

Cómo crear una entrada DNS de punta

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Descripción de punta DNS](#)

[Configurar](#)

[Cree los expedientes DNS SRV](#)

[Configure al servidor DNS de Windows](#)

[Configure al servidor DNS del LAZO](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo crear las entradas de punta para los registros de servicio (SRV) en el Servidor de nombres interno (NS) para trabajar alrededor de la falta de configuraciones del Domain Name System (DNS) de la fractura.

Contribuido por Zoltan Kelemen, editado por Joshua Alero y Lidiya Bogdanova, ingenieros de Cisco TAC.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de dns
- Un dominio que se configura correctamente en el NS autoritario público

Componentes Utilizados

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

- Microsoft Windows server 2012
- Comunicación mediante video sistema (/)/autopista VCS

Nota: La información en este documento se puede utilizar con el servidor DNS de Microsoft,

o el LAZO. Usted necesita solamente utilizar los pasos apropiados para su servidor DNS determinado. Las instrucciones para otros tipos de servidores DNS no se proporcionan, pero el concepto se puede utilizar con cualquier otro servidor DNS si los soportes de servidor esta configuración.

Nota: El NS interno es utilizado por los usuarios internos, así como el sistema de comunicación mediante video (VCS)/la autopista-C de Cisco.

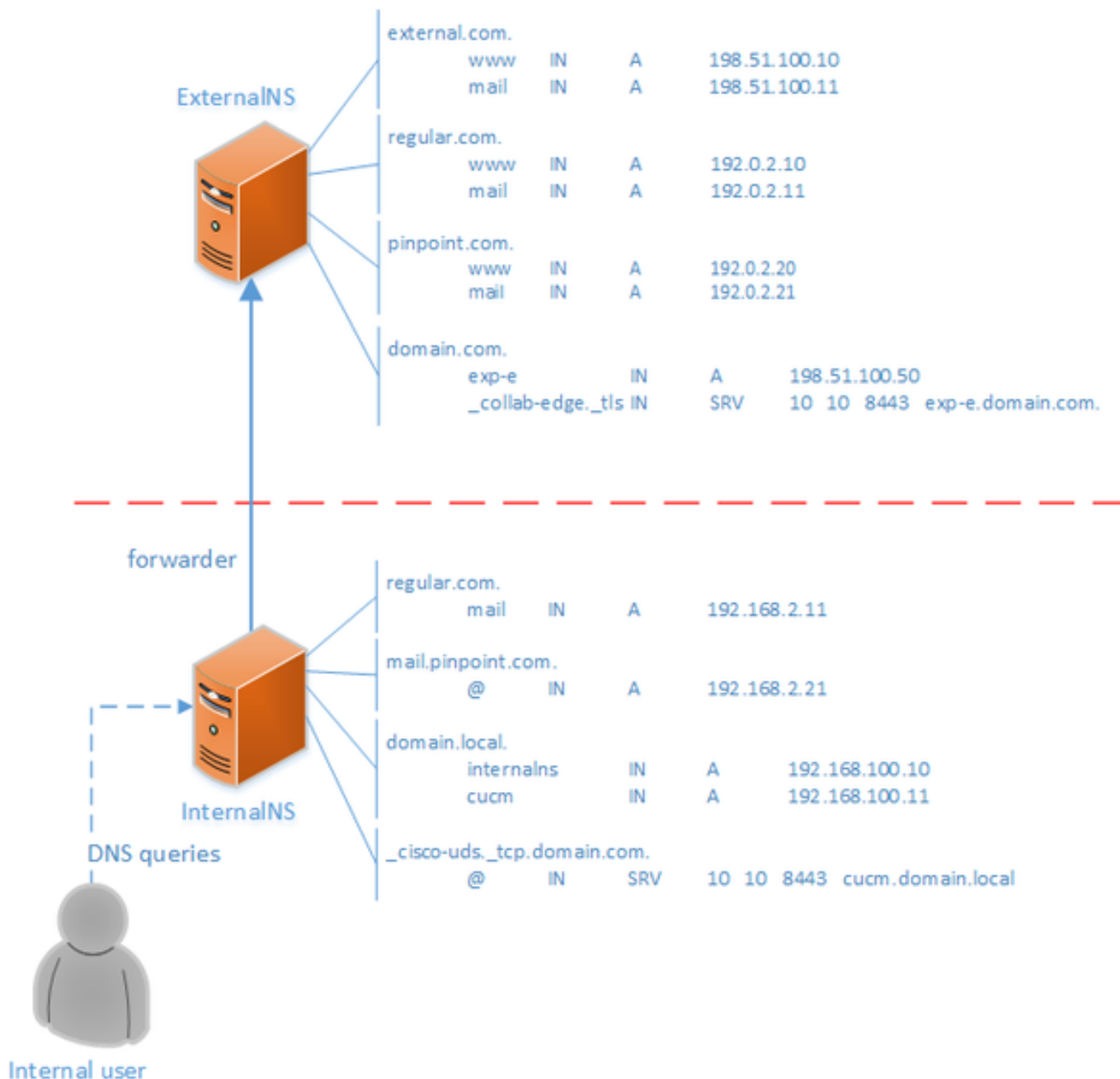
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Establezca claramente la descripción DNS

