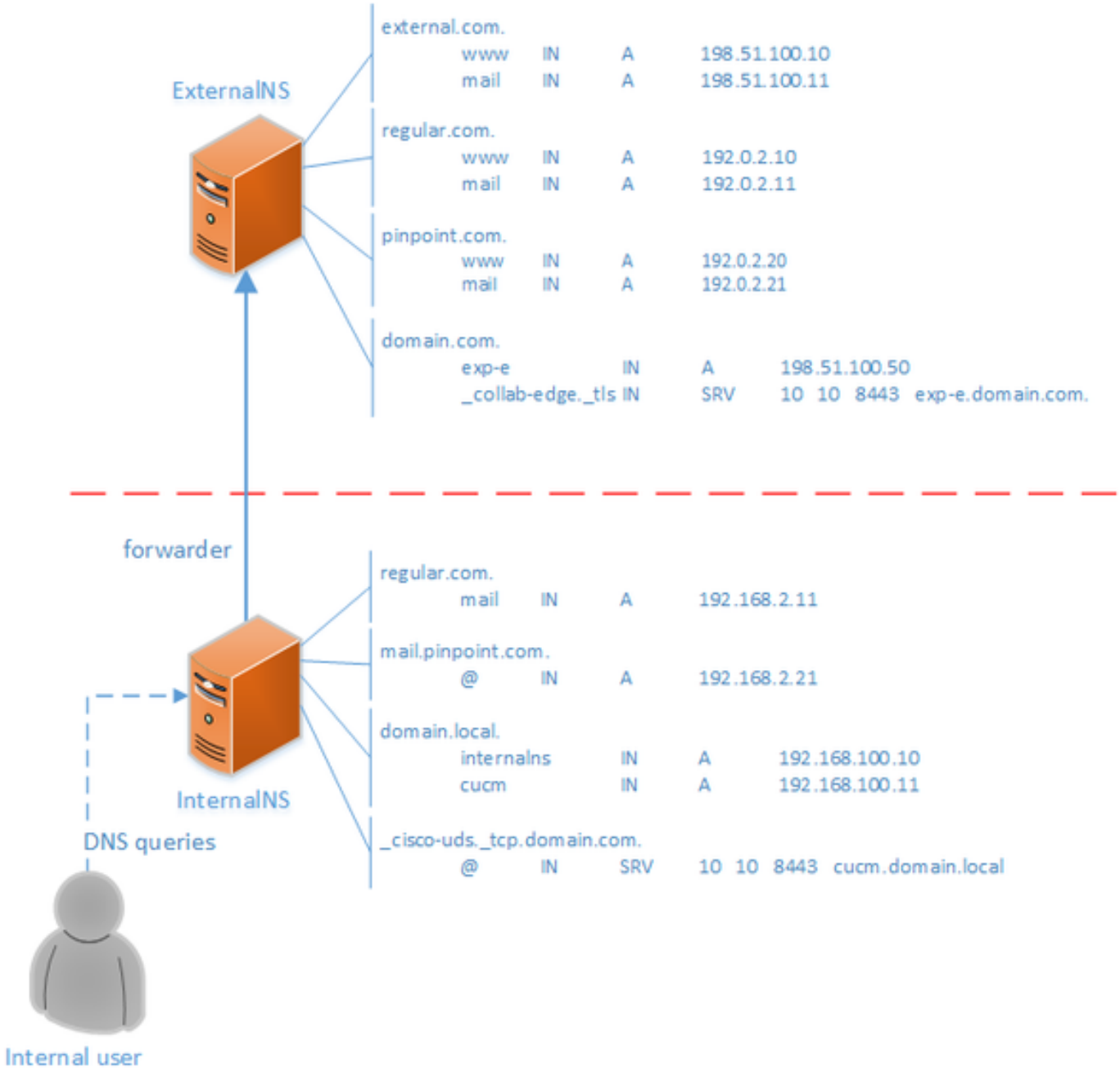
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

# Vue d'ensemble du DNS

L'entrée DNS du point d'identification est une zone créée pour un hôte unique uniquement. Cette entrée peut être définie comme faisant autorité sur un serveur de noms, qui n'est pas autorisé pour le domaine parent. Cela permet aux autres requêtes DNS de ce domaine d'être transmises au serveur faisant autorité.

La zone de point d'identification contient généralement un seul enregistrement en plus des enregistrements de début d'autorité (SOA) et de serveur de noms requis. Cet enregistrement est une auto-référence, identique au nom de la zone et s'affiche comme **le dossier parent** dans **Microsoft DNS**, ou est référencé par un **@** symbole dans le fichier de la **zone BIND**. L'enregistrement peut être de n'importe quel type pris en charge par le DNS. Le symbole **@** est également utilisé dans les outils de l'interface de ligne de commande (CLI) de Windows et fonctionne de la même manière que dans BIND.

L'image suivante fournit un exemple de ces enregistrements :




Il s’agit d’une fonctionnalité du système DNS qui ne repose sur aucun mécanisme des applications Cisco Jabber ou Cisco Expressway. Il s'agit également d'une solution prise en charge pour le déploiement de Cisco Jabber si le DNS partagé n'est pas disponible.

