Erstellen eines Pinpoint-DNS-Eintrags

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie im internen Namenserver (NS) punktuelle Einträge für Dienstdatensätze (Service Records, SRV) erstellen, um das Fehlen von DNS-Aufteilungen (Split Domain Name System) zu umgehen.

Unterstützt von Zoltan Kelemen, herausgegeben von Joshua Alero und Lidiya Bogdanova, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundlegendes DNS-Verständnis
- Eine Domäne, die korrekt auf dem öffentlichen, behördlichen NS konfiguriert ist

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Hinweis: Die Informationen in diesem Dokument können entweder mit dem Microsoft DNS-

Server oder BIND verwendet werden. Sie müssen nur die Schritte ausführen, die für den jeweiligen DNS-Server geeignet sind. Anleitungen für andere DNS-Servertypen sind nicht enthalten. Das Konzept kann jedoch mit jedem anderen DNS-Server verwendet werden, wenn der Server diese Konfiguration unterstützt.

Hinweis: Das interne NS wird von internen Benutzern sowie von Video Communication System (VCS)/Cisco Expressway-C verwendet.

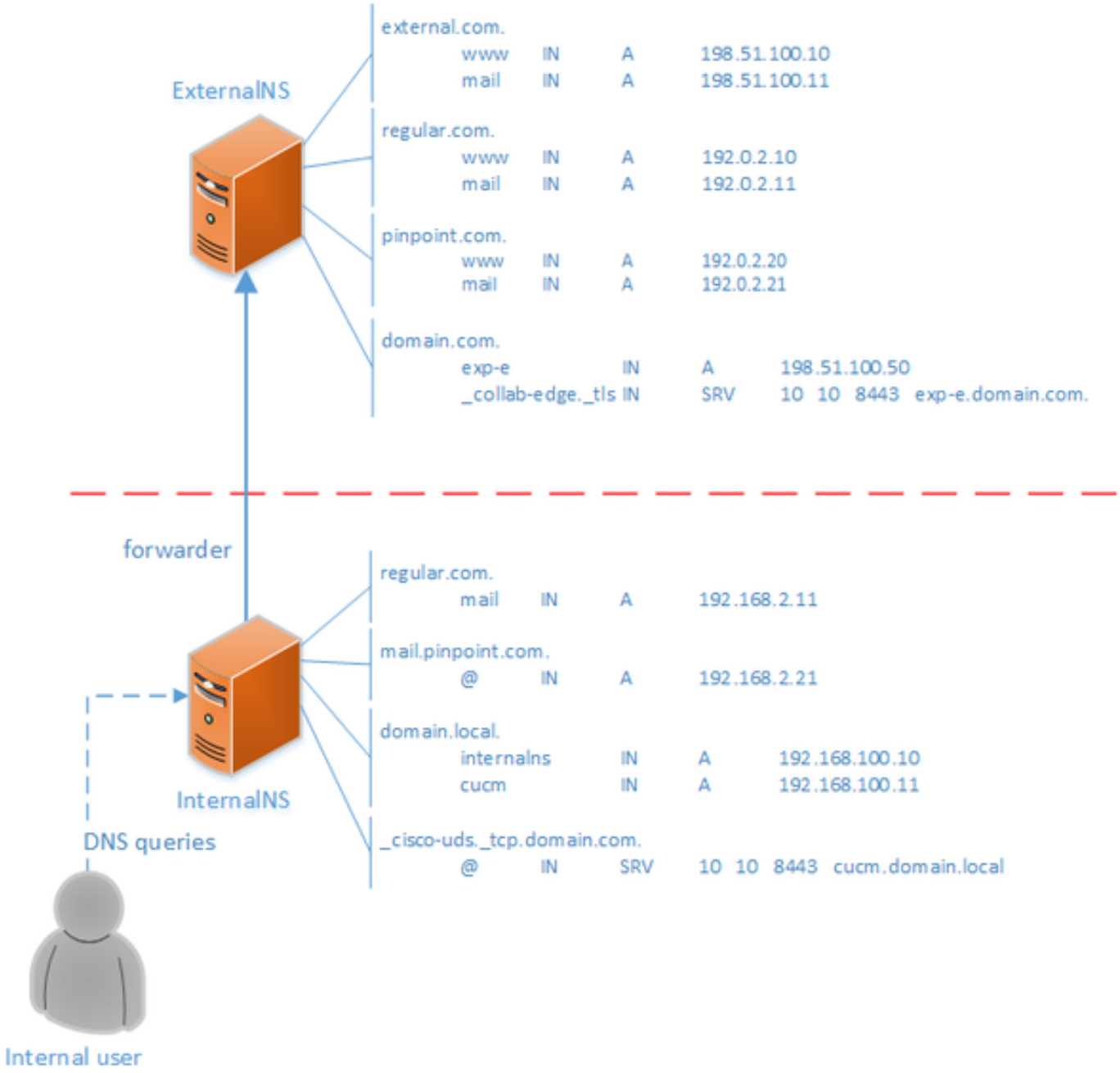
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Pinpoint DNS-Übersicht

