**Introdução**

Concluído100 XP

* 2 minutos

Saiba como proteger o DNS do Windows Server para proteger sua infraestrutura de resolução de nomes de rede e também como implementar políticas de DNS.

**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 gerencia e mantém a infraestrutura de rede do Windows Server que ajudará a Contoso a atingir suas metas de negócios.

Depois de concluir este módulo, você saberá como proteger seus servidores DNS do Windows Server e como implementar políticas de DNS.

**Objetivos de aprendizagem**

Depois de concluir este módulo, você poderá:

* Descrever a omissão de rotas do DNS e explicar como implementá-la.
* Criar políticas de DNS.
* Implementar políticas de DNS.
* Descrever as opções para proteger a função do servidor DNS.
* Implementar segurança de DNS.

**Pré-requisitos**

Para ter uma experiência melhor de aprendizagem deste módulo, você precisa conhecer e ter experiência em:

* Conceitos e tecnologias do AD DS.
* Função DNS do Windows Server.
* Principais tecnologias de rede.
* Melhores práticas de segurança básica.
* Noções básicas do Windows PowerShell.

**Implementar omissão de rotas do DNS**

Concluído100 XP

* 10 minutos

Em sistemas operacionais do Windows, o DNS tem duas funções principais: determinar endereços IP para nomes (e vice-versa) e facilitar a comunicação e a autenticação no nível de domínio do AD DS. A capacidade de armazenar os registros do SRV permite que clientes membros do domínio encontrem controladores de domínio para autenticação e segurança enquanto equilibram o acesso a vários controladores de domínio usando a funcionalidade round robin do DNS.

No entanto, usuários não confiáveis no nível da Internet de fora do firewall nunca devem acessar os registros do SRV e outras informações confidenciais do AD DS dos servidores DNS internos. Esses dados devem permanecer separados e inacessíveis de fora do firewall. Ao mesmo tempo, os registros do DNS de servidores e serviços que hospedam recursos de nível da Internet, como servidores Web, de email e proxy, devem permanecer acessíveis.

Esse é o problema enfrentado pelos engenheiros de infraestrutura da Contoso. Eles devem determinar uma maneira conveniente de gerenciar esse problema.

**O que é um DNS dividido?**

O *DNS dividido*, também conhecido como omissão de rotas do DNS, usa o mesmo nome de domínio DNS para recursos de membro de domínio interno e da Internet. No entanto, a função de servidor DNS é atribuída a servidores separados: um ou mais servidores para a Internet e outros servidores para o domínio AD DS. Implantar o DNS dessa forma requer etapas adicionais para garantir que as informações confidenciais encontradas no lado do domínio AD DS sejam separadas do lado da Internet e para garantir que apenas o servidor DNS implantado no lado da Internet, ou seja, fora do firewall interno, possa ser acessado por consultas de fora do firewall.

**Observação**

Como o DNS é uma função fundamental para o AD DS, a função de servidor DNS geralmente é incluída com controladores de domínio quando eles são implantados.

Você pode integrar a função DNS no AD DS para que os registros do DNS sejam armazenados como objetos e atributos do Active Directory. O tipo de zona DNS nessa instância é conhecida como zona integrada ao Active Directory. As zonas integradas ao Active Directory substituem as transferências da zona DNS pela replicação do AD DS e podem garantir atualizações dinâmicas seguras de registros de cliente para a zona. Em um domínio, o uso do DNS integrado ao Active Directory é uma prática recomendada.

Com o DNS dividido, os clientes internos são configurados apenas com os endereços IP dos servidores DNS integrados ao Active Directory, que são controladores de domínio. Todas as atualizações dinâmicas de DNS de cliente são gravadas nos controladores de domínio. Todas as consultas DNS de clientes internos vão apenas para esses servidores DNS.

Se uma resolução de nomes for necessária além do domínio interno, como para servidores Web da Internet, você deverá criar esses registros manualmente ou usar políticas DNS para determinar como essas consultas são resolvidas.

**Observação**

Normalmente, você implanta servidores DNS para a Internet na rede de perímetro entre os firewalls.

Embora os servidores DNS para a Internet tenham o mesmo nome de domínio que os servidores DNS integrados ao Active Directory, os servidores DNS para a Internet não armazenam os mesmos dados. Todos os registros na zona do servidor DNS para a Internet são criados manualmente.

