

Een Pinpoint-DNS-ingang maken

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[DNS-overzicht instellen](#)

[Configureren](#)

[DNS SRV-records maken](#)

[Windows DNS-server configureren](#)

[BIND-DNS-server configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u puntitems voor servicerecords (SRV) op de interne naamserver (NS) kunt maken om te werken bij het gebrek aan DNS-instellingen (split Domain Name System).

Bijgedragen door Zoltan Kelemen, bezorgd door Joshua Alero en Lidiya Bogdanova, Cisco TAC Engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van DNS
- Een domein dat correct is ingesteld op de openbare gezaghebbende NS

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows Server 2012
- Video Communication System (VCS)/Express

Opmerking: De informatie in dit document kan met Microsoft DNS-server of BIND worden gebruikt. U hoeft alleen de stappen te gebruiken die geschikt zijn voor uw specifieke DNS-server. Er worden geen instructies voor andere typen DNS-servers gegeven, maar het

concept kan met een andere DNS-server worden gebruikt als de server deze configuratie ondersteunt.

Opmerking: De interne NS wordt door interne gebruikers gebruikt, evenals Video Communication System (VCS) / Cisco Expressway-C.

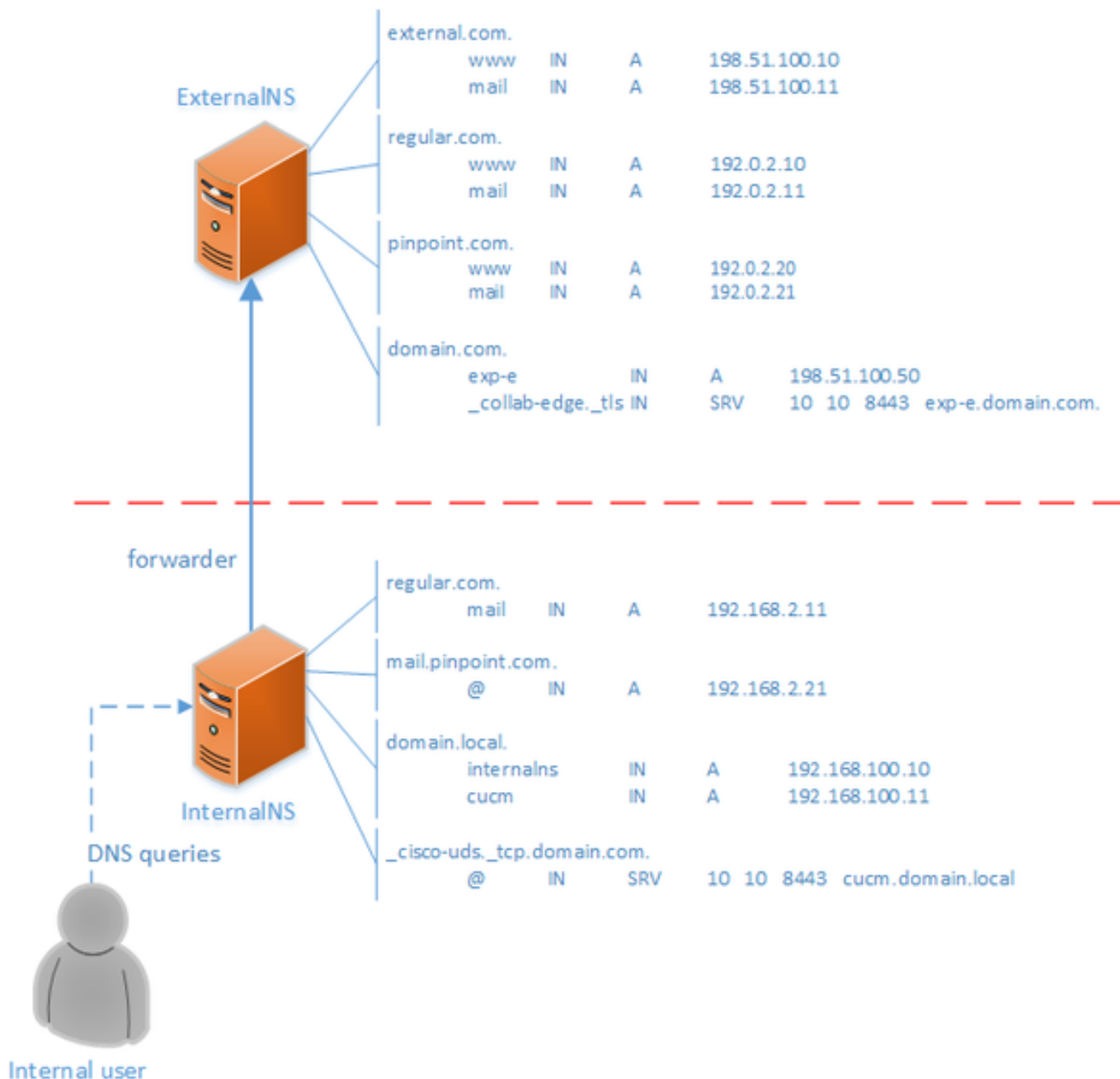
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

