Cómo Crear una Entrada DNS de Punto de Destino

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Descripción general de DNS de punto de vista](#)
[Configurar](#)
[Crear registros SRV DNS](#)
[Configurar servidor DNS de Windows](#)
[Configurar servidor DNS BIND](#)
[Verificación](#)
[Troubleshoot](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo crear entradas de puntos de conexión para los registros de servicio (SRV) en el servidor de nombres interno (NS) para solucionar la falta de configuraciones divididas del sistema de nombres de dominio (DNS).

Colaborado por Zoltan Kelemen, Editado por Joshua Alero y Lidiya Bogdanova, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de DNS
- Un dominio que se configura correctamente en el NS de autoridad pública

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows Server 2012
- Sistema de comunicación por vídeo (VCS)/Expressway

Nota: La información de este documento se puede utilizar con el servidor DNS de Microsoft o BIND. Sólo necesita utilizar los pasos adecuados para su servidor DNS concreto. No se proporcionan instrucciones para otros tipos de servidores DNS, pero el concepto se puede utilizar con cualquier otro servidor DNS si el servidor admite esta configuración.

Nota: Los usuarios internos, así como Video Communication System (VCS) / Cisco Expressway-C, utilizan el NS interno.

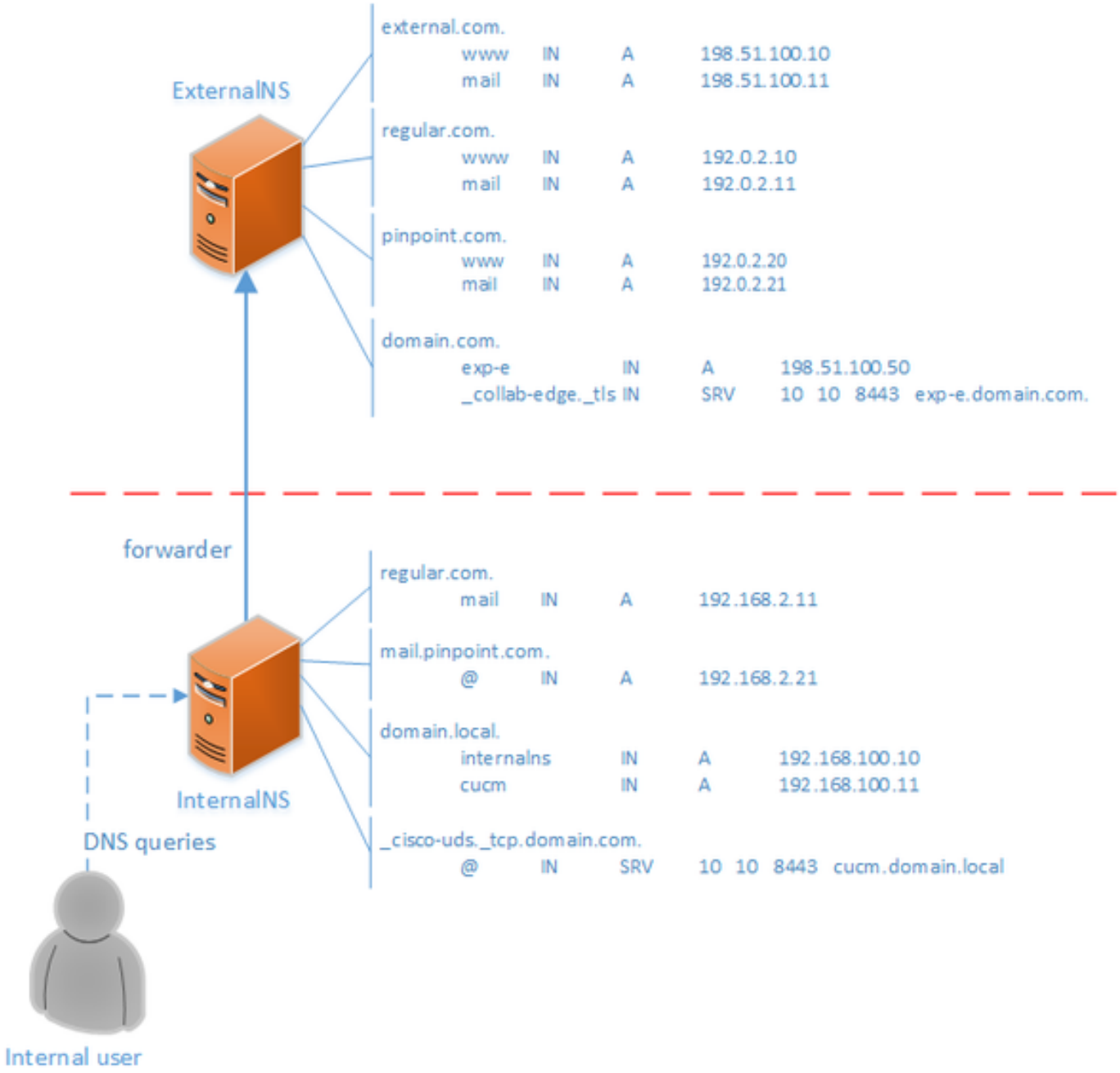
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Descripción general de DNS de punto de vista