**Dica**

Normalmente, a zona do servidor DNS para a Internet contém apenas registros para si mesmo e outros servidores localizados na rede do perímetro e que precisam ser acessados pela Internet.

Quando uma consulta ao servidor DNS para a Internet vem da Internet solicitando uma resolução de um recurso de nível de domínio, como um registro de SRV, o servidor DNS para a Internet rejeita a consulta porque ela não tem nenhum dos registros de SRV — eles são armazenados apenas nos servidores DNS integrados ao domínio Active Directory. Como ele se considera autoritativo para a zona, o servidor DNS para a Internet não faz uma consulta iterativa para os servidores DNS integrados ao Active Directory.

**Dica**

Para aumentar ainda mais a segurança, você pode definir uma regra de firewall no firewall interno, ou seja, o firewall entre as redes internas e de perímetro, pode rejeitar todas as consultas DNS (TCP e UDP porta 53) do perímetro para a rede interna e, ao mesmo tempo, permitir respostas DNS.

**Implementar DNS dividido**

Usar o mesmo namespace interna e externamente simplifica o acesso aos recursos da perspectiva dos usuários, mas também aumenta a complexidade do gerenciamento. Você não deve tornar os registros DNS internos disponíveis externamente, mas normalmente é necessária sincronização de registros para recursos externos. Por exemplo, os namespaces internos e externos podem usar o nome Contoso.com.

O uso de namespaces exclusivos para os namespaces interno e público fornece um delineamento claro entre o DNS interno e o externo e evita a necessidade de sincronizar registros entre os namespaces. No entanto, em alguns casos, ter vários namespaces pode confundir o usuário. Por exemplo, você pode escolher o namespace externo de Contoso.com e o namespace interno de Contoso.local.

**Dica**

Ao implementar uma configuração de namespace exclusiva, você não precisa mais usar nomes de domínio registrados.

O uso de um subdomínio do namespace público para o AD DS evita a necessidade de sincronizar registros entre os servidores DNS internos e externos. Como os namespaces são vinculados, normalmente os usuários acham essa estrutura fácil de reconhecer. Por exemplo, se o seu namespace público for Contoso.com, você pode optar por implementar seu namespace interno como um subdomínio do AD ou como AD.Contoso.com.

**Considerações sobre DNS dividido**

Ter um namespace DNS interno e externo correspondente pode trazer certos problemas. No entanto, o DNS dividido pode fornecer uma solução para esses problemas. O DNS dividido é uma configuração na qual seu domínio tem duas zonas de servidor raiz que contêm informações de registro de nome de domínio.

Os hosts de rede interna são direcionados para uma zona e os hosts externos são direcionados para outra, para resolução de nomes. Por exemplo, em uma configuração de DNS não dividido para o domínio contoso.com, você pode ter uma zona DNS parecida com o exemplo na tabela a seguir.

| **Host** | **Tipo de registro** | **Endereço IP** |
| --- | --- | --- |
| www | Um | 131.107.1.200 |
| Retransmissão | Um | 131.107.1.201 |
| WebServer1 | Um | 192.168.1.200 |
| Exchange1 | Um | 192.168.0.201 |

Quando um computador cliente na Internet deseja acessar a retransmissão SMTP usando o nome publicado de relay.contoso.com, ele consulta o servidor DNS que retorna o resultado 131.107.1.201. Então o cliente estabelece uma conexão via SMTP com esse endereço IP.

No entanto, os computadores cliente na intranet da organização também usam o nome publicado de relay.contoso.com. O servidor DNS retorna o mesmo resultado: um endereço IP público de 131.107.1.201. O cliente tenta estabelecer uma conexão com esse endereço IP usando a interface externa do computador de publicação. Dependendo da configuração do cliente, isso pode ser bem-sucedido ou não.

Ao configurar duas zonas para o mesmo nome de domínio — uma em cada um dos dois servidores DNS – você pode evitar esse problema.

