**Introdução**

Concluído100 XP

* 2 minutos

Aprenda a implementar o IPAM para ajudar a gerenciar servidores DHCP e DNS da sua organização, além de gerenciar o espaço de endereços IP.

**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 empresa está migrando os servidores locais para o Windows Server 2019. Como administrador da infraestrutura do Windows Server, você é responsável por gerenciar e manter 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 usar o IPAM para gerenciar servidores DNS e DHCP. Você também aprenderá a usar o IPAM para gerenciar o endereçamento IP e os espaços de endereços em sua organização.

**Objetivos de aprendizagem**

Depois de concluir este módulo, você poderá:

* Descrever o IPAM.
* Implantar o IPAM.
* Descrever como administrar o IPAM.
* Configurar as opções do IPAM.
* Gerenciar zonas DNS com o IPAM.
* Gerenciar servidores DHCP com o IPAM.
* Usar o IPAM para gerenciar o endereçamento IP.

**Pré-requisitos**

Para ter a melhor experiência de aprendizagem com este módulo, você deve ter conhecimento e experiência em:

* Conceitos e tecnologias do Active Directory Domain Services.
* Windows Server.
* Tecnologias de rede principal, como endereçamento IP, resolução de nomes e DHCP.
* Noções básicas do Windows PowerShell.

# Definir Gerenciamento de Endereços IP

Concluído100 XP

* 10 minutos

O gerenciamento da alocação de endereços IP pode ser uma tarefa complexa em redes grandes, como na Contoso. O IPAM oferece uma estrutura para descobrir, auditar e gerenciar o espaço de endereços de IP da sua rede. Estes são os benefícios de usar o IPAM:

* Alocação e planejamento do espaço de endereços IPv4 e IPv6.
* Monitoramento tendências e estatísticas de utilização de espaço de endereços IP.
* Gerenciamento de estoque de IP estático, gerenciamento de tempo de vida, criação e exclusão de registro de DNS e DHCP.
* Monitoramento de serviço e zona de servidores DNS.
* Concessão de endereços IP e rastreamento de eventos de entrada.

## Visão geral do IPAM

A equipe de suporte de infraestrutura na Contoso pode usar o IPAM para:

* Monitorar e administrar o DHCP.
* Monitorar e administrar o DNS.
* Determinar onde certos endereços IP são alocados.
* Coletar estatísticas de controladores de domínio de AD DS.
* Coletar estatísticas de servidores NPS (Servidor de Políticas de Rede).

**Dica**

Você pode usar o WID (banco de dados interno do Windows) ou um banco de dados do Microsoft SQL Server, para armazenar os dados coletados.

### Os quatro módulos do IPAM

O IPAM tem quatro módulos, conforme descrito na tabela a seguir.

| **Módulo** | **Descrição** |
| --- | --- |
| Descoberta do IPAM | Você pode configurar o IPAM para usar o AD DS para descobrir servidores ou controladores de domínio que têm DHCP ou DNS instalados. Você também pode adicionar servidores manualmente. |
| Gerenciamento do espaço de endereço IP | Você pode usar este módulo para analisar, monitorar e gerenciar o espaço de endereços IP. Com o DHCP, você pode emitir ou atribuir endereços de forma dinâmica ou estática. Você também pode acompanhar a utilização de endereços e detectar escopos de DHCP sobrepostos. |
| Gerenciamento e monitoramento multisservidor | Use este módulo para gerenciar e monitorar vários servidores DNS e DHCP. Use o gerenciamento multisservidor quando precisar que as tarefas sejam executadas em vários servidores. Por exemplo, você pode configurar e editar as propriedades e os escopos de DHCP, e acompanhar o status da utilização. Também é possível monitorar vários servidores DNS e a integridade e o status das zonas DNS entre servidores DNS autoritativos. |
| Auditoria operacional e acompanhamento de endereço IP | Você pode usar as ferramentas de auditoria para rastrear possíveis problemas de configuração. Nos servidores DHCP gerenciados, é possível coletar, gerenciar e analisar detalhes de alterações na configuração. Também é possível coletar o rastreamento de concessão de endereço de logs a partir da concessão DHCP, além de coletar informações de evento de entrada a partir dos NPS e controladores de domínio. |

## Topologia do IPAM

Uma implantação do IPAM inclui dois componentes, descritos na tabela a seguir.

| **Componente** | **Descrição** |
| --- | --- |
| Servidor IPAM | O servidor IPAM executa a coleta de dados dos servidores gerenciados. Além disso, o servidor IPAM gerencia o WID ou um banco de dados SQL Server e fornece RBAC (controle de acesso baseado em função). |
| Cliente IPAM | O cliente IPAM fornece a interface do computador cliente e interage com o servidor IPAM, chamando cmdlets do Windows PowerShell para executar o gerenciamento remoto, a configuração do DHCP e o monitoramento de DNS. O cliente IPAM pode ser um sistema operacional cliente do Windows ou sistema operacional do Windows Server. |

**Importante**

Os servidores IPAM não coordenam entre si ou acumulam informações de um servidor IPAM para outro.

