**Introdução**

Concluído100 XP

* 2 minutos

Aprenda a implantar e configurar a resolução de nomes com o DNS do Windows Server.

**Cenário**

A Contoso Ltda. é uma empresa de serviços financeiros sediada em Seattle e com grandes escritórios pelo mundo. A maior parte de seu ambiente de computação é executado localmente no Windows Server. Isso inclui as cargas de trabalho virtualizadas nos hosts do Windows Server 2016.

A equipe de TI da Contoso está migrando os servidores Contoso locais para o Windows Server 2022. Como administrador de infraestrutura do Windows Server, você é responsável por gerenciar e manter a infraestrutura de rede do Windows Server que ajudará a Contoso a atingir seus objetivos comerciais. Isso inclui a configuração e o gerenciamento da resolução de nomes usando o DNS.

Depois de concluir este módulo, você saberá como configurar e gerenciar servidores DNS no Windows Server.

**Objetivos de aprendizagem**

Depois de concluir este módulo, você poderá:

* Descreva o DNS do Windows Server.
* Descreva as zonas e os registros DNS.
* Instale e configure a função e as zonas DNS.
* Descreva como implementar o encaminhamento de DNS.

**Pré-requisitos**

Para realizar este módulo com sucesso, você deve ter conhecimento e experiência em:

* Conceitos e tecnologias do AD DS (Active Directory Domain Services).
* Windows Server.
* Principais tecnologias de rede.
* Sistemas operacionais do cliente Windows, como Windows 10.
* Noções básicas do Windows PowerShell.

# Conheça a arquitetura de DNS

Concluído100 XP

* 10 minutos

É essencial que a equipe de infraestrutura de TI da Contoso faça o planejamento e a implementação da resolução de nomes com cuidado para dar suporte a seus aplicativos e serviços. Além dos aplicativos e serviços organizacionais, a comunicação de rede geral e o AD DS também requerem o DNS como um serviço de rede crítico.

A resolução de nomes é o processo de conversão de nomes de computador em endereços IP. Ela é parte essencial da rede de computador porque é mais fácil para os usuários lembrar nomes do que números abstratos, como um endereço IPv4 ou IPv6. O Windows dá suporte a vários métodos diferentes para resolver nomes de computador, tendo o DNS como o principal.

## O que é o DNS?

O DNS é um serviço de resolução de nomes padrão do setor. Os servidores que executam a função de servidor DNS respondem a solicitações de hosts e de outros dispositivos de rede para resolver nomes de computadores e de hosts gerando endereços IP. Os servidores DNS também podem resolver endereços IP em nomes. Eles usam registros de recursos DNS armazenados em zonas DNS. Quando um servidor DNS não consegue resolver uma consulta para um dispositivo de rede, ele pode fazer referência a outros servidores DNS usando dicas de raiz ou encaminhamento.

**Observação**

O formato exato da zona depende de seu tipo.

Os registros de recursos DNS podem ser criados manualmente ou os hosts de IP e dispositivos de rede podem registrar seus registros DNS automaticamente em um servidor DNS.

O uso mais comum do DNS é a resolução de FQDNs (nomes de domínio totalmente qualificados), como sea-dc1.contoso.com, para endereços IP. Os usuários precisam dessa funcionalidade para acessar recursos de rede e sites.

Os administradores usam a resolução de nomes no DNS ao configurar e gerenciar aplicativos, em parte porque as pessoas podem lembrar nomes mais facilmente do que endereços IP. Os clientes e servidores Windows conectados ao domínio também usam o DNS para localizar controladores de domínio em um domínio AD DS.

## Nome de domínio DNS

A estrutura de nomenclatura usada pelo DNS é o namespace DNS. Ele é hierárquico, o que significa que começa com um domínio raiz. Esse domínio raiz pode ter qualquer número de subdomínios. Cada subdomínio pode, por sua vez, ter qualquer número de subdomínios próprios.

Os nomes de domínio podem ser públicos (para a Internet) ou privados. Se forem privados, você decidirá como definir o namespace de sua organização. Se forem públicos, você deverá trabalhar com a Internet Corporation para ICANN (nomes e números atribuídos) ou outras autoridades de registro de nomenclatura na Internet que possam delegar (vender) nomes exclusivos a você. Com esses nomes, você pode criar nomes de subdomínio apropriados.

**Dica**

É comum usar um nome de domínio público registrado na Internet para obter certificados confiáveis para aplicativos e autenticações.

## Servidores DNS

Um servidor DNS responde a solicitações de registros DNS feitas por resolvedores de DNS. Por exemplo, um cliente do Windows 10 pode enviar uma solicitação DNS para resolver sea-dc1.contoso.com para um servidor DNS e a resposta desse servidor inclui o endereço IP de sea-dc1.contoso.com.