DNS-overzicht instellen

Het punt DNS-ingang is een zone die alleen voor één host wordt gecreëerd. Deze ingang kan als gezaghebbend op een Server van de Naam worden gedefinieerd, wat niet gezaghebbend voor het ouderdomein is. Hiermee kunnen andere DNS-vragen voor dit domein worden doorgestuurd naar de gezaghebbende server.

Het puntgebied bevat gewoonlijk één record naast de vereiste Start of Authority (SOA)- en Name Server records. Deze opname is een zelfverwijzing, identiek aan de naam van de zone en **hetzelfde** beeld **als oudermap** in **Microsoft DNS**, of wordt in het **BIND**-zone aangegeven door een **@**symbool. De record kan van elk type zijn dat door de DNS wordt ondersteund. Het **@** symbool wordt ook gebruikt in CLI-gereedschappen (Windows Opdracht Line Interface) en werkt op dezelfde manier als in BIND.

De volgende afbeelding geeft een voorbeeld van deze records:



Dit is een eigenschap van het DNS-systeem en is niet afhankelijk van een mechanisme in Cisco Jabber of Cisco Express-toepassingen. Het is ook een ondersteunde oplossing voor Cisco Jabber-implementatie als gesplitste DNS niet beschikbaar is.

Als een Name Server als gezaghebbend of master voor een domein is ingesteld, worden de vragen niet verzonden voor namen binnen dat domein aan zijn expediteurs, zelfs wanneer het niet in staat is om een specifieke naam op te lossen. Om binnen hetzelfde domein een andere naamresolutie aan interne en externe gebruikers van het domein normaal te kunnen geven, wordt dus een gesplitste DNS gebruikt. In een gesplitste DNS-configuratie behoudt een interne DNS-server een kopie van de zone met interne items en een externe DNS-server handhaaft een kopie van de zone met externe specifieke items. Verhalen die aanwezig zijn in de externe zone, maar niet in de interne zone moeten niet worden opgelost voor interne vragen.

Aangezien dit tot beheer over kop kan leiden, geven sommige netwerkbeheerders er de voorkeur aan gesplitste DNS-configuraties te vermijden. Pinpoint DNS-items bieden in deze gevallen een alternatief.

Configureren

DNS SRV-records maken

Voor Cisco Jabber: automatische provisioning, evenals mobiele en afstandsbediening (MRA), zijn twee SRV records betrokken voor elk domein (met gebruik van **domein.com** als voorbeeld):

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

U kunt meerdere items voor deze records hebben als de Expressway en/of Cisco Unified Communications Manager (CUCM) is geclusterd.

Wanneer het **authoratieve** zone bestand voor **domain.com** alleen bestaat op de externe NS, **moet** een DNS-ingang voor **_cisco-uds._tcp** op de interne NS zijn aangebracht. Eerst moet de DNS-zone worden ingesteld en daarna de SRV binnen de zone.

De record **_cisco-uds._tcp** SRV mag alleen worden opgelost op het interne netwerk en niet vanaf het externe netwerk, en moet worden opgelost in de volledig gekwalificeerde domeinnaam (FQDN) van het CUCM-knooppunt(en) met User Data Services (UDS).