Der pinpoint DNS-Eintrag ist eine Zone, die nur für einen einzelnen Host erstellt wurde. Dieser Eintrag kann auf einem Namenserver als autorativ definiert werden, der für die übergeordnete Domäne nicht autoritär ist. Dadurch können andere DNS-Abfragen für diese Domäne an den autoritativen Server weitergeleitet werden.

Die Pinpoint-Zone enthält in der Regel einen Datensatz neben den erforderlichen SOA- (Start of Authority) und Namenserver-Datensätzen. Dieser Datensatz ist ein Selbstverweis, der mit dem Namen der Zone identisch ist und als **übergeordneter Ordner** in **Microsoft DNS** angezeigt wird, oder er wird durch ein **@**Symbol in der **BIND-Zone-**Datei referenziert. Der Datensatz kann von jedem vom DNS unterstützten Typ sein. Das **@** Symbol wird auch in CLI-Tools (Windows Command Line Interface) verwendet und funktioniert genauso wie in BIND.

Das folgende Bild zeigt ein Beispiel für diese Datensätze:



Dies ist eine Funktion des DNS-Systems und basiert nicht auf einem Mechanismus in den Anwendungen Cisco Jabber oder Cisco Expressway. Wenn kein Split DNS verfügbar ist, wird die Lösung auch für die Bereitstellung von Cisco Jabber unterstützt.

Wenn ein Name-Server als autoritär oder Master für eine Domäne konfiguriert ist, werden Abfragen für Namen innerhalb dieser Domäne nicht an die Weiterleitungsmitglieder weitergeleitet, auch wenn ein bestimmter Name nicht aufgelöst werden kann. Damit interne und externe Benutzer der Domäne in der Regel unterschiedliche Namensauflösungen innerhalb derselben Domäne erhalten, wird ein geteilter DNS verwendet. In einer Split-DNS-Konfiguration unterhält ein interner DNS-Server eine Kopie der Zone mit internen Einträgen, und ein externer DNS-Server unterhält eine Kopie der Zone mit externen Einträgen. Einträge in der externen Zone, aber nicht in der internen Zone müssen bei internen Abfragen nicht aufgelöst werden können.

Da dies zu Verwaltungsaufwand führen kann, ziehen es einige Netzwerkadministratoren vor, Split-DNS-Konfigurationen zu vermeiden. Pinpoint DNS Einträge bieten in diesen Fällen eine Alternative.

Konfigurieren

DNS SRV-Datensätze erstellen

Für die automatische Bereitstellung von Cisco Jabber sowie für den Mobile and Remote Access (MRA)-Service sind für jede Domäne zwei SRV-Datensätze beteiligt (Beispiel: **domain.com**):

- **_collab-edge._tls.domain.com**
- **_cisco-uds_tcp.domain.com**

Wenn Expressway und/oder Cisco Unified Communications Manager (CUCM) geclustert sind, können mehrere Einträge für diese Datensätze vorhanden sein.

Wenn die autorative Zonendatei für **domain.com** nur auf dem externen NS vorhanden ist, ist ein DNS-Pinpoint-Eintrag für **_cisco-uds._tcp** auf dem internen NS erforderlich. Zuerst muss die DNS-Zone für den Point festgelegt werden, dann die SRV innerhalb der Zone.

> Der SRV-Datensatz **_cisco-uds.**_tcp darf nur im internen Netzwerk aufgelöst werden, nicht von extern, und er muss auf den vollqualifizierten Domänennamen (FQDN) der CUCM-Knoten(s) mit User Data Services (UDS) aufgelöst werden.
>
> Der SRV-Datensatz **_collab-edge.tls** muss vom externen Netzwerk auflösbar sein und in den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Expressway-E-Servers aufgelöst werden können.