Um servidor DNS recupera essas informações de um banco de dados local que contém registros de recursos. Como alternativa, se o servidor DNS não tiver as informações solicitadas, ele poderá encaminhar solicitações DNS para outro servidor desse tipo. Um servidor DNS também armazena em cache as informações solicitadas anteriormente por outros servidores DNS.

Embora seja possível configurar qualquer servidor Windows como um servidor DNS, também é comum instalar a função de servidor DNS em qualquer computador Windows Server promovido a um controlador de domínio do AD DS.

**Observação**

O Windows Server é configurado para ser um servidor DNS quando você instala a função de servidor DNS.

## Registros de recursos e zonas DNS

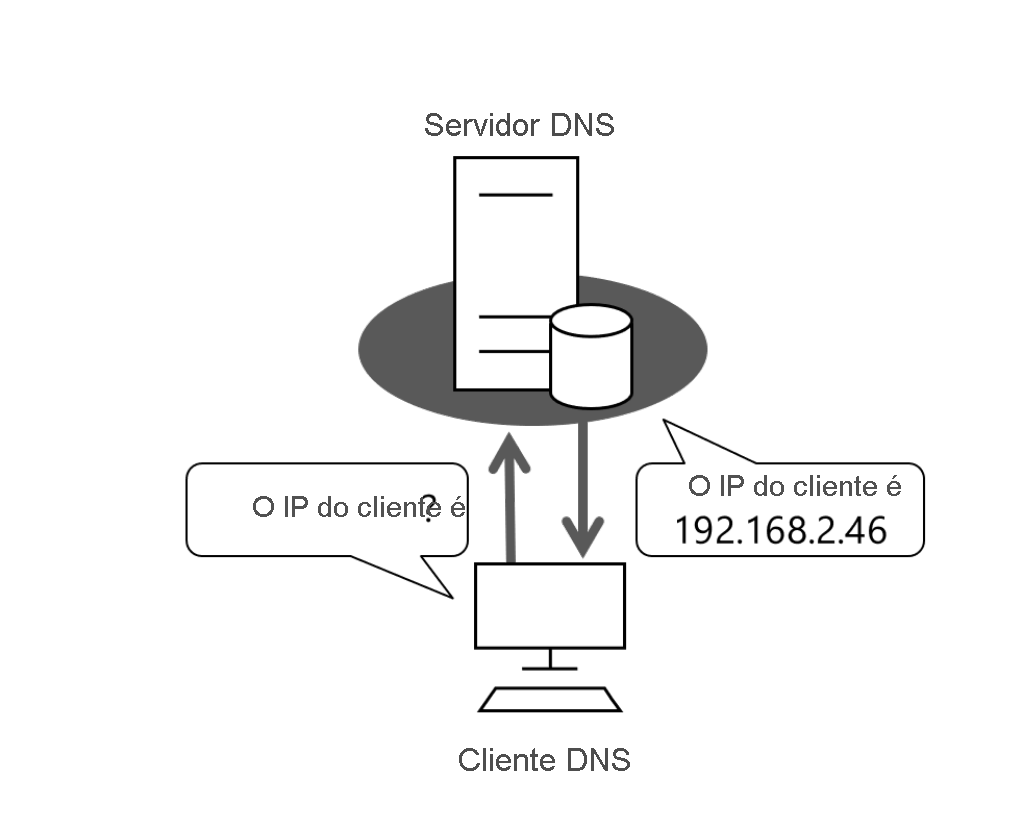
Quando um servidor DNS é responsável por resolver solicitações para um namespace específico, você cria uma zona nele que corresponda a esse namespace. Por exemplo, se um servidor DNS for responsável por contoso.com, você criará uma zona contoso.com. Na zona, você cria registros de recursos com as informações usadas para responder a consultas.

## Resolvedores de DNS

Um resolvedor de DNS é um cliente, como um cliente do Windows, que precisa resolver os registros DNS. No Windows, o serviço do cliente DNS envia solicitações DNS ao servidor DNS configurado nas propriedades de IP. Depois de receber uma resposta para uma solicitação DNS, o Windows a armazena em cache para uso futuro. Para isso, usa-se o cache do resolvedor de DNS.

**Observação**

O computador Windows 10 verifica seu cache DNS antes de fazer a solicitação ao servidor DNS, caso ele tenha resolvido recentemente o registro necessário.



**Dica**

Você pode acessar o conteúdo do cache do resolvedor de DNS usando o cmdlet Get-DnsClientCache ou executando o comando ipconfig /displaydns. Para limpar o conteúdo do cache do resolvedor de DNS, use o cmdlet Clear-DnsClientCache ou execute o comando ipconfig /flushdns.