Het **_collab-edge._tls** SRV record moet ontbinden zijn vanaf het externe netwerk en lost op tot de Full Qualified Domain Name (FQDN) van de Expressway-E server.

Windows DNS-server configureren

Het punt DNS ingang wordt gecreëerd zoals om het even welke andere zone, en zijn naam moet de volledige naam SRV bevatten (bijvoorbeeld, **_cisco-uds._tcp.domain.com**). Deze stap kan ook via de grafische gebruikersinterface (GUI) worden uitgevoerd, hoewel het onderstaande voorbeeld ervan uitgaat dat de DNS-ingang van het toppunt niet al is gemaakt.

Om de SRV-opname zelf toe te voegen, moet een CLI-gereedschap worden gebruikt. U moet geen SRV-record aan een DNS-ingang met het beginpunt via de GUI toevoegen, omdat dit niet werkt. Zodra toegevoegd via CLI, zijn deze SRV records hanteerbaar met de reguliere tools net zoals bij elke andere ingang. Windows CLI presenteert twee methoden - ofwel **dnscmd** of **PowerShell**-opdrachten. Beide voorbeelden die volgen, maken de twee DNS-posten in het hoofdpunt en voegen één SRV-record voor **_cisco-uds._tcp** toe

Er kan slechts één van deze twee methoden tegelijk worden gebruikt:

- voorbeeld 1 - gebruik van **dnscmd**

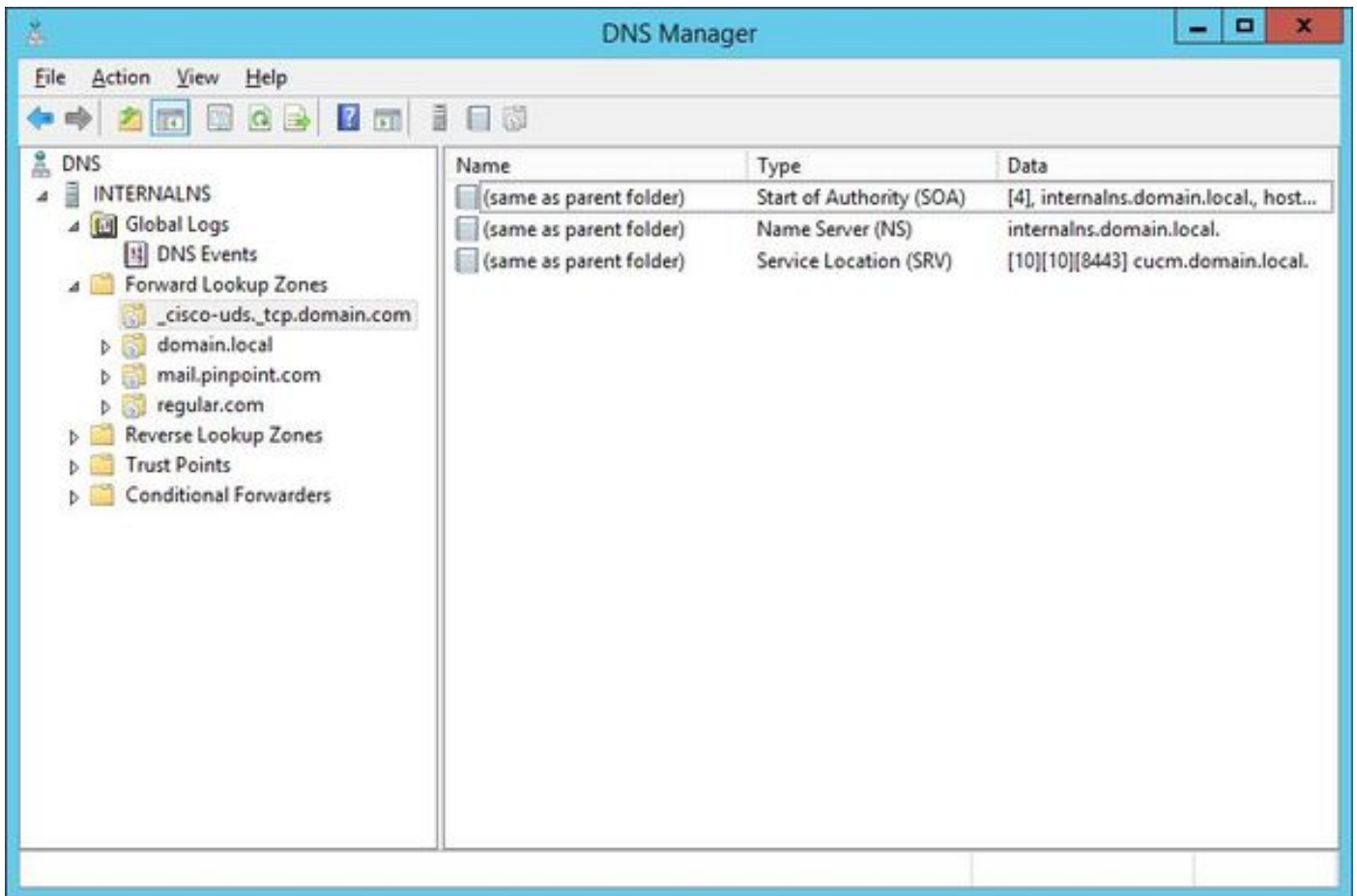
```
dnscmd . /zoneadd _cisco-uds._tcp.domain.com. /dsprimary
dnscmd . /recordadd _cisco-uds._tcp.domain.com. "@" SRV 10 10 8443 cucm.domain.local
```

