Entender como bloquear o cliente de roaming Umbrella no AD

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Overview

Processo

Introdução

Este documento descreve como bloquear o cliente Umbrella Roaming em um ambiente do Ative Diretory (AD) usando Objetos de Diretiva de Grupo (GPOs).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Umbrella Roaming Client

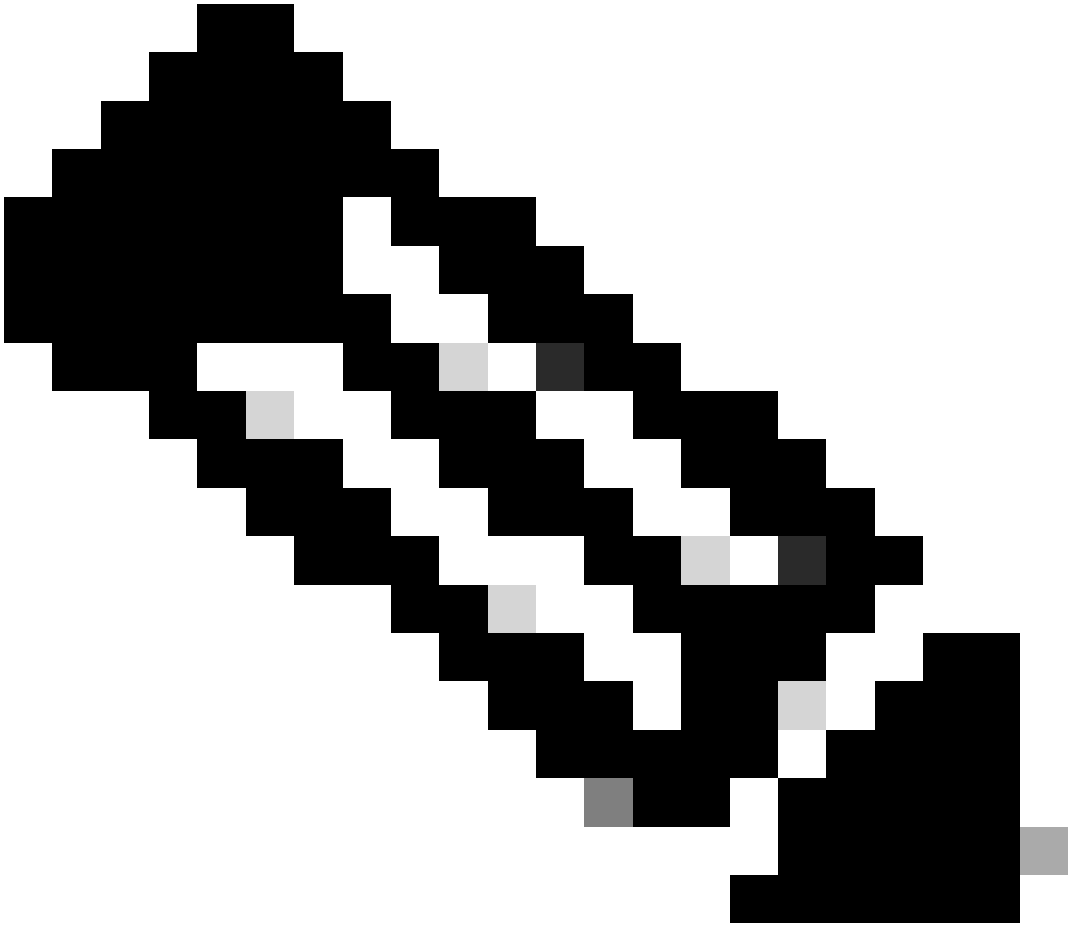
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Verifique se os usuários com permissões administrativas locais não podem desabilitar o serviço Umbrella Roaming.

Processo

Conclua estas etapas em um Controlador de Domínio do Windows 2003/2008:



Note: Se o serviço que você deseja configurar não estiver presente na lista, instale o GPMC em um computador que tenha o serviço em execução.

---

1. Crie um Novo Grupo de Segurança no Ative Diretory chamado Umbrella_Roaming.

- Isso é necessário, pois você já pode ter um grupo de segurança que contém diferentes membros de Administradores do Domínio.

2. Abra o Editor de Diretiva de Grupo (Start > Run > Type: gpmc.msc >) e crie um Novo Objeto de Diretiva de Grupo chamado Umbrella.

3. Edite a nova política de grupo e navegue para Configuração do Computador > Políticas > Configurações do Windows > Configurações de Segurança > Serviços do Sistema.