Lembre-se de que o DNS não é a única maneira de resolver nomes em computadores host que executam o Windows. Um computador Windows 10 pode usar os seguintes métodos, de acordo com a configuração:

* Verifique o cache do resolvedor de DNS.
* Verifique o arquivo Hosts em C:\Windows\System32\Drivers\etc.
* Servidor DNS configurado por solicitação.
* Transmita uma consulta de nome NetBIOS.
* Verifique o arquivo LMHOSTS em C:\Windows\System32\Drivers\etc.
* Use um serviço configurado de resolução de nomes NetBIOS, como o WINS (serviço de cadastramento na Internet do Windows).

**Dica**

Você pode instalar o recurso do servidor WINS no Windows Server quando sua organização requer a resolução de nomes NetBIOS para dar suporte a um aplicativo específico.

### Nomes de computador e de host

Um nome de host é um nome amigável que está associado ao endereço IP de um host e que o identifica como um host TCP/IP. Ele não pode exceder 255 caracteres e deve conter apenas caracteres alfanuméricos, pontos e hifens. Um nome de host é um alias ou um FQDN. Os elementos dele incluem pontos como separadores. Os aplicativos usam o FQDN estruturado na Internet. Um exemplo de FQDN é payroll.contoso.com.

Um nome NetBIOS é um nome não hierárquico usado por alguns aplicativos mais antigos. Um nome NetBIOS de 16 caracteres identifica o recurso NetBIOS de uma rede. Um nome NetBIOS representa um único computador ou um grupo de computadores. O NetBIOS usa os primeiros 15 caracteres para o nome de um computador específico e o décimo sexto caractere final para identificar um recurso ou serviço nesse computador. Um exemplo de um nome NetBIOS é **SEA-SVR2[20h]**.

# Trabalhar com zonas e registros DNS

Concluído100 XP

* 10 minutos

A equipe de infraestrutura de TI da Contoso deve implantar o DNS para dar suporte aos seus aplicativos e serviços, incluindo o AD DS. A primeira etapa desse processo é planejar e implementar zonas DNS.

## O que é uma zona DNS?

Uma zona DNS é a parte específica de um namespace DNS (como ) que é hospedada em um servidor DNS. Essa zona contém registros de recursos e o servidor DNS responde a consultas de registros nesse namespace. Por exemplo, um servidor DNS autoritativo quanto à resolução de www.contoso.com para um endereço IP conterá a zona Contoso.com.

A equipe de infraestrutura de TI da Contoso pode optar por armazenar o conteúdo da zona DNS Contoso.com em um arquivo ou no banco de dados AD DS.

**Observação**

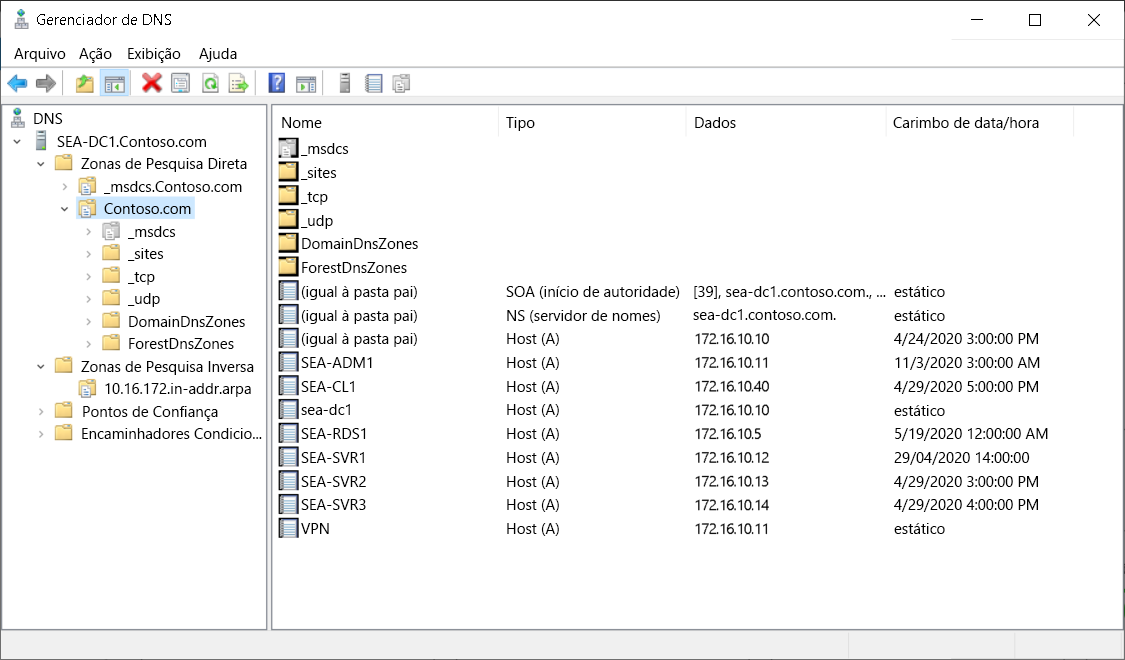
No caso de um servidor DNS que também é um controlador de domínio do AD DS, você só pode optar por armazenar as zonas no banco de dados AD DS.