Ao implantar o IPAM, a equipe de TI da Contoso deve escolher entre as opções de topologia disponíveis: centralizado, distribuído ou híbrido.

### Topologia centralizada

Na topologia centralizada, você implanta um único servidor IPAM para toda a floresta. Um único servidor IPAM proporciona controle centralizado e visibilidade para tarefas de endereçamento IP. Com a topologia centralizada, você pode analisar toda a infraestrutura de endereçamento IP a partir de um único console. Você pode usar um único servidor IPAM para diversas florestas de AD DS, estabelecendo uma relação de confiança bidirecional.

O gráfico a seguir exibe um exemplo de implantação de IPAM usando uma abordagem centralizada. Exibidos neste gráfico:

* O cliente IPAM. Um administrador usa o Gerenciador do Servidor para acessar o servidor IPAM. O RBAC controla o nível de acesso de um administrador.

**Dica**

Um administrador também pode instalar o **RSAT: recurso de cliente IPAM**e o gerenciar de outro servidor ou cliente do Windows 10.

* Servidor IPAM. O servidor se conecta a um banco de dados configurado para fornecer armazenamento para o IPAM. As tarefas agendadas também estão disponíveis no servidor IPAM.
* Servidores gerenciados. Uma coleção de servidores DNS, DHCP, NPS e controladores de domínio são descobertos e acessíveis pelo IPAM.

### Topologia distribuída

Em uma topologia distribuída, você implanta um servidor IPAM para cada site em sua floresta. É comum usar a topologia distribuída quando sua organização tem vários sites com uma infraestrutura relevante de endereçamento IP em vigor. Um servidor em cada local pode ajudar a distribuir uma carga de trabalho grande demais para ser gerenciada por um único servidor.

O gráfico a seguir exibe um exemplo de implantação de IPAM usando uma abordagem distribuída. Exibidos neste gráfico:

* Uma filial. A filial tem seu servidor IPAM e servidores gerenciados exclusivos, como um controlador de domínio e servidores DHCP, NPS e DNS.
* Um datacenter regional. Assim como a filial, o datacenter regional tem seu servidor IPAM e servidores gerenciados exclusivos.
* Um datacenter corporativo. O datacenter corporativo fornece suporte a vários servidores gerenciados e tem seu servidor IPAM exclusivo.
* Administradores de sistema, administradores forenses e administradores de rede. Esses usuários, controlados por meio do RBAC, podem executar várias tarefas de gestão nos servidores gerenciados em toda a organização.

**Dica**

Também é possível usar a topologia distribuída para permitir que unidades de negócios ou locais distintos administrem sua gestão exclusiva de endereçamento IP.

### Topologia híbrida

Você também pode implementar uma topologia híbrida com um servidor IPAM centralizado e um distribuído em cada site. Os dois servidores IPAM monitoram servidores gerenciados. Você pode controlar o escopo de gerenciamento ao monitorar alguns serviços centralmente e outros serviços em cada site.

Implantar Gerenciamento de Endereços IP

Concluído

200 XP

10 minutos

Antes de implantar o IPAM, você deve conhecer os requisitos e as limitações da implantação.

Requisitos do servidor IPAM

O servidor IPAM deve atender aos seguintes requisitos:

O servidor IPAM deve ser um servidor membro no domínio. A instalação do servidor IPAM não é compatível com um controlador de domínio.

O servidor IPAM deve ser um servidor usado para uma única finalidade. Você não deve instalar outras funções de rede, como DHCP ou DNS, no mesmo servidor.

Cuidado

Se você instalar o servidor IPAM em um servidor DHCP, o IPAM não poderá detectar outros servidores DHCP na rede.

O servidor IPAM precisa acessar um banco de dados. Você pode usar o WID no servidor IPAM ou em um banco de dados do Microsoft SQL Server. Se você usar um banco de dados do SQL Server no IPAM, poderá usar um banco de dados em um servidor separado.

Importante

Se você usar o SQL Server para hospedar seu banco de dados IPAM, essa deverá ser a única instância do SQL Server em execução nesse servidor.

O IPAM precisa de muito armazenamento. Veja se o disco que hospeda o banco de dados do SQL é grande o suficiente para armazenar os dados coletados. Por exemplo, os dados de utilização de endereço IP para 10 mil clientes exigem aproximadamente 1 GB de espaço em disco por mês.

