Como criar uma entrada DNS de ponto de identificação

Contents

Introduction

Este documento descreve como criar entradas pontuais para registros de serviços (SRV) no Servidor de Nomes (NS) interno para contornar a falta de configurações de Sistema de Nomes de Domínio (DNS - Domain Name System) dividido.

Contribuído por Zoltan Kelemen, editado por Joshua Alero e Lidiya Bogdanova, Engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica do DNS
- Um domínio configurado corretamente no NS de autoridade pública

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

Note: As informações neste documento podem ser usadas com o servidor Microsoft DNS ou BIND. Você só precisa usar as etapas apropriadas para seu servidor DNS específico. Não são fornecidas instruções para outros tipos de servidores DNS, mas o conceito pode ser usado com qualquer outro servidor DNS se o servidor suportar essa configuração.

Note: O NS interno é usado por usuários internos, assim como o Video Communication System (VCS) / Cisco Expressway-C.

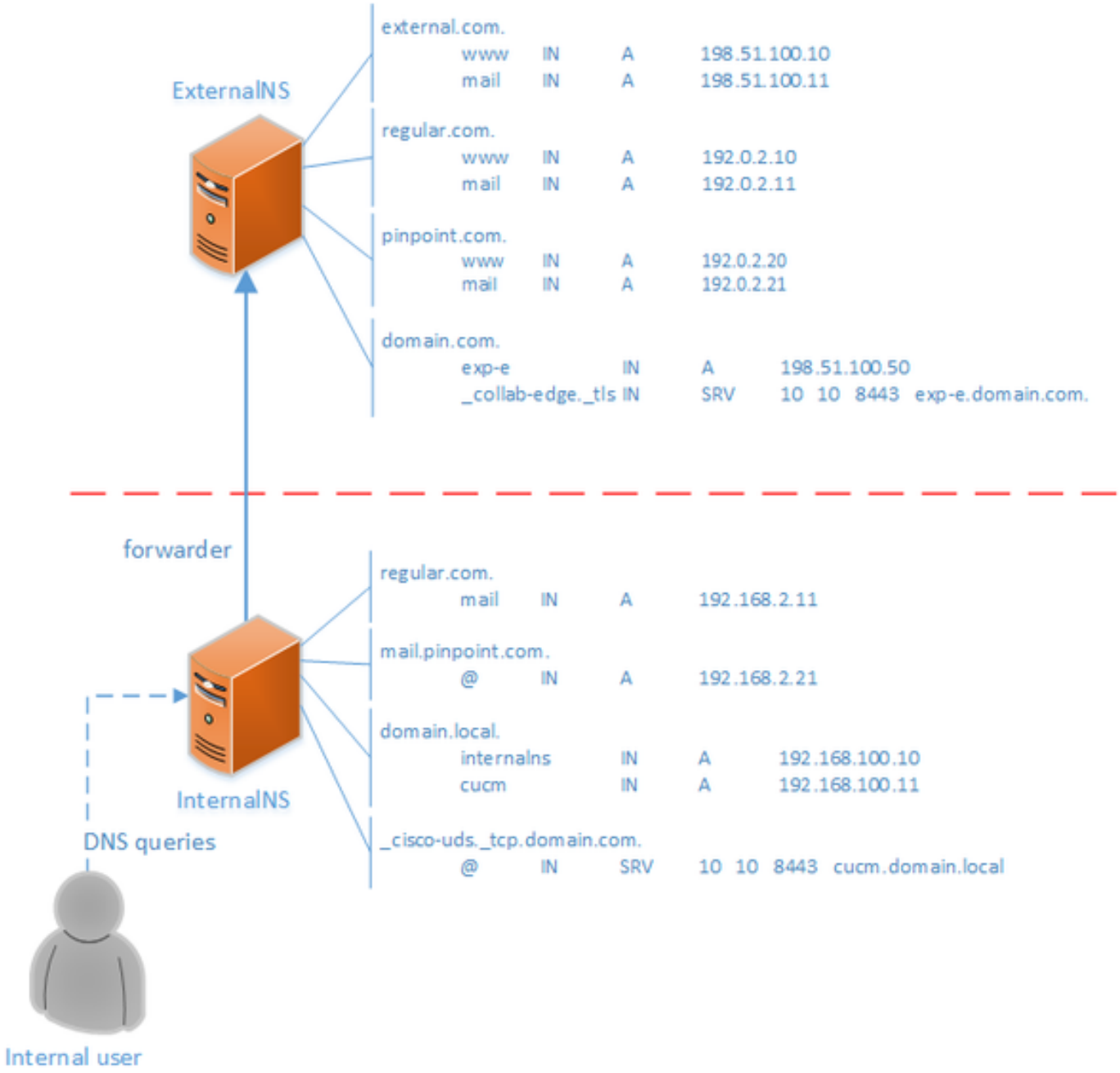
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral de DNS de ponto de Pinpoint