Windows-DNS-Server konfigurieren

Der DNS-Pinpoint-Eintrag wird wie jede andere Zone erstellt, und sein Name muss den gesamten SRV-Namen enthalten (z. B. **_cisco-uds._tcp.domain.com**). Dieser Schritt kann auch über die grafische Benutzeroberfläche (GUI) durchgeführt werden, obwohl im folgenden Beispiel davon ausgegangen wird, dass der DNS-Eintrag für den Pinpoint noch nicht erstellt wurde.

Um den SRV-Datensatz selbst hinzuzufügen, muss ein CLI-Tool verwendet werden. Sie dürfen einen SRV-Datensatz über die GUI nicht zu einem DNS-Eintrag auf einen bestimmten Punkt hinzufügen, da dies nicht funktioniert. Nach dem Hinzufügen über die CLI können diese SRV-Datensätze mit den regulären Tools wie jeder andere Eintrag verwaltet werden. Die Windows-CLI stellt zwei Methoden bereit - entweder **dnscmd** oder **PowerShell-**Befehle. In beiden folgenden Beispielen werden die beiden DNS-Einträge für "pinpoint" erstellt und ein SRV-Datensatz für **_cisco-uds_tcp** hinzugefügt**.**

Es kann jeweils nur eine dieser beiden Methoden verwendet werden:

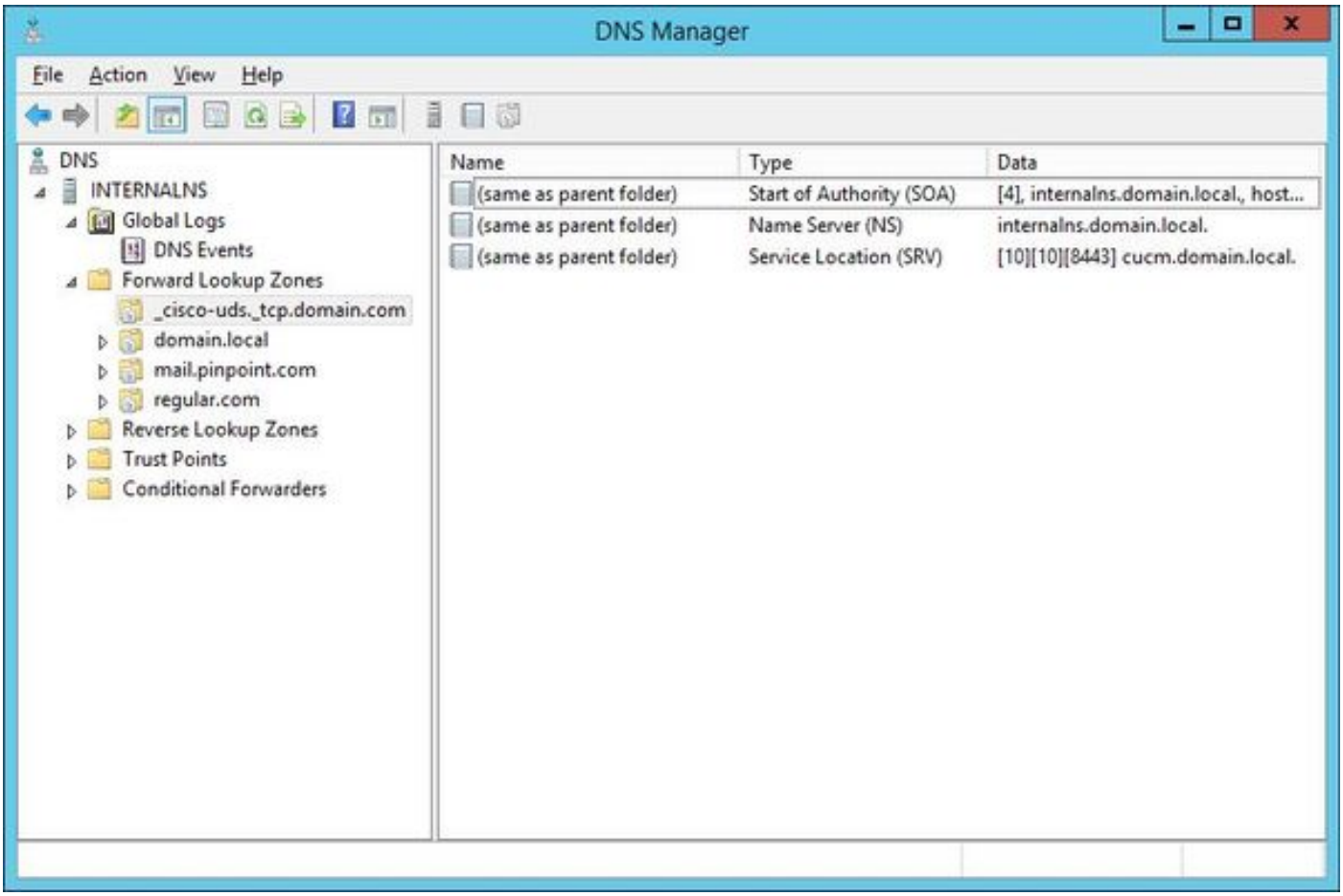
- Beispiel 1 - Verwenden von **dnscmd**

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

- Beispiel 2 - Verwendung von **PowerShell-**Befehlen (als **dnscmd** in zukünftigen Versionen von Microsoft Windows Server veraltet sein soll, **PowerShell** kann für denselben Zweck verwendet werden). **Die Replikationsbereichsoptionen** sind **Domain**, **Forest**, oder Sie können eine Datei mit dem Parameter **-ZoneFile** einrichten, wenn die Zone nicht in Active Directory (AD) integriert ist.

```
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"
```

Das folgende Bild zeigt ein Beispiel dafür, wie der DNS-Eintrag mit dem SRV-Eintrag in der GUI aussieht:



BIND DNS-Server konfigurieren

Bei BIND DNS-Server wird der DNS-Pinpoint-Eintrag genauso erstellt wie eine reguläre Zonendatei.

Der **$ORIGIN-**Eintrag muss auf den FQDN des SRV-Datensatzes (z. B. **_cisco-uds._tcp.domain.com**) zeigen, und SOA- und NS-Datensätze werden wie gewohnt hinzugefügt. Die SRV ist optional (unabhängig davon, ob der DNS-Eintrag den SRV-Datensatz definiert oder überschreibt), und der verwendete Name ist **@**, was dem Namen / ORIGIN der Zone entspricht.

Hier ein Beispiel für einen **_cisco-uds._tcp.domain.com.zone** Dateiinhalt:

```
$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.
```

Im Folgenden finden Sie ein Beispiel **zum Hinzufügen** der Zonendefinition zu **name.conf**:

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- Verwenden Sie den Befehl **nslookup** mit dem auf das interne NS festgelegten Server, um DNS-Einträge zu überprüfen.

Im Folgenden finden Sie ein Beispiel für das Nachschlagen eines Hostnamens aus der übergeordneten Domäne und für das Nachschlagen des SRV-Datensatzes, der auf dem internen NS erstellt wurde:

```
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
```

Im Folgenden finden Sie ein Beispiel, wie Sie einen Hostnamen nachschlagen, der nicht auf dem internen NS konfiguriert ist, um zu überprüfen, ob die Anfragen wie erwartet weitergeleitet werden.

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

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

- Legen Sie für den Server ein öffentliches NS oder ein externes NS fest, und wiederholen Sie die gleichen Schritte. Die SRV-Suche für den Datensatz **_cisco-uds.**_tcp SRV schlägt fehl.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Wenn die **nslookup**-Verifizierung einen Hostnamen mit doppelten Teilen zurückgibt (z. B. **cucm.domain.local.domain.local**), müssen die DNS-Einträge durch ein vollständiges Stoppzeichen terminiert werden, ansonsten würde der Ursprung der Zone dem aufgelösten Hostnamen hinzugefügt.

Wenn Bedenken hinsichtlich der erstellten Einträge bestehen, können diese einfach vom DNS-Server gelöscht werden. Obwohl CLI erforderlich ist, um Einträge zu Microsoft DNS hinzuzufügen, können Einträge sicher und einfach in der GUI gelöscht werden.

Zugehörige Informationen

Informationen zur Bereitstellung mehrerer Domänen (verschiedene interne und externe Domänennamen) von MRA finden Sie in diesem Dokument:

Konfigurationsbeispiel: Mobiler und Remote-Zugriff über Expressway/VCS in einer Bereitstellung mit mehreren Domänen