A zona interna para Contoso.com contém as informações na tabela a seguir.

| **Host** | **Tipo de registro** | **Endereço IP** |
| --- | --- | --- |
| www | CNAME | Webserver1.contoso.com |
| Retransmissão | CNAME | Exchange1.contoso.com |
| WebServer1 | Um | 192.168.1.200 |
| Exchange1 | Um | 192.168.0.201 |

A zona externa para Contoso.com contém as informações na tabela a seguir.

| **Host** | **Tipo de registro** | **Endereço IP** |
| --- | --- | --- |
| www | Um | 131.107.1.200 |
| Retransmissão | Um | 131.107.1.201 |
|  | MX | Relay.contoso.com |

Agora, os computadores cliente nas redes internas e externas podem resolver o nome relay.contoso.com para o endereço IP interno ou externo apropriado.

**Criar políticas de DNS**

Concluído100 XP

* 10 minutos

A equipe de infraestrutura da Contoso tem uma pergunta: "Como o DNS do Windows Server lida com o fato de que queremos que resultados diferentes para a mesma consulta sejam retornados aos resolvedores de DNS com base nas respectivas localizações?". Eles explicaram que para os usuários em Seattle, a consulta ao FQDN www.Contoso.com deve retornar um endereço IP diferente do que para os usuários em Londres.

**Cenários para usar políticas DNS**

Você pode usar as políticas de DNS para manipular como um servidor DNS gerencia consultas com base em fatores diferentes. Por exemplo, você pode criar uma política DNS para responder a consultas solicitando que o endereço IP de um servidor Web responda com um endereço IP diferente com base no datacenter mais próximo do cliente.

**Observação**

Isso difere de outras abordagens, como reordenação de máscara de rede, porque o cliente não tem o mesmo endereço de sub-rede local que o servidor Web, mas do ponto de vista do cliente, o servidor Web específico está mais próximo do que outros.

Você pode criar várias políticas de DNS dependendo de suas necessidades. Vários fatores podem se beneficiar da criação de uma política de DNS, com base nos seguintes cenários:

* Alta disponibilidade de Aplicativo. Os clientes são redirecionados para o ponto de extremidade mais íntegros de um aplicativo. O termo "mais íntegros" é determinado por fatores de alta disponibilidade em um cluster de failover.
* Gerenciamento de tráfego. Os clientes são redirecionados para a localização do datacenter ou servidor mais próximo.
* Dividir DNS. Os clientes recebem uma resposta, sendo eles internos ou externos e os registros DNS são divididos em escopos de zona diferentes.
* Filtragem. As consultas DNS são bloqueadas se forem de uma lista de endereços IP mal-intencionados ou FQDNs.
* Análises forenses. Os clientes DNS mal-intencionados são redirecionados para um sinkhole e não para o computador que estão tentando alcançar.
* Redirecionamento baseado na hora do dia. Os clientes são redirecionados para datacenters com base na hora do dia.

**Objetos da política de DNS**

Para usar os cenários mencionados anteriormente para criar políticas, você deve identificar grupos de registros em uma zona, grupos de clientes em uma rede ou outros elementos. Você pode identificar os elementos pelos objetos da política de DNS descritos na tabela a seguir.

| **Elemento** | **Descrição** |
| --- | --- |
| Sub-rede do Cliente | Representa a sub-rede IPv4 ou IPv6 a partir da qual as consultas são enviadas para um servidor DNS. Você cria sub-redes para depois definir as políticas que você aplica com base na sub-rede que gera as solicitações. Por exemplo, você pode ter um cenário de DNS dividido em que a solicitação de resolução de nomes para www.contoso.com pode ser respondida com um endereço IP interno para clientes internos e um endereço IP diferente para clientes externos. |
| Escopo da recursão | Representa instâncias exclusivas de um grupo de configurações que controlam a recursão do servidor DNS. Um escopo de recursão contém uma lista de encaminhadores e especifica se a recursão é usada. Um servidor DNS pode ter vários escopos de recursão. Você pode usar as políticas de recursão do servidor DNS para escolher um escopo de recursão para um determinado conjunto de consultas. Se o servidor DNS não for autoritativo para determinadas consultas, as políticas de recursão do servidor DNS permitirão que você controle a resolução dessas consultas. Nesse caso, você pode especificar quais encaminhadores usar e se a recursão deve ser usada. |
| Escopos de zona | As zonas DNS podem ter vários escopos de zona, e cada escopo de zona pode conter seu conjunto de registros de recursos de DNS. O mesmo registro de recurso pode estar presente em vários escopos, com endereços IP diferentes, dependendo do escopo. Além disso, as transferências de zona podem ocorrer no nível de escopo da zona. Isso permitirá que os registros de recursos de um escopo de zona em uma zona primária sejam transferidos para o mesmo escopo de zona em uma zona secundária. |

**Implementar políticas de DNS**

Concluído200 XP

* 10 minutos

Você cria políticas de DNS com base no nível e no tipo. Você pode usar políticas de resolução de consulta para definir como gerenciar consultas de resolução de nomes de cliente e usar políticas de transferência de zona para definir transferências de zona.