La entrada DNS de punta es una zona creada para un solo host solamente. Esta entrada se puede definir como autoritario en un Servidor de nombres, que no es autoritario para el dominio del padre. Esto permite que otras interrogaciones DNS para que este dominio sea remitido al autoritario separa.

La zona de punta contiene generalmente un único registro además del comienzo requerido de los expedientes de la autoridad (SOA) y del Servidor de nombres. Este expediente es una autorreferencia, idéntica al nombre de la zona y aparece como **lo mismo que la carpeta principal en Microsoft DNS**, o es referido por **@** un símbolo en el **archivo de zona del LAZO**. El expediente puede ser de cualquier tipo soportado por el DNS. **@** el símbolo también se utiliza en las herramientas del comando line interface(cli) de Windows, y trabaja la misma manera que en el LAZO.

La imagen siguiente proporciona un ejemplo de estos expedientes:



Ésta es una característica del sistema DNS y no confía en ningún mecanismo en el Jabber de Cisco o las aplicaciones de la autopista de Cisco. Es también una solución soportada para el despliegue del Jabber de Cisco si el DNS dividido no está disponible.

Si configuran a un Servidor de nombres como autoritario o principal para un dominio, después las interrogaciones no se remiten para los nombres dentro de ese dominio a sus promotores, incluso si puede no poder resolver un nombre específico. Así, para proporcionar diversa resolución de nombre dentro del mismo dominio a interno y a los usuarios externos del dominio normalmente, el DNS dividido sería utilizado. En una configuración del DNS dividido, un servidor DNS interno mantiene una copia de la zona con las entradas interno-específicas y un servidor DNS externo mantiene una copia de la zona con las entradas externo-específicas. Las entradas presentes en la zona externa, pero no en la zona interna deben no poder resolver para las interrogaciones internas.

Puesto que esto puede llevar a la tara de administración, algunos administradores de la red prefieren evitar las configuraciones del DNS dividido. Las entradas DNS de punta ofrecen una

alternativa en estos casos.

Configurar

Cree los expedientes DNS SRV

Para el auto-provisionamiento del Jabber de Cisco, así como el servicio del móvil y del Acceso Remoto (MRA), dos expedientes SRV están implicados para cada dominio (usando **domain.com** como un ejemplo):

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

Usted puede tener entradas múltiples para estos expedientes si agrupan la autopista y/o al administrador de las Comunicaciones unificadas de Cisco (CUCM).

Cuando el archivo de zona authoritative para **domain.com** existe solamente en el externo NS, una entrada DNS de punta para el **_tcp de los _cisco-uds.** se requiere en el NS interno. Primero la zona de DNS de punta necesita ser creada, entonces el SRV dentro de la zona.