Considerações sobre a implantação do IPAM

Ao implementar o IPAM considere o seguinte:

Para gerenciar o espaço de endereços IPv6, o IPv6 não deve estar desabilitado no servidor IPAM.

Entre no servidor IPAM com uma conta de domínio e não com uma conta local.

Para que o recurso de rastreamento e auditoria de endereço IP do IPAM funcione é preciso habilitar o log de eventos de entrada de conta nos controladores de domínio e nos servidores NPS.

Você pode definir o escopo de descoberta para um subconjunto de domínios na floresta.

Um único servidor IPAM pode dar suporte a até 150 servidores DHCP, 6 mil escopos DHCP, 500 servidores DNS e 150 zonas DNS.

As tendências de utilização de endereços IP são fornecidas apenas para IPv4.

O suporte à recuperação de endereço IP é fornecido apenas para o IPv4.

O IPAM não verifica a consistência do endereço IP com roteadores e comutadores.

Implantar o IPAM

Antes de implantar o IPAM, conclua um processo de planejamento para determinar como deseja usar o IPAM e a topologia de implantação que oferece suporte às suas necessidades organizacionais. Você só deve iniciar a implantação do IPAM após concluir este processo de planejamento. Para implantar o IPAM é preciso implantar servidores IPAM e clientes IPAM.

Implantar servidores IPAM

A implantação de servidores IPAM começa com a instalação do recurso de servidor IPAM. Depois de determinar qual topologia do IPAM usar, você pode implantar servidores IPAM executando as seguintes etapas:

Instale o recurso do servidor IPAM. Você pode instalar o servidor IPAM usando o Windows Admin Center, o Gerenciador do Servidor ou o seguinte comando do Windows PowerShell:

PowerShell

Copiar

Install-WindowsFeature IPAM -IncludeManagementTools

Provisionar servidores IPAM. Depois de instalar o recurso de servidor IPAM, você deve provisionar cada um deles. Ao provisionar os servidores IPAM, configure como os servidores que o IPAM vai monitorar serão configurados (inclusive a configuração de permissões, compartilhamentos e tarefas agendadas). Durante o provisionamento do servidor IPAM, especifique como isso deve ser feito. Você pode especificar manualmente ou usando GPOs. Se você optar por usar GPOs, especifique seu prefixo. Você também precisa criar GPOs manualmente, executando o Invoke-IpamGpoProvisioning cmdlet.

Dica

O uso de GPOs é recomendado porque automatiza o processo de configuração para servidores gerenciados.

Configurar e executar a descoberta de servidor. Você deve configurar o escopo da descoberta para os servidores que vai gerenciar. Selecionar o domínio(s) nos quais o servidor IPAM executará a descoberta determina o escopo da descoberta. Também é possível adicionar manualmente um servidor no console de gerenciamento do IPAM especificando o FQDN (nome de domínio totalmente qualificado) do servidor que você deseja gerenciar.

Escolha e gerencie os servidores descobertos. Após a conclusão da descoberta e de adicionar manualmente os servidores que não foram descobertos, escolha os servidores que você deseja gerenciar. Faça isso ao editar as propriedades do servidor no console do IPAM e alterar o Status de Gerenciamento para Gerenciado. Depois de definir a permissão de gerenciamento para um servidor, observe o indicador de status exibindo Acesso do IPAM Desbloqueado no inventário do servidor IPAM.

Implantar clientes IPAM

Você usa o cliente IPAM para configurar e gerenciar servidores IPAM. Ao instalar a função IPAM no Windows Server com a Experiência Desktop, o cliente IPAM é instalado automaticamente no servidor IPAM. Se você instalar a função IPAM no Server Core, precisará instalar manualmente o cliente IPAM em outro Windows Server usado para gerenciamento ou um cliente Windows para gerenciar o IPAM remotamente. A instalação do IPAM varia de acordo com o sistema operacional:

Windows Server. É possível instalar o cliente IPAM instalando o recurso do Windows em Ferramentas de Administração de servidor remoto\Recurso de Administração/IPAM de endereço IP do cliente.

Windows 10. Instale as RSAT: a ferramenta IPAM de endereço IP do cliente a partir de Configurações.

Demonstração

O vídeo a seguir demonstra como implementar o IPAM usando o Windows Admin Center e o Gerenciador do Servidor. As principais etapas do processo são:

Abra o Windows Admin Center.

No painel Ferramentas, selecione Recursos e funções.

Adicione o recurso servidor IPAM.

Adicione o recurso IPAM do cliente.

Abra o Server Manager.