**Dica**

Você pode aplicar os dois tipos de política no nível do servidor ou da zona.

Você pode criar várias políticas de resolução de consulta no mesmo nível, se elas tiverem um valor diferente para a ordem de processamento. As políticas de recursão são um tipo especial de política de nível de servidor. Elas controlam como um servidor DNS executa a recursão de consulta. As políticas de recursão se aplicam somente quando o processamento da consulta chega ao ponto de recursão. Você pode escolher um valor de NEGAR ou IGNORAR para recursão em um determinado conjunto de consultas. Caso contrário, você pode escolher um conjunto de encaminhadores em um conjunto de consultas.

**Criar e gerenciar políticas de DNS**

Estas são as etapas de alto nível para resolver um registro de host de forma diferente para os usuários de um intervalo de endereços IP específico:

1. Criar uma sub-rede de cliente do servidor DNS para o intervalo de endereços IP.
2. Criar um escopo de zona do servidor DNS para a zona que contém o registro do host.
3. Adicionar um registro de host à zona que é específica para o escopo da zona.
4. Adicionar uma política de resolução de consulta do servidor DNS que permita que a sub-rede do cliente do servidor DNS consulte o escopo da zona.

Veja a seguir um exemplo das etapas usadas para configurar a política de DNS usando o Windows PowerShell:

# Create the required subnets

Add-DnsServerClientSubnet -Name "LondonSubnet" -IPv4Subnet "172.16.18.0/24"

Add-DnsServerClientSubnet -Name "SeattleSubnet" -IPv4Subnet "172.16.10.0/24"

# Create the DNS server zone scopes

Add-DnsServerZoneScope -ZoneName "Contoso.com" -Name "LondonZoneScope"

Add-DnsServerZoneScope -ZoneName "Contoso.com" -Name "SeattleZoneScope"

# Add the required host records

Add-DnsServerResourceRecord -ZoneName "Contoso.com" -A -Name "www" -IPv4Address "172.16.10.41" -ZoneScope "SeattleZoneScope"

Add-DnsServerResourceRecord -ZoneName "Contoso.com" -A -Name "www" -IPv4Address "172.16.18.17" -ZoneScope "LondonZoneScope"

# Create the DNS server query resolution policies

Add-DnsServerQueryResolutionPolicy -Name "LondonPolicy" -Action ALLOW -ClientSubnet "eq,LondonSubnet" -ZoneScope "LondonZoneScope,1" -ZoneName "Contoso.com"

Add-DnsServerQueryResolutionPolicy -Name "SeattlePolicy" -Action ALLOW -ClientSubnet "eq,SeattleSubnet" -ZoneScope "SeattleZoneScope,1" -ZoneName Contoso.com

**Demonstração**

O vídeo a seguir monstra como implementar políticas de DNS usando o Windows PowerShell. As principais etapas do processo são:

1. Abrir o Gerenciador do Servidor e o console do DNS.
2. Criar um novo registro de alias para um servidor existente na zona Contoso.com.
3. Alternar para um computador cliente e verificar qual endereço IP retorna quando o alias é testado com o NSLookup.
4. Abrir um servidor e uma janela com privilégios elevados do Windows PowerShell.
5. Executar o $s = New-PSSession –ComputerName <target server> e o Enter-PSSession $s comando para se conectar ao <target server> com a comunicação remota do PowerShell.
6. Criar as sub-redes necessárias executando o Add-DnsServerClientSubnet cmdlet.
7. Criar os escopos de zona do servidor DNS executando o Add-DnsServerZoneScope cmdlet.
8. Adicionar os registros de host necessários executando o Add-DnsServerResourceRecord cmdlet.
9. Criar as políticas de resolução de consulta do servidor DNS executando o Add-DnsServerQueryResolutionPolicy cmdlet.
10. Voltar para o cliente, limpar o cache do resolvedor e testar a resolução de nomes para o www.Contoso.com registro.