- voorbeeld 2 - met opdrachten PowerShell (zoals **dnscmd** in toekomstige versies van Microsoft Windows Server moet worden afgebroken, kan PowerShell voor hetzelfde doel

gebruikt worden). De opties voor replicatiebereik zijn **Domain**, **Forest**, of u kunt een bestand instellen met de **-ZoneFile** parameter, als de zone niet actief is in Map (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"
```

Het volgende beeld geeft een voorbeeld van hoe het punt DNS-ingang met SRV-record er in de GUI uitziet:



BIND-DNS-server configureren

Met BIND DNS server wordt de DNS-ingang op het eerste punt op dezelfde manier gecreëerd als een regulier zone bestand.

De ingang van **\$ORIGIN** moet aan FQDN van het SRV record wijzen (bijvoorbeeld, **_cisco-uds._tcp.domein.com**) en de records van SOA en NS worden toegevoegd zoals gebruikelijk. De SRV is optioneel (of het punt-DNS-ingang de SRV-record definieert of overschrijdt) en de gebruikte naam is **@** wat gelijk is aan de naam/OORSPRONG van de zone.

Hier is een voorbeeld van een **_cisco-uds._tcp.domain.com.zo** bestandsinhoud:

```
$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.

```

Hier is een voorbeeld van hoe de zonedefinitie aan **name.conf toe te voegen**:

```

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

```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

- Gebruik de opdracht **nslookup** met een server die op de interne NS is ingesteld om de DNS-items te controleren.

Hier is een voorbeeld van hoe je één hostname uit het parent-domein kunt opzoeken in het SRV-record dat op de interne NS is gecreëerd:

```
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
```

Hier is een voorbeeld van hoe je één hostname op moet zoeken die niet is ingesteld in de interne NS, om te controleren of de verzoeken worden doorgestuurd zoals verwacht.

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

Non-authoritative answer:

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

- Stel een server in op een openbare NS of op de externe NS en herhaal dezelfde stappen. De SRV lookup for **_cisco-uds._tcp SRV** record faalt.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Als de nslookup-verificatie een hostname met dubbele delen teruggeeft (bijvoorbeeld **cucm.domain.local.domain.local**), moeten de DNS-vermeldingen worden geverifieerd en met een

volledig stopteken worden beëindigd, anders wordt de oorsprong van de zone toegevoegd aan de gezaghebbende naam.

Als er problemen zijn met de gemaakte items, kunnen deze eenvoudigweg van de DNS-server worden verwijderd. Hoewel CLI de items aan Microsoft DNS moet toevoegen, kunnen de items veilig en eenvoudig in de GUI worden verwijderd.

Gerelateerde informatie

Voor een toepassing op meerdere domeinen (verschillende interne en externe domeinnamen) van MRA raadpleegt u dit document:

[Configuratievoorbeeld: Mobiele en externe toegang via snelweg/VCS in een meervoudige uitrol](#)