La entrada DNS de punto de conexión es una zona creada para un solo host. Esta entrada se puede definir como autoritativa en un servidor de nombres, que no es autoritativa para el dominio primario. Esto permite que otras consultas DNS para este dominio se reenvíen al servidor autorizado.

La zona de punto de clavija normalmente contiene un único registro además de los registros de inicio de autoridad (SOA) y de servidor de nombres requeridos. Este registro es una referencia automática, idéntica al nombre de la zona y aparece como **la misma carpeta que la carpeta principal** en **Microsoft DNS**, o se hace referencia a él mediante un símbolo **@** en el archivo **BIND zone**. El registro puede ser de cualquier tipo compatible con el DNS. El símbolo **@** también se utiliza en las herramientas de la interfaz de línea de comandos (CLI) de Windows y funciona de la misma manera que en BIND.

La siguiente imagen proporciona un ejemplo de estos registros:



Se trata de una función del sistema DNS y no se basa en ningún mecanismo de las aplicaciones Cisco Jabber o Cisco Expressway. También es una solución compatible para la implementación de Cisco Jabber si DNS dividido no está disponible.

Si un servidor de nombres está configurado como autorizado o maestro para un dominio, las consultas no se reenvían para nombres dentro de ese dominio a sus reenviadores, incluso si no puede resolver un nombre específico. Por lo tanto, para proporcionar una resolución de nombres diferente dentro del mismo dominio a usuarios internos y externos del dominio normalmente, se usaría un DNS dividido. En una configuración DNS dividida, un servidor DNS interno mantiene una copia de la zona con entradas específicas internas y un servidor DNS externo mantiene una copia de la zona con entradas específicas externas. Las entradas presentes en la zona externa, pero no en la zona interna, deben fallar en resolver para las consultas internas.

Dado que esto puede provocar sobrecarga de administración, algunos administradores de red prefieren evitar las configuraciones de DNS divididas. Las entradas DNS de puntos de acceso ofrecen una alternativa en estos casos.

Configurar

Crear registros SRV DNS

Para el aprovisionamiento automático de Cisco Jabber, así como para el servicio de acceso remoto y móvil (MRA), se incluyen dos registros SRV para cada dominio (utilizando **domain.com** como ejemplo):

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

Puede tener varias entradas para estos registros si Expressway o Cisco Unified Communications Manager (CUCM) están agrupados.

Cuando el archivo de zona autorizado para **domain.com** sólo existe en el NS externo, se requiere una entrada de DNS de punto para **_cisco-uds._tcp** en el NS interno. Primero debe crearse la zona DNS de punto de precisión y luego el SRV dentro de la zona.

> El registro SRV **_cisco-uds._tcp** sólo debe resolverse en la red interna, no desde el externo, y debe resolverse con el nombre de dominio completo (FQDN) de los nodos CUCM con User Data Services (UDS).