**Proteger o DNS do Windows Server**

Concluído100 XP

* 10 minutos

Como o DNS é um serviço de rede crítico, a equipe de TI da Contoso está preocupada em proteger o serviço DNS. O DNS do Windows Server fornece várias opções para proteger a função de servidor DNS, inclusive:

* Bloqueio de Cache DNS.
* Pool de Soquetes DNS.
* DNS-Based autenticação de entidades nomeadas (DANE).
* Limitação de taxa de resposta (RRL).
* Suporte a registro desconhecido.
* DNSSEC (Extensões de Segurança de DNS).

**Bloqueio de Cache DNS**

O bloqueio de cache é um recurso de segurança do Windows Server que você pode usar para controlar quando as informações no cache DNS podem ser substituídas. Quando um servidor DNS recursivo responde a uma consulta, o servidor armazena os resultados em cache para que ele possa responder rapidamente caso receba outra consulta solicitando as mesmas informações.

O período de tempo pelo qual o servidor DNS mantém informações no cache é determinado pelo valor TTL de um registro de recurso. As informações no cache podem ser substituídas antes que o TTL expire se as informações atualizadas sobre esse registro de recurso forem recebidas. Se um usuário mal-intencionado substituir as informações no cache com êxito, então o usuário mal-intencionado poderá redirecionar o tráfego de rede para um site mal-intencionado.

Quando você usa o bloqueio de cache, o servidor DNS proíbe que os registros armazenados em cache sejam substituídos pela duração do valor TTL.

Configure o bloqueio de cache como um valor percentual. Por exemplo, se o valor de bloqueio de cache for definido como 50, o servidor DNS não substituirá uma entrada armazenada em cache pela metade da duração do TTL. Por padrão, o valor da porcentagem de bloqueio de cache é 100. Isso significa que as entradas armazenadas em cache não serão substituídas durante toda a duração do TTL.

Você pode configurar o bloqueio de cache ao executar dnscmd /Config /CacheLockingPercent <percent> em um prompt de comando com privilégios elevados.

**Dica**

Você também poderá usar o Set-DnsServerCache –LockingPercent cmdlet do Windows PowerShell

**Pool de Soquetes DNS**

O pool de soquetes DNS permite que um servidor DNS use a randomização de porta de origem ao emitir consultas DNS. Quando o serviço DNS é iniciado, o servidor escolhe uma porta de origem de um pool de soquetes disponíveis para a emissão de consultas. Em vez de usar uma porta de origem previsível, o servidor DNS usa um número de porta aleatório que ele seleciona no pool de soquetes DNS.

O pool de soquetes DNS torna os ataques de adulteração de cache mais difíceis porque um usuário mal-intencionado deve adivinhar corretamente a porta de origem de uma consulta DNS e uma ID de transação aleatória para executar o ataque com êxito.

**Observação**

O pool de soquetes DNS é habilitado por padrão no Windows Server.

Quanto maior o valor, de 0 a 10 mil, maior é a proteção que você terá contra-ataques de falsificação de DNS.

**Observação**

O tamanho padrão do pool de soquetes DNS é 2.500.

Você pode configurar o tamanho do pool de soquetes DNS executando dnscmd /Config /SocketPoolSize <value> em um prompt de comando com privilégios elevados.

**Protocolo DANE**

O protocolo DANE é um recurso disponível na função de servidor DNS do Windows Server. O DANE permite que você use registros de TLSA (autenticação de segurança de camada de transporte) para fornecer informações aos clientes DNS que preparam a AC (autoridade de certificação) da qual os clientes devem esperar um certificado para seu nome de domínio. Isso impede ataques man-in-the-Middle, nos quais alguém pode corromper o cache DNS para apontar para seu site e fornecer um certificado emitido por uma autoridade de certificação diferente.

Por exemplo, vamos supor que sua organização hospede um site seguro usando HTTPS em www.Contoso.com usando um certificado de uma autoridade conhecida chamada CANorth. Alguém ainda poderá obter um certificado para www.Contoso.com de uma autoridade de certificação diferente desconhecida, denominada CAEast.