Quando o servidor DNS armazena a zona em um arquivo:

* Esse arquivo está em uma pasta local no servidor.
* Somente uma cópia da zona é gravável.
* As outras, que são somente leitura, são chamadas de zonas secundárias.

### Zonas de pesquisa direta

As zonas de pesquisa direta podem conter uma ampla variedade de registros de recursos diferentes, mas o tipo mais comum é o registro de host (A). Um registro de host é usado para resolver um nome de host para um endereço IP.



Ao usar o AD DS, os servidores DNS internos de sua organização têm uma zona que corresponde ao domínio do AD DS. Por exemplo, se o nome de domínio do AD DS for Contoso.com, também haverá uma zona DNS Contoso.com. O AD DS armazena os registros de recursos que os servidores e clientes do Windows usam para localizar serviços de rede.

**Dica**

Você não precisa disponibilizar na Internet os registros DNS que contêm as informações dos recursos do AD DS. Na verdade, você não deve fazer isso.

Ao fornecer a clientes da Internet a resolução de nomes para uma zona, é possível hospedá-la em um servidor Windows acessível na Internet.

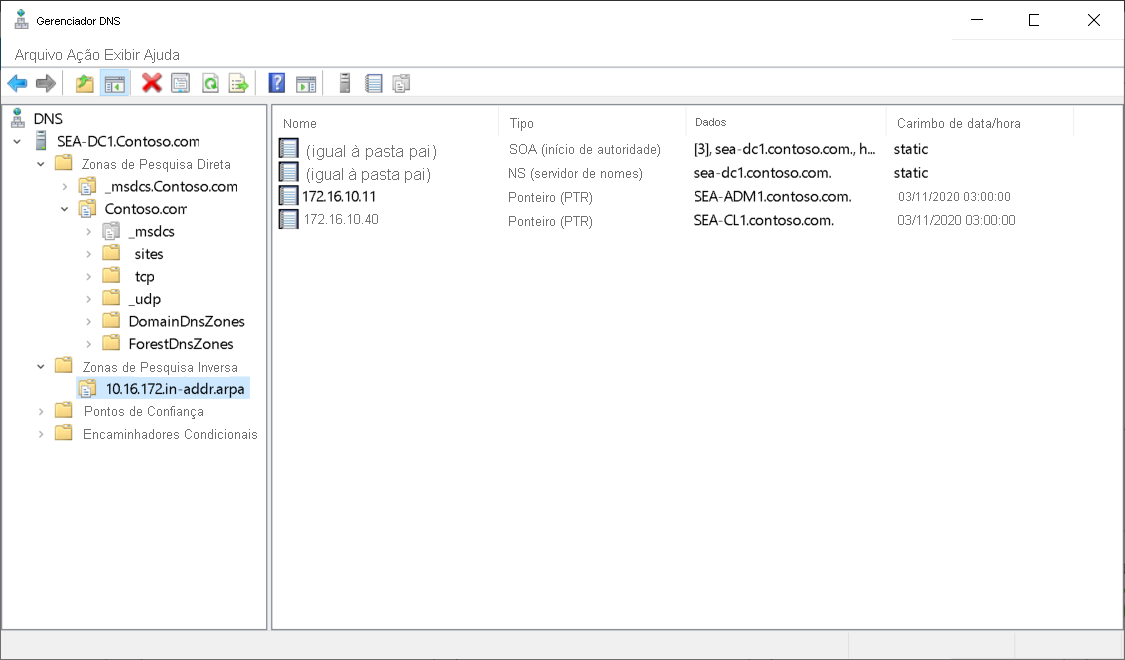
**Dica**

Outra opção é posicionar seus servidores DNS para Internet na rede de perímetro.

Você também pode hospedar a zona em um serviço DNS de terceiros que seja especializado em fornecer a resolução de nomes de Internet.