A entrada DNS do ponto de extremidade é uma zona criada somente para um único host. Essa entrada pode ser definida como autoritativa em um Servidor de Nomes, que não é autoritativa para o domínio pai. Isso permite que outras consultas DNS para esse domínio sejam encaminhadas ao servidor autoritativo.

A zona do ponto de extremidade geralmente contém um único registro além dos registros necessários do início da autoridade (SOA) e do servidor de nome. Este registro é uma referência automática, idêntica ao nome da zona e aparece como **igual à pasta pai** no **Microsoft DNS**, ou é referenciado por um **@** símbolo no arquivo de **zona BIND**. O registro pode ser de qualquer tipo suportado pelo DNS. O símbolo **@** também é usado em ferramentas da CLI (Command Line Interface, interface de linha de comando) do Windows e funciona da mesma forma que em BIND.

A imagem a seguir fornece um exemplo dos seguintes registros:



Esse é um recurso do sistema DNS e não depende de nenhum mecanismo nos aplicativos Cisco Jabber ou Cisco Expressway. Também é uma solução compatível para a implantação do Cisco Jabber se o DNS dividido não estiver disponível.

Se um Servidor de Nomes estiver configurado como autoritativo ou mestre para um domínio, as consultas não serão encaminhadas para nomes dentro desse domínio para seus encaminhadores, mesmo que ele não possa resolver um nome específico. Assim, para fornecer uma resolução de nome diferente dentro do mesmo domínio para usuários internos e externos do domínio normalmente, seria usado um DNS dividido. Em uma configuração DNS dividida, um servidor DNS interno mantém uma cópia da zona com entradas específicas internas e um servidor DNS externo mantém uma cópia da zona com entradas específicas externas. As entradas presentes na zona externa, mas não na zona interna, devem falhar ao resolver consultas internas.

Como isso pode levar à sobrecarga de gerenciamento, alguns administradores de rede preferem evitar configurações DNS divididas. As entradas DNS do ponto de identificação oferecem uma

alternativa nesses casos.

Configurar

Criar registros SRV DNS

Para o provisionamento automático do Cisco Jabber, bem como para o serviço de Acesso Móvel e Remoto (MRA - Mobile and Remote Access), dois registros SRV estão envolvidos para cada domínio (usando **domain.com** como exemplo):

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

Você pode ter várias entradas para esses registros se o Expressway e/ou o Cisco Unified Communications Manager (CUCM) estiver em cluster.

Quando o arquivo de zona autorativa para **domain.com** existe apenas no NS externo, uma entrada DNS pinpoint para **_cisco-uds._tcp** é necessária no NS interno. Primeiro, é necessário criar a zona DNS pinpoint, depois o SRV dentro da zona.

> O registro SRV **_cisco-uds._tcp** deve ser resolvido somente na rede interna, não no externo, e deve ser resolvido para o nome de domínio totalmente qualificado (FQDN) do(s) nó(s) CUCM com o User Data Services (UDS).