Nesse ponto, uma entidade que hospeda um site não legítimo www.Contoso.com pode corromper o cache DNS de um cliente ou servidor para apontar www.Contoso.com sobre seu site falso. O usuário final recebe um certificado da CAEast e pode desavisadamente reconhecer e se conectar ao site falso.

Com o DANE, o cliente faz uma solicitação ao servidor DNS para Contoso.com solicitar o registro TLSA e descobre que o certificado para www.Contoso.com foi emitido pela CANorth. Se receber uma oferta de certificado de outra AC, a conexão será encerrada.

**RRL**

O RRL é um aprimoramento do protocolo DNS que pode ajudar a mitigar ataques de amplificação de DNS. Um ataque de amplificação é um tipo de DDoS (negação de serviço distribuído) em que os invasores usam servidores DNS abertos publicamente para inundar um sistema de destino com tráfego de resposta DNS. O método principal envolve um invasor enviando uma solicitação de pesquisa de nome DNS para um servidor DNS aberto com o endereço de origem falsificado para ser o endereço do destino.

Em vez disso, o servidor DNS envia a resposta de registro DNS para o destino. Você pode evitar isso habilitando o RRL nos servidores DNS. O RRL monitora constantemente as consultas DNS do cliente e caso muitas consultas sejam feitas de uma única fonte solicitando nomes semelhantes dentro de um curto período de tempo, a RRL vai sinalizar essas consultas como potencialmente mal-intencionadas. O RRL pode simplesmente ignorar as consultas ou respondê-las em truncamento, o que força o cliente a negociar um handshake TCP de três vias para confirmação.

**Suporte a registro desconhecido**

Os registros que não são explicitamente suportados pelo servidor DNS do Windows podem ser adicionados em uma zona DNS do Windows Server por meio da funcionalidade de registro desconhecido. Isso significa que você pode adicionar os tipos de registro não suportados às zonas do servidor DNS do Windows em um formato binário. Um servidor DNS do Windows Server não fará um processamento específico do registro para os registros desconhecidos, mas enviará a resolução de volta em respostas se as consultas forem recebidas para esse registro.

# Implementar DNSSEC

Concluído200 XP

* 8 minutos

Interceptar e adulterar a resposta de consulta DNS de uma organização é um método de ataque comum. Se hackers mal-intencionados puderem alterar as respostas dos servidores DNS da Contoso ou enviarem respostas falsificadas para os computadores cliente em seus próprios servidores, eles obterão acesso às informações confidenciais da Contoso. Qualquer serviço que dependa do DNS para a conexão inicial, como os servidores Web de comércio eletrônico e servidores de email — está vulnerável.

## O que é DNSSEC?

O DNSSEC previne que os clientes que estão fazendo consultas DNS aceitem respostas de DNS falsas. Quando um servidor DNS que está hospedando uma zona assinada digitalmente recebe uma consulta, o servidor retorna as assinaturas digitais com os registros solicitados. Um resolvedor ou outro servidor pode obter a chave pública do par de chaves pública/privada de uma âncora de confiança e assim validar as respostas como autênticas e não violadas. Para fazer isso, você deve configurar o resolvedor ou o servidor com uma âncora de confiança para a zona assinada ou pai da zona assinada.

Estas são as etapas de alto nível para implantar o DNSSEC:

1. Assinar a zona DNS.
2. Configurar a distribuição da âncora de confiança.
3. Configurar a NRPT (tabela de política de resolução de nomes) em computadores cliente.

### Registros de recursos

A validação de resposta DNS é obtida pela associação de um par de chaves privada/pública (conforme gerado pelo administrador) com uma zona DNS e pela definição de registros de recursos DNS adicionais para assinar e publicar chaves.

Os registros de recursos distribuem a chave pública, enquanto a chave privada permanece no servidor. Quando o cliente solicita validação, o DNSSEC adiciona dados à resposta que permite que o cliente autentique a resposta.