Provisione um novo servidor IPAM e especifique as seguintes opções:

Selecione um tipo de banco de dados e um local.

Clique no provisionamento Baseado em Política de Grupo.

Insira um prefixo GPO.

Abra o Windows PowerShell e crie os GPOs necessários executando o cmdlet.

Verifique os GPOs com o Get-GPO cmdlet.

No Gerenciador do Servidor, clique em Configurar descoberta de servidor.

Após a descoberta, revise os servidores descobertos.

Recupere dados de servidores gerenciados e revise:

Blocos de endereços IP.

Escopos do DHCP.

Zonas DNS.

**Administrar Gerenciamento de Endereços IP**

Concluído100 XP

* 10 minutos

Configurar a administração do IPAM pode ser uma tarefa complexa, dependendo de como sua infraestrutura de IPAM é implantada e de quem está gerenciando a infraestrutura. Por exemplo, a Contoso pode permitir que um administrador gerencie todos os aspectos no IPAM ou limitar a capacidade de gerenciamento. Se ela quiser atribuir certas tarefas administrativas aos administradores, pode limitar tarefas com base em áreas funcionais ou servidores específicos do IPAM.

**RBAC**

Para definir e estabelecer um controle refinado para usuários e grupos, você pode usar o RBAC para personalizar:

* Funções.
* Escopos de acesso.
* Políticas de acesso.

Isso permite aos usuários e grupos executar um conjunto específico de operações administrativas em objetos específicos que o IPAM gerencia.

Implemente o gerenciamento baseado em funções no IPAM usando os componentes na tabela a seguir.

| **Componente** | **Descrição** |
| --- | --- |
| Função | Uma *função*é uma coleção de operações do IPAM. Você pode associar uma função a um usuário ou grupo no Windows por meio de uma política de acesso. Oito funções internas de administrador estão disponíveis para conveniência, mas você também pode criar funções personalizadas para atender os requisitos do seu negócio. Você pode criar e editar funções na guia **Controle de Acesso** no nó do**IPAM** em Gerenciador do Servidor. |
| Escopo de acesso | Um *escopo de acesso* determina os objetos aos quais o usuário tem acesso. É possível usar escopos de acesso para definir domínios administrativos no IPAM. Por exemplo, você pode criar escopos de acesso com base na localização geográfica de um usuário. Por padrão, o IPAM inclui um escopo de acesso **Global**. Todos os outros escopos de acesso são subconjuntos do escopo de acesso **Global**. Os usuários ou grupos atribuídos ao escopo de acesso **Global** têm acesso a todos os objetos no IPAM que a função atribuída permitir. Você pode criar e editar escopos de acesso do nó **Controle de Acesso** no console de **Gerenciamento do IPAM**. |
| Política de acesso | Uma *política de acesso* combina uma função a um escopo de acesso para atribuir permissões a um usuário ou grupo. Por exemplo, você pode definir uma política de acesso para um usuário, combinando uma função chamada **Administrador de Bloqueio de IP** com um escopo de acesso chamado **Global\Ásia**. Esse usuário teria permissão para editar e excluir os blocos de endereços IP associados ao escopo de acesso da **Ásia**, mas não teria permissão para editar ou excluir nenhum outro bloco de endereço IP no IPAM. Você pode criar e editar políticas de acesso do nó **Controle de Acesso** no console de **Gerenciamento do IPAM**. |

**Grupos de segurança do IPAM**

O IPAM tem vários grupos de segurança com base em funções internos que você pode usar para gerenciar sua infraestrutura de IPAM, conforme descrito na tabela a seguir.

| **Nome do grupo** | **Descrição** |
| --- | --- |
| Administradores do IPAM | Os membros desse grupo têm privilégios para acessar todos os dados do IPAM e para executar todas as tarefas do IPAM. |
| Administradores do IPAM MSM | Os membros desse grupo podem gerenciar servidores DHCP, escopos, políticas, servidores DNS e zonas e registros associados. |
| Administradores de DNS do IPAM | Os membros desse grupo podem gerenciar servidores DNS, suas zonas de DNS e registros de recursos associados. |
| Administradores de registro DNS | Os membros deste grupo podem gerenciar registros de recursos de DNS. |
| Administradores do IPAM ASM | Os membros desse grupo podem executar tarefas de espaço de endereços IP, além de tarefas comuns de gerenciamento de IPAM. |
| Administradores de registro de endereço IP | Os membros desse grupo podem gerenciar endereços IP, inclusive endereços não alocados. Os membros podem criar e excluir instâncias de endereço IP. |
| Administradores de DHCP do IPAM | Os membros desse grupo podem gerenciar servidores DHCP e seus escopos. |
| Administradores de escopo de DHCP do IPAM | Os membros desse grupo podem gerenciar escopos de DHCP. |
| Administradores de reservas de DHCP do IPAM | Os membros desse grupo podem gerenciar reservas de DHCP. |