### Zonas de pesquisa inversa

As zonas de pesquisa inversa são usadas apenas para resolver um endereço IP para um nome. Essa funcionalidade é usada por diversos aplicativos e, muitas vezes, por administradores. Por exemplo, um administrador pode observar um endereço IP específico em um arquivo de log e usar uma pesquisa inversa para identificar o nome do computador que corresponde a ele.



Você cria zonas de pesquisa inversa apenas para intervalos de endereços IP de sua responsabilidade.

**Dica**

Como prática recomendada, você deve criar zonas de pesquisa inversa para todos os intervalos de endereços IP em sua rede interna e hospedá-las em seus servidores DNS internos.

O nome das zonas de pesquisa inversa termina com in-addr.arpa e é baseado no intervalo de endereços IPv4. Por exemplo, o nome da zona de pesquisa inversa 172.16.35.0/24 será 35.16.172.in-addr.arpa.

**Dica**

As zonas de pesquisa inversa são sempre baseadas em um octeto completo do endereço IP.

### Zonas primárias e secundárias

Ao criar uma zona em um servidor DNS, você deve identificar se ela é primária ou secundária. Para criar, editar ou excluir registros de recursos, use a zona primária. Como uma zona secundária é uma cópia somente leitura de uma zona primária, você não pode gerenciar os registros de recursos nela.

Na maioria dos casos, essas zonas copiam periodicamente os registros de recursos diretamente da zona primária. Mas, em algumas configurações complexas, uma zona secundária pode copiar registros de recursos de outra zona secundária.

Você pode armazenar uma zona primária padrão em um arquivo local ou armazenar dados de zona no AD DS. Ao armazenar dados de zona no AD DS, a zona é chamada de integrada ao Active Directory e habilita recursos adicionais, como atualizações dinâmicas seguras.

**Observação**

As zonas integradas ao Active Directory estão disponíveis somente em controladores de domínio com a função de servidor DNS instalada. A maioria dos servidores DNS baseados em Windows usa zonas integradas ao Active Directory.

## O que são registros DNS?

Os registros DNS são registros de recursos armazenados em zonas DNS. Eles contêm as informações que os servidores DNS enviam em resposta às solicitações de DNS. Todas as zonas DNS de pesquisa direta e inversa contêm os seguintes registros:

* SOA (início de autoridade). Contém informações de configuração para a zona, como o nome do servidor DNS primário e a frequência de sincronização dos servidores secundários. Há um registro SOA por zona.
* NS (servidor de nomes). Identifica um servidor DNS para o domínio. Há um registro NS para cada servidor DNS com uma cópia da zona.

### Registros de recursos em zonas de pesquisa direta

A tabela a seguir descreve alguns dos registros de recursos disponíveis em zonas de pesquisa direta.

| **Tipos de registro DNS** | **Descrição** |
| --- | --- |
| Host (A) | Usado para resolver um nome para um endereço IPv4. |
| Host (AAAA) | Usado para resolver um nome para um endereço IPv6. |
| Alias (CNAME) | Usado para resolver um nome para outro nome. Por exemplo, um alias pode resolver app.contoso.com para sea-svr1.contoso.com. |
| Local de serviço (SRV) | Usado por aplicativos para identificar o local dos servidores que hospedam esse aplicativo. Por exemplo, o AD DS usa os registros SRV para identificar o local dos controladores de domínio e dos serviços relacionados. |
| Servidor de mensagens (MX) | Usado para identificar servidores de email para um domínio. |
| Texto (TXT) | Usado para armazenar cadeias arbitrárias de informações no DNS. |

### Registros de recursos em zonas de pesquisa inversa

O tipo de registro mais comum criado em zonas de pesquisa inversa é o de ponteiro (PTR). Um registro de ponteiro é usado para resolver um endereço IP para um nome. Por exemplo, ele pode ser usado para resolver o endereço IP 172.16.35.100 para filesrv.contoso.com. Esse registro receberia o nome 100 e estaria na zona 35.16.172.inaddr.arpa.

### Vida útil

Todos os registros de recursos são configurados com TTL (vida útil). A TTL de um registro de recurso define por quanto tempo os clientes e servidores DNS podem armazenar em cache uma resposta DNS para ele. Por exemplo, se um registro tiver uma TTL de 60 minutos, quando um cliente fizer uma consulta DNS para ele, a resposta será armazenada em cache por 60 minutos. Se o cliente tentar usar o nome consultado e resolvido dentro de 60 minutos, o registro em cache será usado.

**Dica**

Ao solucionar problemas de registros DNS em cache, pode ser necessário limpar o cache no cliente e no servidor DNS usados pelo cliente.