> O registro SRV **_collab-edge._tls** deve ser resolvido a partir da rede externa e é resolvido para o FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) do servidor Expressway-E.

Configurar o servidor DNS do Windows

A entrada DNS do ponto de extremidade é criada como qualquer outra zona, e seu nome deve conter o nome inteiro do SRV (por exemplo, **_cisco-uds._tcp.domain.com**). Essa etapa também pode ser executada através da Interface Gráfica do Usuário (GUI), embora o exemplo abaixo considere que a entrada DNS do ponto de extremidade ainda não foi criada.

Para adicionar o próprio registro SRV, uma ferramenta CLI deve ser usada. Você não deve adicionar um registro SRV a uma entrada DNS de ponto de extremidade por meio da GUI, pois isso não funciona. Depois de adicionados via CLI, esses registros SRV são gerenciáveis com as ferramentas regulares assim como qualquer outra entrada. A CLI do Windows apresenta dois métodos - os comandos **dnscmd** ou **PowerShell**. Ambos os exemplos a seguir criam as duas entradas DNS do ponto de extremidade e adicionam um registro SRV para **_cisco-uds._tcp**

Apenas um destes dois métodos por vez pode ser usado:

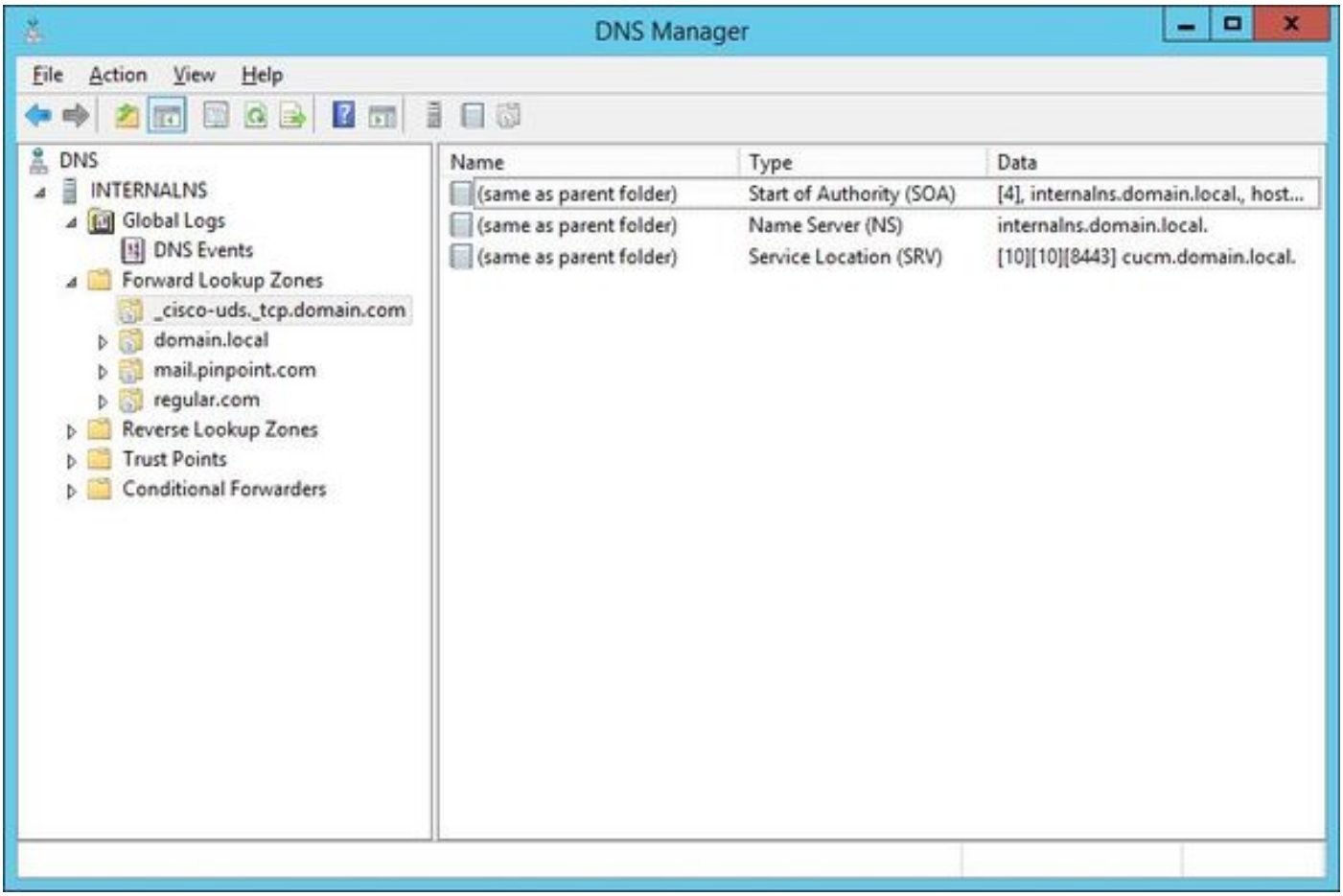
- exemplo 1 - usando **dnscmd**

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

- exemplo 2 - usando comandos **PowerShell** (como **dnscmd** deve ser substituído em versões futuras do Microsoft Windows Server, o **PowerShell** pode ser usado para o mesmo fim). As opções **do Escopo de Replicação** são **Domínio**, **Floresta** ou você pode configurar um arquivo com o **parâmetro -ZoneFile**, se a zona não estiver integrada ao Ative Diretory (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"
```

A imagem a seguir fornece um exemplo de como a entrada de DNS do ponto de extremidade com registro SRV se parece na GUI:



Configurar servidor BIND DNS

Com o servidor DNS BIND, a entrada DNS pinpoint é criada da mesma forma que um arquivo de zona regular.