**Administrar Gerenciamento de Endereços IP**

Concluído100 XP

* 10 minutos

Configurar a administração do IPAM pode ser uma tarefa complexa, dependendo de como sua infraestrutura de IPAM é implantada e de quem está gerenciando a infraestrutura. Por exemplo, a Contoso pode permitir que um administrador gerencie todos os aspectos no IPAM ou limitar a capacidade de gerenciamento. Se ela quiser atribuir certas tarefas administrativas aos administradores, pode limitar tarefas com base em áreas funcionais ou servidores específicos do IPAM.

**RBAC**

Para definir e estabelecer um controle refinado para usuários e grupos, você pode usar o RBAC para personalizar:

* Funções.
* Escopos de acesso.
* Políticas de acesso.

Isso permite aos usuários e grupos executar um conjunto específico de operações administrativas em objetos específicos que o IPAM gerencia.

Implemente o gerenciamento baseado em funções no IPAM usando os componentes na tabela a seguir.

| **Componente** | **Descrição** |
| --- | --- |
| Função | Uma *função*é uma coleção de operações do IPAM. Você pode associar uma função a um usuário ou grupo no Windows por meio de uma política de acesso. Oito funções internas de administrador estão disponíveis para conveniência, mas você também pode criar funções personalizadas para atender os requisitos do seu negócio. Você pode criar e editar funções na guia **Controle de Acesso** no nó do**IPAM** em Gerenciador do Servidor. |
| Escopo de acesso | Um *escopo de acesso* determina os objetos aos quais o usuário tem acesso. É possível usar escopos de acesso para definir domínios administrativos no IPAM. Por exemplo, você pode criar escopos de acesso com base na localização geográfica de um usuário. Por padrão, o IPAM inclui um escopo de acesso **Global**. Todos os outros escopos de acesso são subconjuntos do escopo de acesso **Global**. Os usuários ou grupos atribuídos ao escopo de acesso **Global** têm acesso a todos os objetos no IPAM que a função atribuída permitir. Você pode criar e editar escopos de acesso do nó **Controle de Acesso** no console de **Gerenciamento do IPAM**. |
| Política de acesso | Uma *política de acesso* combina uma função a um escopo de acesso para atribuir permissões a um usuário ou grupo. Por exemplo, você pode definir uma política de acesso para um usuário, combinando uma função chamada **Administrador de Bloqueio de IP** com um escopo de acesso chamado **Global\Ásia**. Esse usuário teria permissão para editar e excluir os blocos de endereços IP associados ao escopo de acesso da **Ásia**, mas não teria permissão para editar ou excluir nenhum outro bloco de endereço IP no IPAM. Você pode criar e editar políticas de acesso do nó **Controle de Acesso** no console de **Gerenciamento do IPAM**. |

**Grupos de segurança do IPAM**

O IPAM tem vários grupos de segurança com base em funções internos que você pode usar para gerenciar sua infraestrutura de IPAM, conforme descrito na tabela a seguir.

| **Nome do grupo** | **Descrição** |
| --- | --- |
| Administradores do IPAM | Os membros desse grupo têm privilégios para acessar todos os dados do IPAM e para executar todas as tarefas do IPAM. |
| Administradores do IPAM MSM | Os membros desse grupo podem gerenciar servidores DHCP, escopos, políticas, servidores DNS e zonas e registros associados. |
| Administradores de DNS do IPAM | Os membros desse grupo podem gerenciar servidores DNS, suas zonas de DNS e registros de recursos associados. |
| Administradores de registro DNS | Os membros deste grupo podem gerenciar registros de recursos de DNS. |
| Administradores do IPAM ASM | Os membros desse grupo podem executar tarefas de espaço de endereços IP, além de tarefas comuns de gerenciamento de IPAM. |
| Administradores de registro de endereço IP | Os membros desse grupo podem gerenciar endereços IP, inclusive endereços não alocados. Os membros podem criar e excluir instâncias de endereço IP. |
| Administradores de DHCP do IPAM | Os membros desse grupo podem gerenciar servidores DHCP e seus escopos. |
| Administradores de escopo de DHCP do IPAM | Os membros desse grupo podem gerenciar escopos de DHCP. |
| Administradores de reservas de DHCP do IPAM | Os membros desse grupo podem gerenciar reservas de DHCP. |

**Gerenciar zonas DNS com Gerenciamento de Endereços IP**

Concluído100 XP

* 5 minutos

A Contoso pode usar o IPAM para gerenciar servidores e zonas DNS para todos os servidores gerenciados pelo servidor IPAM. Durante a descoberta, o IPAM revela todos os servidores DNS nos domínios que foram especificados.