# Instalar e configurar a função DNS

Concluído200 XP

* 12 minutos

Você pode criar e configurar zonas DNS com o Windows Admin Center, o Gerenciador de DNS e o Windows PowerShell. No momento, o Windows Admin Center fornece acesso às opções mais configuradas pelos usuários, como atualizações dinâmicas e armazenamento de zona. Outros recursos, como vencimento e limpeza, só são configuráveis usando o Gerenciador de DNS e o Windows PowerShell.

## Criar zonas

Ao criar uma zona primária, você pode criar um arquivo de zona ou armazená-la no AD DS. Ao criar um arquivo de zona, ela será uma zona primária padrão. Ao armazenar a zona no AD DS, ela será integrada ao Active Directory. Uma zona secundária é sempre armazenada em um arquivo de zona.

Ao configurar uma zona integrada ao Active Directory, os dados dela são armazenados no AD DS e replicados em controladores de domínio. É possível escolher um das seguintes opções:

* **Para todos os servidores DNS sendo executados em controladores de domínio nesta floresta**. Útil em uma floresta de vários domínios quando você deseja que a zona esteja disponível para servidores DNS em todos os domínios. Ao selecionar essa opção, a zona DNS é armazenada na partição ForestDnsZones.
* **Para todos os servidores DNS sendo executados em controladores de domínio neste domínio**. Selecionado por padrão e ideal para ambientes de domínio único. Ao selecionar essa opção, a zona DNS é armazenada na partição DomainDnsZones.
* **Para todos os controladores de domínio neste domínio (para compatibilidade com o Windows 2000)**. Raramente selecionado porque a replicação em todos os controladores do domínio é menos eficiente do que a replicação somente em servidores DNS sendo executados neles. Ao selecionar essa opção, a zona DNS é armazenada na partição de domínio.
* **Para todos os controladores de domínio no escopo desta partição de diretório**. Use esta opção para selecionar uma partição de aplicativo criada para o armazenamento da zona.

**Dica**

Para partições personalizadas de aplicativo, você pode especificar os controladores de domínio na floresta na qual a zona é replicada.

### Transferências de zona

Os registros de zona são sincronizados de uma zona primária para uma secundária por meio de uma transferência de zona. É possível controlar, para cada zona, quais servidores hospedando zonas secundárias podem solicitar uma transferência de zona. Ao permitir transferências de zona, é possível controlá-las com as seguintes opções:

* Para qualquer servidor
* Somente para servidores listados na guia Servidores de nomes
* Somente para os servidores a seguir

Você também pode configurar notificações para transferências de zona. Quando as notificações são habilitadas, o servidor primário notifica o servidor secundário quando alterações estão disponíveis para sincronização.

**Observação**

Após a conclusão da replicação inicial de uma zona secundária, ocorrerão transferências de zona incrementais.

### Segurança para atualizações dinâmicas

Você pode configurar cada zona DNS com configurações de segurança para atualizações dinâmicas. Para zonas integradas ao Active Directory, você pode restringir a zona para permitir apenas atualizações dinâmicas seguras. Essas atualizações garantem que apenas o cliente que tem um registro DNS possa atualizá-lo. Se um segundo dispositivo com o mesmo nome tentar realizar uma atualização dinâmica segura, o registro não será atualizado.

**Importante**

Quando uma zona não está integrada ao Active Directory, ainda é possível permitir atualizações dinâmicas, mas não é possível impor a segurança.

**Dica**

Somente os computadores Windows conectados ao domínio que fazem parte da mesma floresta podem executar essas atualizações. Para permitir que clientes do Windows não conectados ao domínio ou que dispositivos que não são Windows executem atualizações dinâmicas, você deve permitir atualizações dinâmicas não seguras.

### Cmdlets do Windows PowerShell para gerenciar zonas DNS

Há muitos cmdlets do Windows PowerShell que você pode usar para gerenciar as zonas DNS. A tabela a seguir lista alguns dos métodos que podem ser usados.

| **Cmdlet** | **Descrição** |
| --- | --- |
| Add-DnsServerPrimaryZone | Criar uma zona DNS primária |
| Add-DnsServerSecondaryZone | Criar uma zona DNS secundária |
| Get-DnsServerZone | Exibir informações de configuração de uma zona DNS |
| Get-DnsServerZoneAging | Exibir a configuração de vencimento de uma zona DNS |
| Remove-DnsServerZone | Remover uma zona DNS |
| Restore-DnsServerPrimaryZone | Recarregar o conteúdo da zona do AD DS ou de um arquivo de zona |
| Set-DnsServerPrimaryZone | Modificar as configurações de uma zona DNS primária |
| Start-DnsServerZoneTransfer | Disparar uma transferência de zona para uma zona DNS secundária |

## Criar registros no DNS

Você deve criar registros de recursos DNS para usá-los na resolução de nomes da infraestrutura de DNS. Ao criar um registro de recurso DNS, ele passa a existir em uma zona DNS. Essa zona constitui vários registros relacionados. Você pode criar registros DNS manualmente em uma zona, mas a maioria dos registros de recursos de host e de ponteiro de servidores e clientes Windows são criados dinamicamente.