A entrada **$ORIGIN** deve apontar para o FQDN do registro SRV (por exemplo, **_cisco-uds._tcp.domain.com**) e os registros SOA e NS são adicionados como de costume. O SRV é opcional (quer a entrada DNS pinpoint defina ou substitua o registro SRV) e o nome usado é **@** que é equivalente ao nome / ORIGEM da zona.

Aqui está um exemplo de um conteúdo de arquivo **_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.
```

Aqui está um exemplo de como **adicionar** a definição de zona ao **nome.conf**:

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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

- Use o comando **nslookup** com servidor definido para o NS interno, para verificar entradas DNS de ponto de extremidade.

Aqui está um exemplo de como procurar um nome de host do domínio pai e como procurar o registro SRV criado no 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
```

Aqui está um exemplo de como procurar um nome de host que não esteja configurado no NS interno, para verificar se as solicitações são encaminhadas conforme esperado.

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

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

- Defina o servidor para um NS público ou para o NS externo e repita as mesmas etapas. A pesquisa SRV para **_cisco-uds._tcp SRV** falha no registro.

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Se a verificação **nslookup** retornar um nome de host com partes duplicadas (por exemplo, **cucm.domain.local.domain.local**), então as entradas DNS devem ser verificadas para serem terminadas por um sinal de parada completo, caso contrário, a origem da zona seria adicionada ao nome de host resolvido.

Se houver preocupações com as entradas criadas, elas podem ser simplesmente excluídas do servidor DNS. Embora a CLI seja necessária para adicionar as entradas ao Microsoft DNS, as entradas podem ser excluídas com segurança e simplesmente na GUI.

Informações Relacionadas

Para uma implantação de vários domínios (nomes de domínio internos e externos diferentes) do MRA, consulte este documento:

Exemplo de configuração: Acesso móvel e remoto através do Expressway/VCS em uma implantação multidomínio