> El registro SRV **_collab-edge.tls** debe resolverse desde la red externa y se resuelve en el nombre de dominio completo (FQDN) del servidor de Expressway-E.

Configurar servidor DNS de Windows

La entrada DNS de punto de conexión se crea como cualquier otra zona y su nombre debe contener el nombre SRV completo (por ejemplo, **_cisco-uds._tcp.domain.com**). Este paso se puede realizar también a través de la interfaz gráfica de usuario (GUI), aunque en el ejemplo siguiente se asume que la entrada de DNS de punto de inflexión no se ha creado todavía.

Para agregar el registro SRV, se debe utilizar una herramienta CLI. No debe agregar un registro SRV a una entrada DNS de punto de vista a través de la GUI, ya que esto no funciona. Una vez agregados a través de la CLI, estos registros SRV son manejables con las herramientas regulares como cualquier otra entrada. La CLI de Windows presenta dos métodos: los comandos **dnscmd** o **PowerShell**. Los dos ejemplos siguientes crean las dos entradas de DNS de punto de precisión y añaden un registro SRV para **_cisco-uds._tcp**

Sólo se puede utilizar uno de estos dos métodos a la vez:

- ejemplo 1 - utilización de **dnscmd**

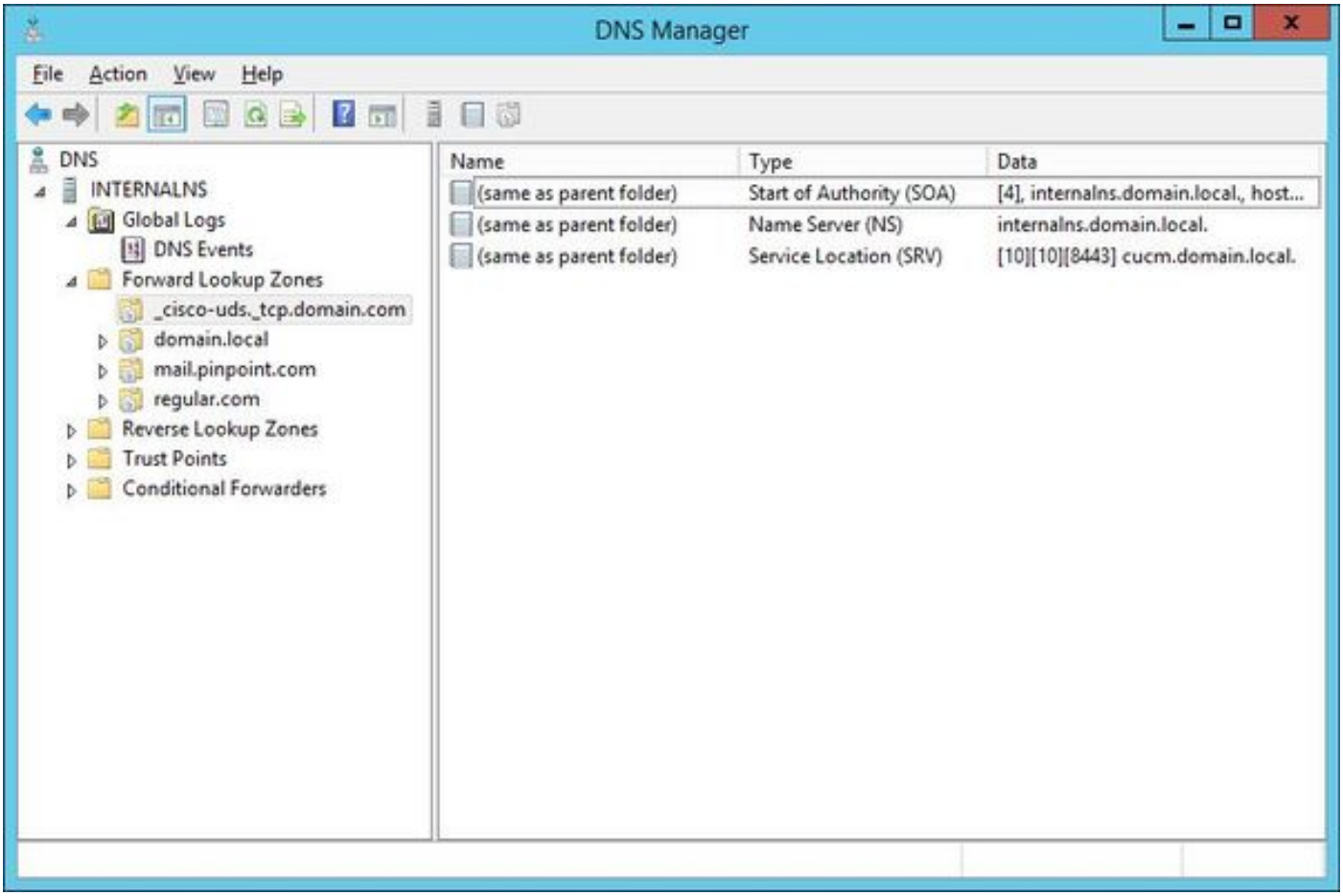
```
dnscmd . /zoneadd _cisco-uds._tcp.domain.com. /dsprimary
dnscmd . /recordadd _cisco-uds._tcp.domain.com. "@" SRV 10 10 8443 cucm.domain.local
```