**Executar o gerenciamento de DNS**

Você pode usar o IPAM para executar as seguintes tarefas de gerenciamento de DNS:

* Analisar as zonas e servidores DNS. Você pode analisar todos os servidores DNS gerenciados, além das zonas de pesquisa direta e das zonas de pesquisa inversa nesses servidores DNS. O status e integridade da zona estão disponíveis para zonas de pesquisa direta, mas não para zonas de pesquisa inversa.
* Criar novas zonas. Para criar zonas DNS, no painel de navegação, selecione o nó **Servidores DNS e DHCP**. Clique com o botão direito do mouse ou acesse o menu de contexto do servidor DNS no qual deseja adicionar uma zona e clique em **Criar zona DNS**.
* Criar registros de DNS. Você pode criar registros DNS para qualquer zona que o IPAM gerencia. Para fazer isso, execute estas etapas:
  1. No painel de navegação do IPAM, clique em **Zonas DNS**e depois selecione a zona apropriada, por exemplo, .
  2. Clique com o botão direito do mouse ou acesse o menu de contexto da zona e clique em **Adicionar registro de recurso DNS**.
  3. Verifique se o nome de zona DNS e o nome do servidor DNS são exibidos corretamente na lista e adicione um novo registro de recurso DNS. Por exemplo, clique em **Registro de recurso tipo A** e adicione as informações necessárias: nome, FQDN e endereço IP.
* Gerenciar encaminhadores condicionais.
  1. Para adicionar um encaminhador condicional no painel de navegação, selecione o nó **Servidores DNS e DHCP**. Clique com o botão direito do mouse ou acesse o menu de contexto do servidor DNS no qual deseja adicionar uma zona e clique em **Criar encaminhador condicional DNS**.
  2. Para gerenciar um encaminhador condicional depois de criá-lo, no painel de navegação, em Zonas DNS, clique em **Encaminhadores Condicionais**. E então gerenciar as configurações de encaminhamento condicional no painel **detalhes**.
* Abrir o console DNS para qualquer servidor que o IPAM gerencia. Você pode abrir o **MMC (console de gerenciamento Microsoft)** do DNS ao clica com o botão direito do mouse ou acessar o menu de contexto de um servidor na página servidores DNS e DHCP e então selecionar **Iniciar o MMC**.

**Gerenciar servidores DHCP com o gerenciamento de endereços IP**

Concluído100 XP

* 10 minutos

Os administradores de TI da Contoso podem configurar servidores DHCP e informações de escopo do DHCP usando a interface de administração do IPAM. O IPAM permite que eles configurem vários servidores DHCP e usem funcionalidades como o Failover do DHCP para que os servidores funcionem juntos em sua implementação de DHCP.

**Configurar servidores DHCP**

Normalmente, você executa a configuração DHCP para servidores individuais na página servidores DNS e DHCP. Você pode executar várias tarefas de configuração em um servidor DHCP no console de administração do IPAM:

* Analise as informações de escopo do DHCP em todos os servidores.
* Editar Propriedades do Servidor DHCP. Você pode editar propriedades de servidor, como log de auditoria de DHCP, configuração de atualização dinâmica de DNS e filtragem de endereço MAC (controle de acesso à mídia).
* Editar opções do Servidor DHCP. É possível configurar e criar opções de servidor DHCP com base em classes de fornecedor ou de usuário.
* Configurar classes de fornecedor ou de usuário do DHCP. Você pode analisar e modificar as classes de usuário e fornecedor.
* Configurar Política do DHCP. Você pode editar as propriedades e condições da política do DHCP.
* Importar Política do DHCP. Você pode importar políticas do DHCP usando arquivos que outros servidores DHCP exportam.
* Adicionar filtros de endereços MAC de DHCP. Você pode adicionar filtros de endereço MAC de DHCP para permitir ou negar atribuições de endereço DHCP com base em endereços MAC.
* Ativar e desativar políticas de DHCP. Você pode controlar a implementação de políticas de DHCP.
* Replicar servidores DHCP. Esta opção replica a configuração de escopos de failover em um servidor para servidores parceiros de failover.
* Abrir o console DHCP. Você pode abrir o console **DHCP** para o servidor selecionado.