El expediente del **_tcp** SRV de los **_cisco-uds.** debe ser solamente resolvable en la red interna, no del externo, y debe resolver al nombre de dominio completo (FQDN) de los nodos CUCM con los servicios de datos del usuario (UD).

El expediente de los **_tls** SRV del **_collab-edge.** debe ser resolvable de la red externa, y de las resoluciones al nombre de dominio completo (FQDN) del servidor de la autopista-e.

Servidor DNS de Windows de la configuración

Se crea la entrada DNS de punta mientras que cualquier otra zona, y su nombre deben contener el nombre entero SRV (por ejemplo, **_cisco-uds._tcp.domain.com**). Este paso se puede realizar con el Interfaz gráfica del usuario (GUI) también, aunque el ejemplo abajo asuma que la entrada DNS de punta no se ha creado ya.

Para agregar el expediente sí mismo SRV, una herramienta CLI debe ser utilizada. Usted no debe agregar un expediente SRV a una entrada DNS de punta con el GUI, pues éste no trabaja. Agregado una vez vía el CLI, estos expedientes SRV son manejables con las herramientas regulares apenas como cualquier otra entrada. Windows CLI presenta dos métodos - **dnscmd** o los comandos de **PowerShell**. Ambos ejemplos que siguen crean las dos entradas DNS de punta y agregan un expediente SRV para el **_tcp de los _cisco-uds.**

Solamente uno de este dos en un momento de los métodos puede ser utilizado:

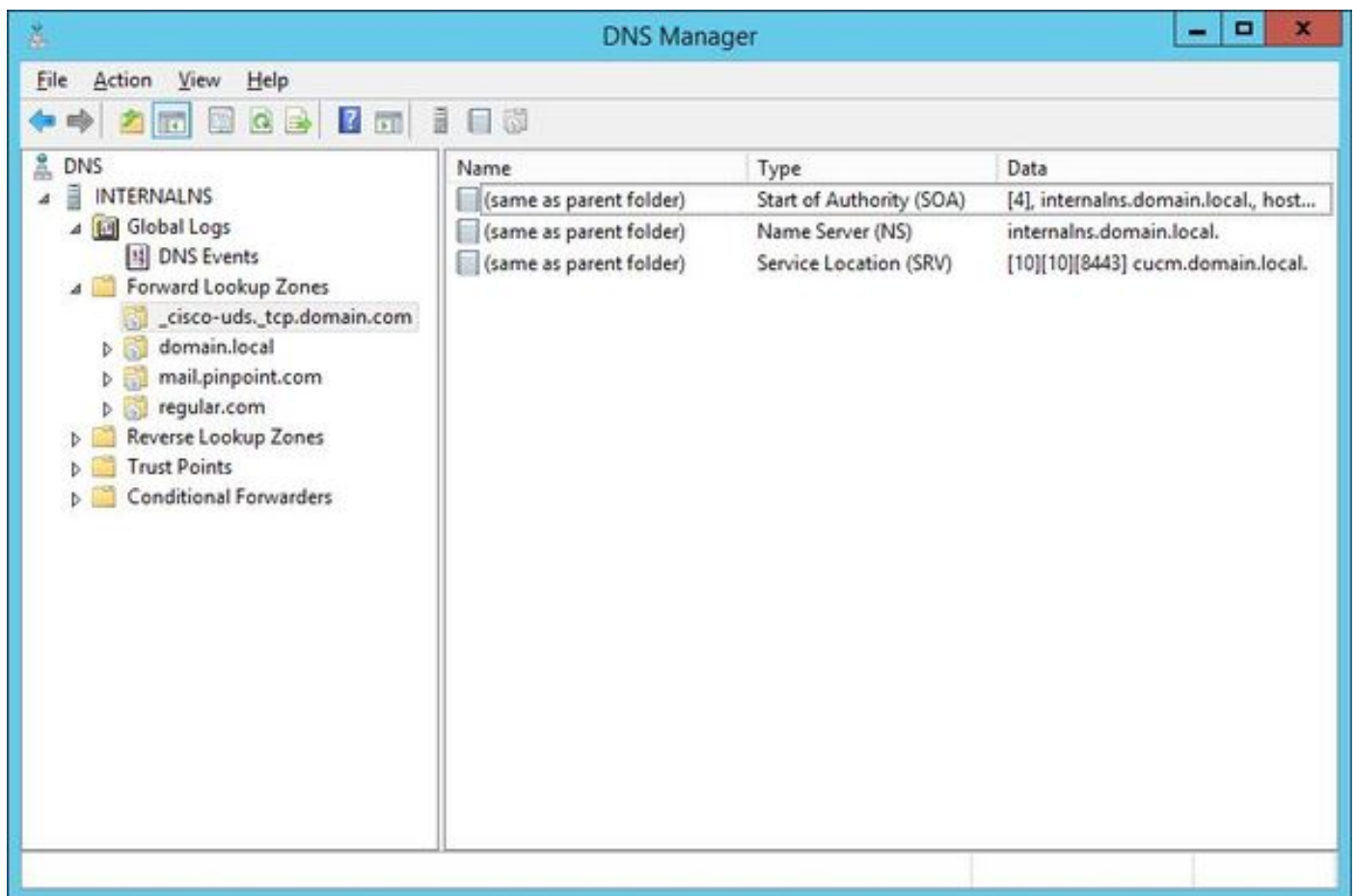
- ejemplo 1 - usando el **dnscmd**

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

- ejemplo 2 - usando los comandos de **PowerShell** (como el **dnscmd** debe ser desaprobadado en las versiones futuras del Microsoft Windows server, **PowerShell** se puede utilizar para el mismo propósito). **Las opciones de alcance de la replicación** son **dominio**, **bosque**, o **usted** puede configurar un archivo con - el parámetro de **ZoneFile**, si la zona no es el Active Directory (AD) integrado

```
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 imagen siguiente proporciona un ejemplo de cómo la entrada DNS de punta con el expediente SRV parece en el GUI:



Servidor DNS del LAZO de la configuración

Con el servidor DNS del LAZO, la entrada DNS de punta se crea la misma manera que un archivo de zona regular.

La entrada **\$ORIGIN** debe señalar al FQDN del expediente SRV (por ejemplo, **_cisco-uds._tcp.domain.com**) y los expedientes de SOA y NS se agregan como de costumbre. El SRV es opcional (si la entrada DNS de punta define o reemplaza el expediente SRV) y es el nombre usado **@** que es equivalente al nombre/al ORIGEN de la zona.

Aquí está un ejemplo de un contenido del archivo **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.

```

Aquí está un ejemplo de cómo toAdd la definición de la 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 establezca al NS interno, para verificar las entradas DNS de punta.

Aquí está un ejemplo de cómo mirar para arriba un nombre de host del dominio del padre y de cómo mirar para arriba el expediente SRV creado en el NS interno:

```
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

```

Aquí está un ejemplo de cómo mirar para arriba un nombre de host que no se configure en el NS interno, para verificar que las peticiones están remitidas como se esperaba.

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

Non-authoritative answer:

```

Name:   www.example.com
Addresses: 203.0.113.42

```

- Fije el servidor a un público NS, o al externo NS, y relance los mismos pasos. Las operaciones de búsqueda SRV para el expediente del **_tcp SRV de los _cisco-uds.** fallan.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Si la verificación del **nslookup** vuelve un nombre de host con las piezas duplicados (por ejemplo, **cucm.domain.local.domain.local**), **después las entradas DNS se deben verificar para ser terminado por una muestra del punto final**, si no el origen de la zona sería agregado al nombre de host resuelto.

Si hay preocupaciones con las entradas creadas, pueden ser borradas simplemente del servidor DNS. Aunque el CLI se requiera agregar las entradas a Microsoft DNS, las entradas se pueden borrar con seguridad y simplemente en el GUI.

Información Relacionada

Para un despliegue del multi-dominio (diversos Domain Name internos y externos) de MRA consulte este documento:

[Ejemplo de configuración: Móvil y Acceso Remoto con Expressway/VCS en un despliegue del multi-dominio](#)