- ejemplo 2: mediante el uso de comandos **PowerShell** (como **dnscmd** se debe dejar de utilizar

en versiones futuras de Microsoft Windows Server, se puede utilizar PowerShell para el mismo propósito). **Las** opciones **del ámbito de replicación** son **Dominio**, **Bosque**, o puede configurar un archivo con el parámetro **-ZoneFile**, si la zona no está integrada en 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"
```

La siguiente imagen proporciona un ejemplo de cómo se ve la entrada DNS de punto de inflexión con el registro SRV en la GUI:



Configurar servidor DNS BIND

Con el servidor DNS BIND, la entrada DNS de punto de conexión se crea de la misma manera que un archivo de zona normal.

La entrada **$ORIGIN** debe apuntar al FQDN del registro SRV (por ejemplo, **_cisco-uds._tcp.domain.com**) y los registros SOA y NS se agregan como siempre. El SRV es opcional (si la entrada DNS del punto de conexión define o anula el registro SRV) y el nombre utilizado es **@**que es equivalente al nombre / ORIGEN de la zona.

Aquí hay un ejemplo de un contenido de archivo **_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.
```

Aquí hay un ejemplo de cómo **agregar** la definición de zona a **named.conf**:

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

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

- Utilice el comando **nslookup** con el servidor configurado en el NS interno, para verificar las entradas DNS de punto de inclemencia.

Este es un ejemplo de cómo buscar un nombre de host del dominio primario y cómo buscar el registro SRV creado en el NS interno:

```
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
```

Este es un ejemplo de cómo buscar un nombre de host que no está configurado en el NS interno, para verificar que las solicitudes se reenvían como se esperaba.

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

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

- Establezca el servidor en un NS público, o en el NS externo, y repita los mismos pasos. La búsqueda SRV para el registro **_cisco-uds._tcp SRV** falla.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Si la verificación **nslookup** devuelve un nombre de host con partes duplicadas (por ejemplo,

cucm.domain.local.domain.local), las entradas DNS deben verificarse para que terminen con un signo de parada completa; de lo contrario, el origen de la zona se agregaría al nombre de host resuelto.

Si hay problemas con las entradas creadas, simplemente se pueden eliminar del servidor DNS. Aunque CLI es necesaria para agregar las entradas a Microsoft DNS, las entradas se pueden eliminar de forma segura y sencilla en la GUI.

Información Relacionada

Para una implementación multidominio (diferentes nombres de dominio internos y externos) de MRA, consulte este documento:

Ejemplo de configuración: Acceso remoto y móvil a través de Expressway/VCS en una implementación de varios dominios