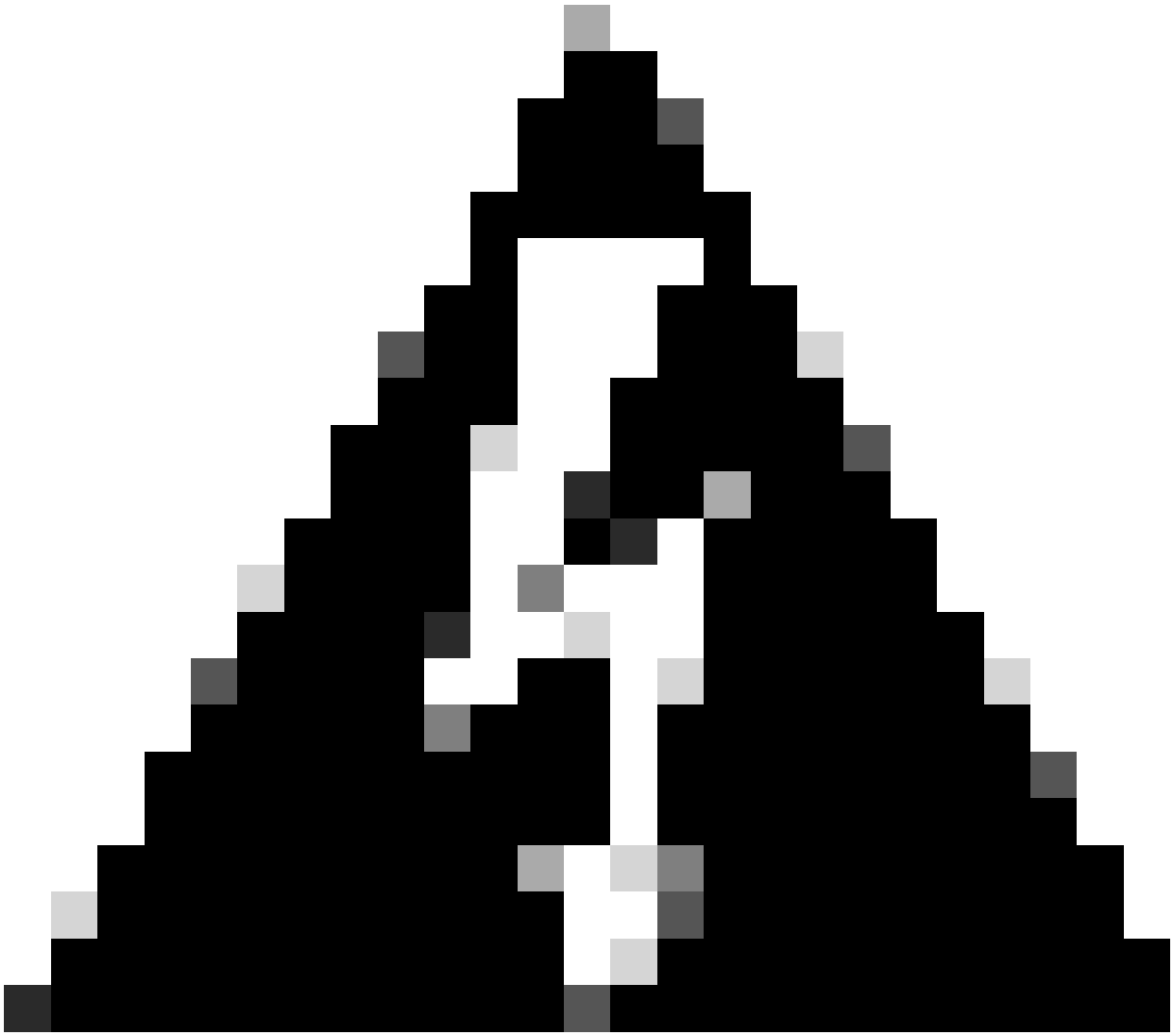
- O `serviço Umbrella Roaming Client` precisa ser importado para que você possa vê-lo em `System Services`. Leia mais sobre como concluir este processo neste artigo da Microsoft.

4. Percorra os serviços listados até chegar ao serviço Umbrella Roaming Client.

- Uma vez concluída a configuração das políticas, certifique-se de que o cliente esteja atualizado com o comando `gpupdate` antes do teste.

5. Configure o serviço clicando duas vezes no nome do serviço, selecione Definir esta política > Automático e edite os grupos de segurança.

6. Adicione a conta Network Service e conceda permissões de Leitura. Remova o grupo Administradores e/ou Administradores de domínio conforme necessário.



aviso: NÃO remova as contas SYSTEM ou INTERATIVE da lista.

Agora você pode aplicar a diretiva de grupo aos contêineres necessários da maneira normal e permitir que a diretiva seja aplicada aos computadores cliente.

Você pode testar a funcionalidade habilitando o GPO e fazendo logon em um computador cliente como administrador ou como uma conta com permissões de grupo restritas. A tentativa de parar o

serviço pode resultar na exibição desta mensagem:

```
Could not stop the service on Local Computer. Error 5: Access is denied.
```

Como alternativa, a opção para interromper o serviço fica acinzentada e indisponível. Qualquer uma dessas opções mostra que o GPO foi configurado e aplicado ao cliente com êxito.

Se a mensagem de erro não for exibida e você ainda puder parar um serviço restrito, verifique se o GPO foi configurado corretamente e se não há GPOs conflitantes. Para obter mais informações, consulte a documentação da Microsoft.

Verifique se os administradores relevantes foram adicionados ao grupo Umbrella_Roaming e se o GPO de serviço permite acesso ao grupo Umbrella_Roaming.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.