### Criação manual

É possível criar registros de recursos manualmente para dar suporte a um serviço ou aplicativo específico. Por exemplo, você pode criar registros de host ou CNAME, como app.contoso.com, para um aplicativo específico em execução em um servidor. O nome do registro pode ser mais fácil de lembrar para os usuários e eles não precisam fazer referência ao nome do servidor.

Você pode criar registros de recursos usando o Gerenciador de DNS, o Windows Admin Center ou o Windows PowerShell. A tabela a seguir lista alguns cmdlets do Windows PowerShell que podem ser usados na criação de registros de recursos DNS.

| **Cmdlet** | **Descrição** |
| --- | --- |
| Add-DnsServerResourceRecord | Criar qualquer registro de recurso, especificado pelo tipo |
| Add-DnsServerResourceRecordA | Criar um registro de recurso de host (A) |
| Add-DnsServerResourceRecordAAAA | Criar um registro de recurso de host (AAAA) |
| Add-DnsServerResourceRecordCNAME | Criar um registro de recurso de alias CNAME |
| Add-DnsServerResourceRecordMX | Criar um registro de recurso MX |
| Add-DnsServerResourceRecordPtr | Criar um registro de recurso PTR |

### Criação dinâmica

Ao permitir atualizações dinâmicas para uma zona DNS, os clientes que usam o DNS se registram no servidor DNS. A atualização dinâmica cria registros de host e de ponteiro para eles. O DNS dinâmico facilita o gerenciamento do DNS porque, quando o DNS dinâmico está habilitado, o endereço IP atual de um computador é registrado automaticamente após uma alteração de endereço IP.

**Observação**

O serviço de cliente DHCP faz o registro mesmo que o endereço IP do cliente tenha sido obtido de um servidor estático, em vez de um DHCP.

O registro DNS dinâmico é disparado pelos seguintes eventos:

* Quando o cliente e o serviço de cliente DHCP são iniciados
* A cada 24 horas durante a execução do serviço de cliente DHCP
* Quando um endereço IP é configurado, adicionado ou alterado em qualquer conexão de rede
* Quando um administrador executa o cmdlet Register-DNSClient
* Quando um administrador executa o comando ipconfig /registerdns

**Observação**

Por padrão, os clientes DNS do Windows executam o registro DNS dinâmico.

## Demonstração

O vídeo a seguir demonstra como implementar, criar e gerenciar zonas e registros DNS com o Windows Admin Center. Veja a seguir as principais etapas do processo:

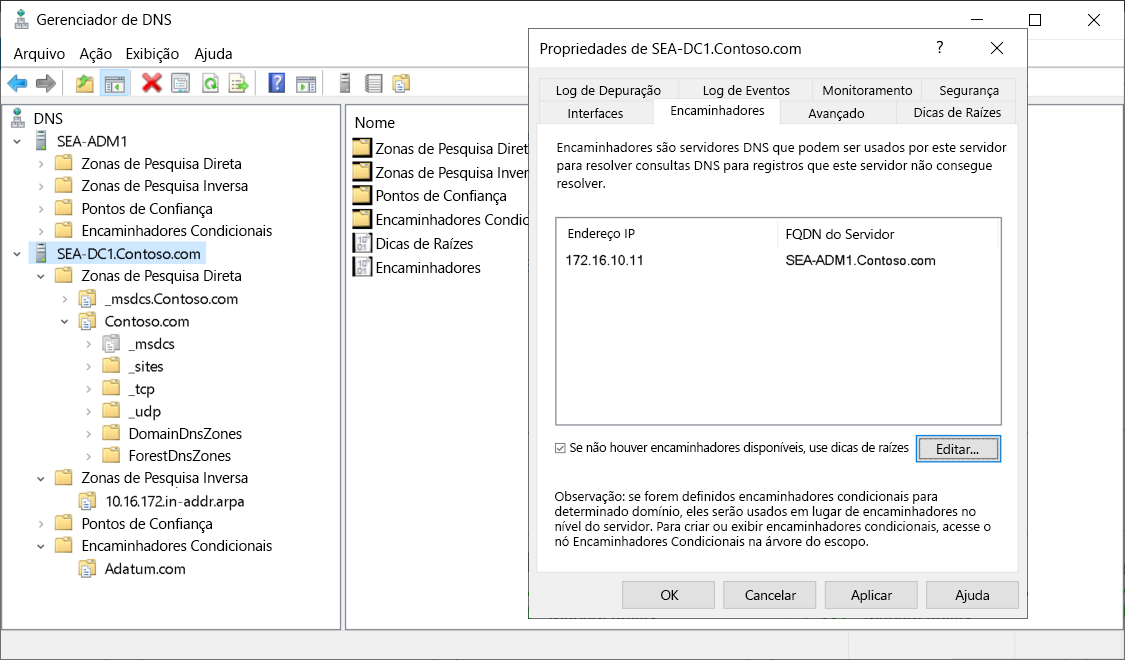
1. Abra o **Microsoft Edge** e acesse o site do **Windows Admin Center**.
2. Conecte-se ao servidor remoto apropriado.
3. No **Windows Admin Center**, selecione **Ferramentas** e depois **Funções e recursos**.
4. Instale a função de servidor DHCP.
5. No novo servidor, crie uma zona DNS. Defina as propriedades a seguir:
   * Tipo de zona
   * Nome da zona
   * Arquivo de zona
   * Atualização dinâmica
6. Na nova zona, crie um registro de host.
7. Abra o **Windows PowerShell**e verifique se a resolução de nomes foi bem-sucedida para o novo registro da nova zona usando o cmdlet .