**Configurar escopos do DHCP**

Você pode configurar os detalhes do escopo do DHCP no IPAM executando as seguintes tarefas:

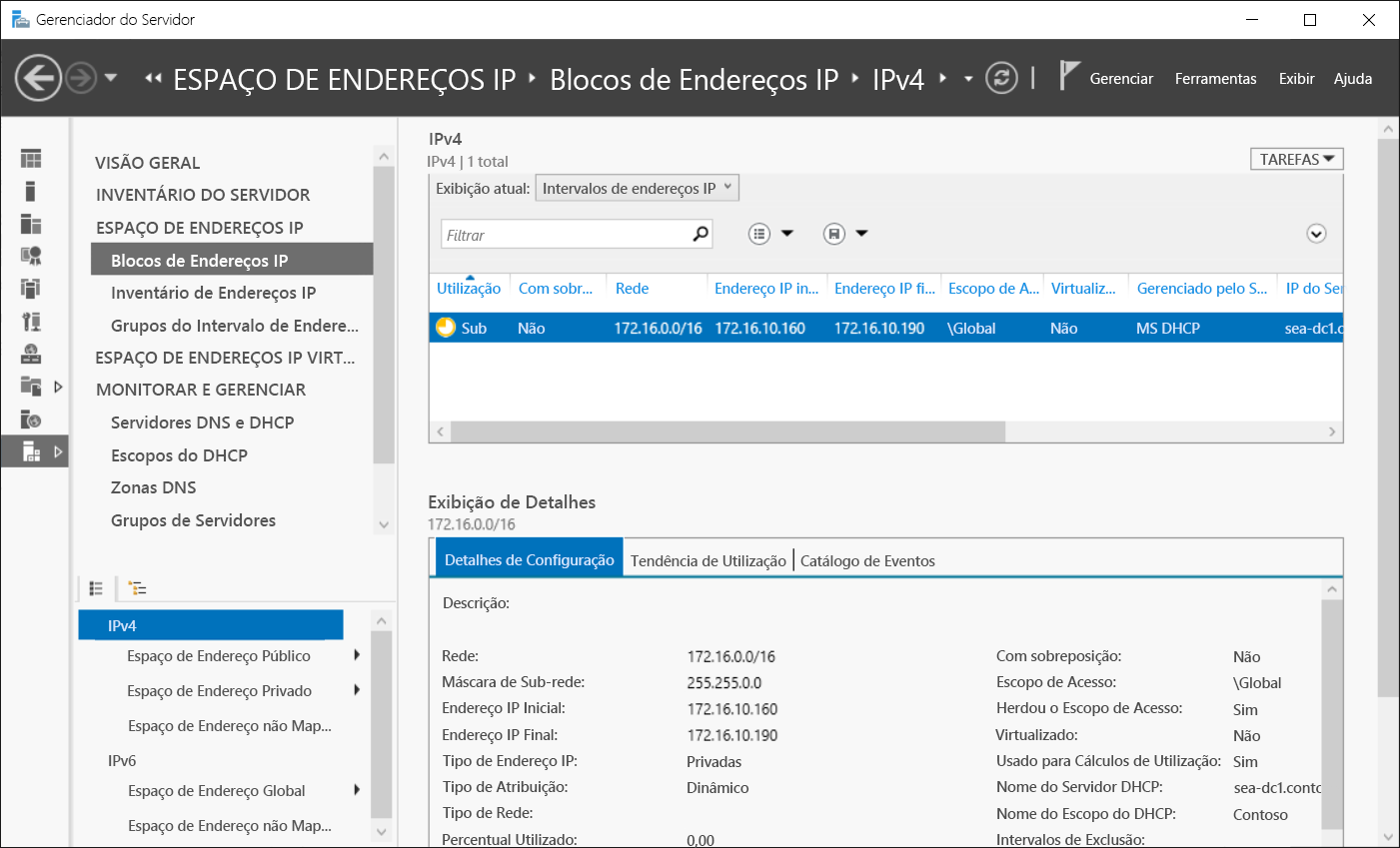
1. Editar as propriedades de escopo do DHCP.
2. Duplicar um escopo do DHCP. Usar um escopo do DHCP como modelo para criar um novo escopo no mesmo servidor ou em um servidor diferente.
3. Criar uma Reserva de DHCP.
4. Adicionar a um superescopo de DHCP.
5. Configurar um Failover de DHCP.
6. Importar uma política de DHCP.
7. Ativar e desativar escopos de DHCP.
8. Ativar e desativar políticas DHCP para o escopo selecionado.
9. Replicar um escopo do DHCP.
10. Remover uma configuração de failover de DHCP.
11. Remover um escopo de um superescopo de DHCP.

**Usar o gerenciamento de endereços IP para gerenciar o endereçamento IP**

Concluído100 XP

* 10 minutos

Os administradores de TI da Contoso podem usar o IPAM para gerenciar, acompanhar, auditar e relatar os espaços de endereço IPv4 e IPv6 da Contoso. O nó IPAM IP ADDRESS SPACE fornece estatísticas de utilização de endereços IP e dados de tendência históricas para que eles possam tomar decisões informadas de planejamento para espaços de endereço dinâmicos, estáticos e virtuais.