Si un serveur de noms est configuré en tant qu'autorité ou maître pour un domaine, les requêtes ne sont pas transférées pour les noms de ce domaine à ses redirecteurs, même s'il peut être impossible de résoudre un nom spécifique. Ainsi, afin de fournir une résolution de noms différente dans le même domaine aux utilisateurs internes et externes du domaine normalement, un DNS partagé serait utilisé. Dans une configuration DNS fractionnée, un serveur DNS interne conserve une copie de la zone avec des entrées spécifiques internes et un serveur DNS externe conserve une copie de la zone avec des entrées spécifiques externes. Les entrées présentes dans la zone externe, mais non dans la zone interne, ne doivent pas être résolues pour les requêtes internes.

Comme cela peut entraîner une surcharge de gestion, certains administrateurs réseau préfèrent éviter les configurations DNS fractionnées. Les entrées DNS Pinpoint offrent une alternative dans ces cas.

# Configuration

## Créer des enregistrements SRV DNS

Pour le provisionnement automatique de Cisco Jabber, ainsi que le service d'accès mobile et distant (MRA), deux enregistrements SRV sont impliqués pour chaque domaine (en utilisant **domain.com** comme exemple) :

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

Vous pouvez avoir plusieurs entrées pour ces enregistrements si l'Expressway et/ou Cisco Unified Communications Manager (CUCM) sont en cluster.

Lorsque le fichier de zone faisant autorité pour **domain.com** n'existe que sur le NS externe, une entrée DNS de point d'identification pour **_cisco-uds._tcp** est requise sur le NS interne. Il faut d'abord créer la zone DNS du point de repère, puis la SRV au sein de la zone.

> L'enregistrement SRV **_cisco-uds._tcp** doit pouvoir être résolu uniquement sur le réseau interne, et non à partir de l'externe, et doit être résolu en nom de domaine complet (FQDN) du ou des noeuds CUCM avec les services de données utilisateur (UDS).
>
> L'enregistrement SRV **_collab-edge._tls** doit pouvoir être résolu à partir du réseau externe et résolu en nom de domaine complet (FQDN) du serveur Expressway-E.

## Configurer le serveur DNS Windows

L'entrée DNS du point d'identification est créée comme toute autre zone et son nom doit contenir le nom SRV entier (par exemple, **_cisco-uds._tcp.domain.com**). Cette étape peut également être effectuée via l'interface utilisateur graphique (GUI), bien que l'exemple ci-dessous présuppose que l'entrée DNS du point de repère n'a pas encore été créée.

Pour ajouter l'enregistrement SRV lui-même, un outil CLI doit être utilisé. Vous ne devez pas ajouter un enregistrement SRV à une entrée DNS de point d'identification via l'interface utilisateur graphique, car cela ne fonctionne pas. Une fois ajoutés via l'interface de ligne de commande, ces enregistrements SRV sont gérables à l'aide des outils habituels, comme n'importe quelle autre entrée. L'interface de ligne de commande de Windows présente deux méthodes : les commandes **dnscmd** ou **PowerShell**. Les deux exemples suivants créent les deux entrées DNS de point de repère et ajoutent un enregistrement SRV pour **_cisco-uds._tcp**

Seule une de ces deux méthodes à la fois peut être utilisée :