# Implementar o encaminhamento DNS

Concluído100 XP

* 7 minutos

Quando um servidor DNS não hospeda uma zona primária ou secundária com os registros de recursos de uma solicitação de DNS, ele precisa de um mecanismo para localizar as informações necessárias. Por padrão, cada um desses servidores é configurado com dicas de raiz que podem ser usadas para resolver solicitações de DNS na Internet por meio da localização de servidores DNS autoritativos. Isso funcionará se o servidor DNS tiver acesso à Internet e o registro de recurso sendo solicitado estiver disponível nela. Às vezes, nenhuma das condições é atendida. Nesses casos, habilite o encaminhamento.



## Encaminhadores

Você pode configurar cada servidor DNS com um ou mais encaminhadores. Se um servidor DNS receber uma solicitação de uma zona para a qual não é autoritativo e que ainda não foi armazenada em cache pelo servidor, ele encaminhará essa solicitação a um encaminhador. Esse tipo de servidor usa um encaminhador para todas as zonas desconhecidas.

Os encaminhadores normalmente são usados para a resolução de nomes de Internet. Os servidores DNS internos encaminham a um servidor DNS que está fora da rede corporativa solicitações para resolver nomes de Internet. Sua organização pode configurar os servidores DNS externos em uma rede de perímetro ou usar um servidor DNS fornecido por seu provedor de serviços de Internet. Essa configuração limita a conectividade externa e aumenta a segurança.

## Encaminhamento condicional

Você pode configurar o encaminhamento condicional para domínios DNS individuais. O processo é semelhante à configuração de um encaminhador, mas se aplica somente a um único domínio DNS. Organizações parceiras e florestas do AD DS confiáveis geralmente usam esse recurso.

Ao criar um encaminhador condicional, você pode escolher se deseja armazená-lo localmente em um único servidor DNS ou no AD DS. Ao armazená-lo no AD DS, ele poderá ser replicado em todos os servidores DNS em execução nos controladores de domínio do domínio ou da floresta, de acordo com a opção selecionada. É mais fácil gerenciar encaminhadores condicionais em vários servidores DNS ao armazená-los no AD DS.

### Zonas de stub

A finalidade de uma zona de stub é fornecer uma lista de servidores de nomes que podem ser usados para resolver informações de um domínio sem sincronizar todos os registros localmente. Para habilitar essa opção, os itens a seguir são sincronizados:

* Registros do servidor de nomes
* Registros de host correspondentes para os servidores de nomes
* Registro SOA

**Dica**

Normalmente, as zonas de stub são usadas na integração com sistemas autônomos, como organizações parceiras.

## Comparando zonas de stub e encaminhadores condicionais

Para resolver solicitações de DNS para zonas para as quais o servidor DNS local não é autoritativo, use zonas de stub ou encaminhadores condicionais. A diferença entre eles está na seleção dos servidores remotos para a consulta:

* Você configura um encaminhador condicional com servidores DNS remotos específicos que são autoritativos para o domínio.
* Uma zona de stub replica e usa todos os registros do servidor de nomes configurados na zona.

Se houver probabilidade de os servidores DNS autoritativos mudarem com o tempo, use uma zona de stub que atualize automaticamente os registros do servidor de nomes e use apenas servidores de nomes válidos para a zona. No entanto, se firewalls controlarem a comunicação, os servidores de nomes atualizados poderão não estar acessíveis.