O IPAM descobre automaticamente espaços de endereço e dados de utilização dos servidores DHCP que o IPAM gerencia. A Contoso também pode importar informações de endereço IP de arquivos do CSV. Os administradores podem usar o IPAM para detectar intervalos de endereços IP sobrepostos definidos em diferentes servidores DHCP. Eles podem usar essas informações para:

* Localizar endereços IP livres dentro de um intervalo.
* Criar Reservas de DHCP.
* Criar registros de DNS.

**Gerenciar o endereçamento IP com exibições**

Você pode personalizar os componentes disponíveis do espaço de endereços IP no console de administração do IPAM usando uma das exibições a seguir.

| **Visualizar** | **Descrição** |
| --- | --- |
| Blocos de endereços IP | Os *blocos de endereço IP* são as entidades de nível mais alto em uma organização de espaço de endereços IP. Um bloco de endereço IP é uma sub-rede IP marcada por um endereço IP inicial e um endereço IP final. Você pode usar blocos de endereços IP para criar e alocar intervalos de endereços IP no DHCP. Você pode adicionar, importar, editar e excluir blocos de endereços IP. O IPAM mapeia os intervalos de endereços IP para o bloco de endereços IP apropriado automaticamente com base nos limites do intervalo. |
| Intervalos de endereços IP | Os *intervalos de endereços IP* são o próximo nível hierárquico de entidades de espaço de endereços IP após os blocos de endereços IP. Um intervalo de endereço IP é uma sub-rede IP que é marcada por um endereço IP inicial e um endereço IP final. Os intervalos de endereços IP geralmente correspondem a um escopo DHCP, um intervalo de endereços IPv4 ou IPv6 estático ou a um pool de endereços que é usado para atribuir endereços a hosts. |
| Endereços IP | Os *endereços IP* são os endereços que compõem o intervalo de endereços IP. O IPAM permite o gerenciamento do ciclo de vida de ponta a ponta de endereços IPv4 e IPv6, incluindo a sincronização de registros com servidores DHCP e DNS. O IPAM mapeia um endereço para o intervalo apropriado automaticamente com base no endereço inicial e final do intervalo de endereços IP. |
| Estoque de endereço IP | O **Inventário de endereço IP** exibe listas de todos os endereços IP na empresa junto aos nomes e tipos de dispositivo. O inventário de endereço IP é um grupo lógico dentro da exibição de **Endereços IP**. Você pode usar esse grupo para personalizar a maneira como o espaço de endereço é exibido para gerenciar e controlar o uso de IP. |
| Grupos de intervalos de endereços IP | Com o IPAM você pode organizar os intervalos de endereços IP em grupos lógicos chamados *Grupos de intervalos de endereços IP*. Por exemplo, é possível organizar intervalos de endereços IP geograficamente ou por divisão de negócios. Você define grupos lógicos selecionando os critérios de agrupamento de campos internos personalizados ou definidos pelo usuário. |

**Monitorar servidores DHCP e DNS**

O IPAM permite monitoramento de serviço automatizado e periódico de servidores DHCP e DNS em uma ou em várias florestas. No **Gerenciador do Servidor**, no nó IPAM, o monitoramento e o gerenciamento de servidores DHCP e DNS são organizados nas exibições listadas na tabela a seguir.

| **Visualizar** | **Descrição** |
| --- | --- |
| Servidores DNS e DHCP | Por padrão, os servidores DHCP e DNS gerenciados são organizados por sua interface de rede em /32 sub-redes para IPv4 e /128 sub-redes para IPv6. Você pode selecionar a exibição para que ela mostre apenas as propriedades do escopo DHCP, só as propriedades do servidor DNS, ou as duas. |
| Escopos do DHCP | Essa exibição permite o monitoramento de utilização de escopo. As estatísticas de utilização são automaticamente coletadas de forma periódica de um servidor DHCP gerenciado. Você pode acompanhar propriedades de escopo importantes, como nome, ID, comprimento do prefixo e status. |
| Monitoramento de zona DNS | Você habilita o monitoramento de zona para zonas de pesquisa direta. O status da zona é baseado em eventos coletados pelo IPAM. O status de cada zona é resumido. |
| Grupos de servidores | Você pode organizar servidores DNS e DHCP gerenciados em grupos lógicos. Por exemplo, você pode organizar servidores por unidade de negócios ou geografia. Você define grupos selecionando os critérios de agrupamento de campos internos ou definidos pelo usuário. |