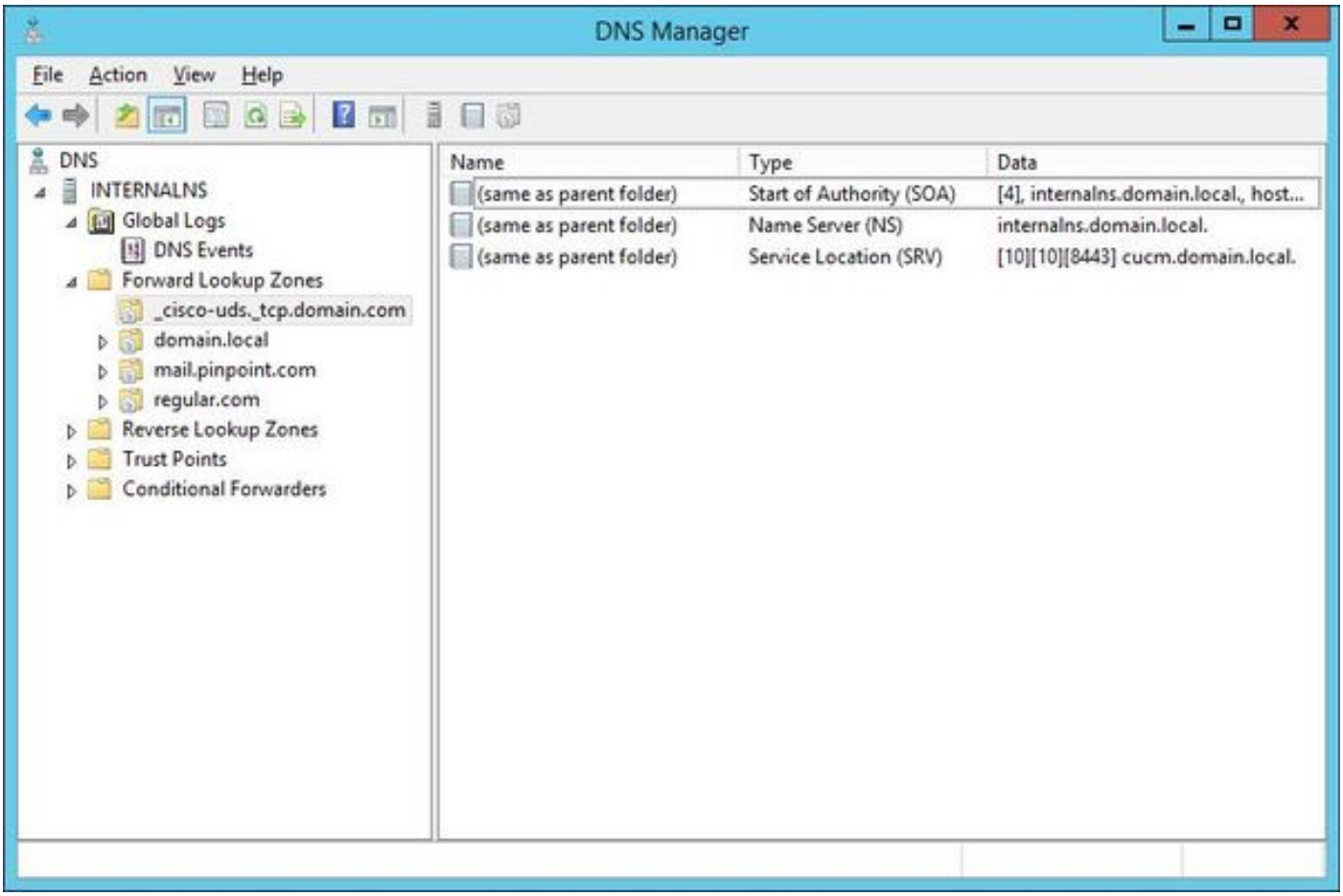
- exemple 1 - utilisation de **dnscmd**

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

- exemple 2 : utilisation des commandes **PowerShell** (comme **dnscmd** doit être déconseillé dans les versions futures de Microsoft Windows Server, **PowerShell** peut être utilisé dans le même but). **Les** options **d'étendue de réplication** sont **Domain**, **Forest** ou vous pouvez configurer un fichier avec le paramètre **-ZoneFile**, si la zone n'est pas intégrée à Active Directory (AD)

```
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 l'apparence de l'entrée DNS de point d'identification avec enregistrement SRV dans l'interface utilisateur graphique :




## Configurer le serveur DNS BIND

Avec le serveur DNS BIND, l'entrée DNS du point d'identification est créée de la même manière qu'un fichier de zone normal.

L'entrée **$ORIGIN** doit pointer sur le nom de domaine complet de l'enregistrement SRV (par exemple, **_cisco-uds._tcp.domain.com**) et les enregistrements SOA et NS sont ajoutés comme d'habitude. Le SRV est facultatif (que l'entrée DNS du point d'identification définit ou remplace l'enregistrement SRV) et le nom utilisé est **@**ce qui équivaut au nom / ORIGIN de la zone.

Voici un exemple de contenu de fichier **_cisco-uds._tcp.domain.com.zone** :

```
$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 **d'ajouter** la définition de zone à **name.conf** :

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

# Vérification

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

- Utilisez la commande **nslookup** avec le serveur défini sur le NS interne, afin de vérifier les entrées DNS de point d'identification.

Voici un exemple de la façon de rechercher un nom d'hôte à partir du domaine parent et de rechercher l'enregistrement SRV créé sur le NS interne :

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

Non-authorative 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 de rechercher un nom d'hôte qui n'est pas configuré sur le NS interne, afin de vérifier que les demandes sont transmises comme prévu.

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

Non-authoritative answer:
Name:    www.example.com
Addresses:  203.0.113.42
```

- Définissez le serveur sur un NS public ou sur le NS externe, puis répétez les mêmes étapes. La recherche SRV pour l'enregistrement **_cisco-uds._tcp SRV** échoue.

# Dépannage

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

Si la vérification **nslookup** renvoie un nom d'hôte avec des parties dupliquées (par exemple, **cucm.domain.local.domain.local**), les entrées DNS doivent être vérifiées pour être terminées par

un signe d'arrêt complet, sinon l'origine de la zone sera ajoutée au nom d'hôte résolu.

Si les entrées créées posent problème, elles peuvent être simplement supprimées du serveur DNS. Bien que l'interface de ligne de commande soit requise pour ajouter les entrées au DNS Microsoft, les entrées peuvent être supprimées en toute sécurité et simplement dans l'interface utilisateur graphique.

## Informations connexes

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

Exemple de configuration : Accès mobile et distant via Expressway/VCS dans un déploiement multidomaine