A tabela a seguir descreve os registros de recursos adicionais usados com o DNSSEC.

| **Registro de recurso** | **Finalidade** |
| --- | --- |
| RRSIG | Mantém uma assinatura para um conjunto de registros DNS. Os clientes DNS podem usá-lo para verificar a autoridade de uma resposta. Quando um registro de recurso é resolvido, um registro de RRSIG (assinatura de registro de recurso) é enviado para verificação. |
| DNSKEY | Publica as chaves públicas para a zona. Ele permite que os clientes validem as assinaturas criadas pela chave privada mantida pelo servidor DNS. |
| NSEC | Quando a resposta DNS não tem dados para fornecer ao cliente, o próximo registro seguro (NSEC) autentica que o host não existe. |
| NSEC3 | Uma versão resumida do registro NSEC, que impede ataques enumerando a zona. |
| DS | Um registro de delegação que contém o código hash da chave pública de uma zona filho. Esse registro é assinado pela chave privada da zona pai. Se uma zona filho de um pai assinado também estiver assinada, você deve adicionar manualmente os registros de DS (signatário de delegação) do filho ao pai para criar uma cadeia de confiança. |

## Assinar a zona DNS

O Windows Server inclui o **Assistente de Assinatura de zona** no Gerenciador DNS para simplificar o processo de configuração e assinatura e para habilitar a assinatura online. O assistente permite que você escolha os parâmetros de assinatura de zona. Se você optar por definir as configurações de assinatura de zona em vez de usar os parâmetros de uma zona existente ou usar os valores padrão, poderá usar o assistente para definir configurações como as seguintes:

* Opções de chave de assinatura principal.
* Opções de chave de assinatura de zona.
* Opções de distribuição da âncora de confiança.
* Parâmetros de assinatura e sondagem.

### Distribuição de âncoras de confiança

Uma âncora de confiança é uma entidade autoritativa que é representada por uma chave pública. A zona TrustAnchors armazena chaves públicas pré-configuradas associadas a uma zona específica. No DNS, a âncora de confiança é o registro de recurso DNSKEY ou DS. Os computadores cliente usam esses registros para criar cadeias de confiança. Você deve configurar uma âncora de confiança da zona em cada servidor DNS de domínio para validar as respostas dessa zona assinada. Todos os servidores DNS que hospedam uma zona precisam ter os mesmos registros de chave DNSKEY para fornecer as informações necessárias para validar os registros de RRSIG.

### Tabela de Políticas de Resolução de Nomes

A NRPT contém regras que controlam o comportamento do cliente DNS para enviar consultas DNS e processar as respostas dessas consultas. Por exemplo, uma regra DNSSEC solicita que o computador cliente verifique a validação da resposta para um determinado sufixo de domínio DNS. A melhor prática é ter a Política de Grupo como método preferencial de configuração da NRPT. Se nenhuma NRPT estiver presente, o computador cliente aceitará respostas sem validá-las.

### Revisar ou alterar as configurações

Depois de concluir a assinatura de zona, você pode revisar ou alterar as configurações usando este procedimento:

1. No Gerenciador DNS, clique com o botão direito do mouse ou ative o menu de contexto para zona, clique em DNSSEC e, em seguida, **Propriedades**.
2. Use as **Propriedades DNSSEC da caixa de diálogo Nome de Zona** para revisar e editar as configurações.
3. Selecione **OK** quando tiver concluído.

## Demonstração

O vídeo a seguir monstra como configurar o DNSSEC no DNS do Windows Server usando o console DNS. As principais etapas do processo são:

1. Abrir o **Gerenciador do Servidor**e o **Gerenciador de DNS**.
2. Localizar a zona de pesquisa direta apropriada, clicar com o botão direito do mouse na zona ou ativar o menu de contexto, selecionar **DNSSEC**e **Assinar a Zona**.
3. Use o **Assistente de Assinatura de Zona** para concluir o processo.
4. No Gerenciador DNS, expanda **Pontos de Confiança**. Verifique se os registros de recursos DNSKEY existem e se seu status é válido.
5. Abra **Gerenciamento de Política de Grupo**.
6. Abra um GPO adequado para edição.
7. Na Editor de Gerenciamento de Política de Grupo, em **Configuração do Computador**, entre em **PolíticasConfigurações do Windows** e**Política de Resolução de nomes**.
8. Na **seção Criar Regras**, na caixa de texto **Sufixo**, insira o sufixo de domínio apropriado.
9. Clique em **Habilitar DNSSEC nesta regra**, **Exigir que os clientes DNS verifiquem se os dados de nome e endereço foram validados pelo servidor DNS** e clique em **Criar**.