Solução de problemas "Acesso negado" Alerta no Umbrella AD Connector

Contents

Introdução

Este documento descreve a solução de problemas de "Acesso Negado" quando o Cisco Umbrella Ative Diretory (AD) Connector está nos estados de Alerta ou Erro.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

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.

Problema

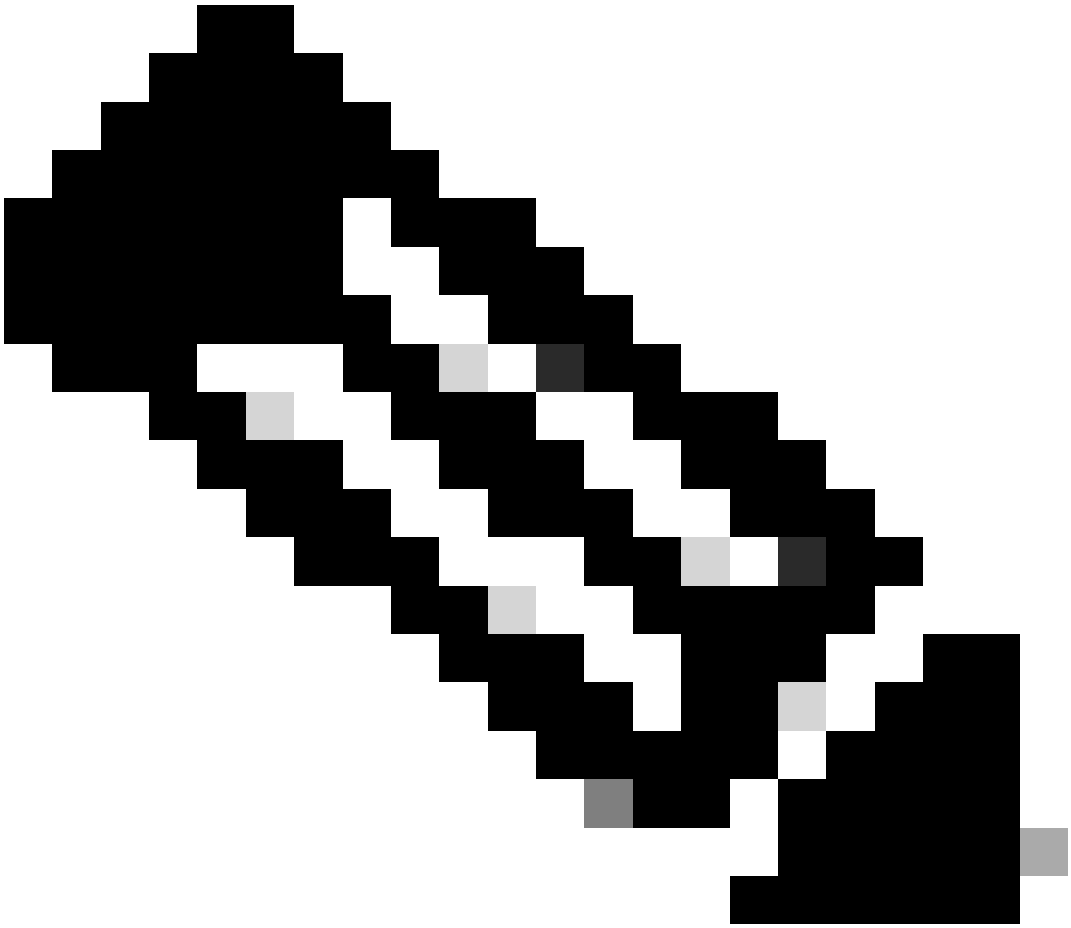
Você percebe que um Conector AD está mostrando um estado de alerta ou de erro e a mensagem listada quando você passa o mouse sobre o alerta inclui "Acesso negado" a um dos servidores AD registrados.

Solução

Verifique se o usuário do OpenDNS_Connector é membro destes Grupos do AD:

- Leitores de Log de Eventos
- Usuários COM distribuídos
- Controladores de Domínio Corporativos Somente Leitura

A solução é verificar se DCOM, WMI e Gerenciar o log de auditoria e segurança estão configurados corretamente no servidor AD em questão.



Note: Por padrão, não há suporte para vários domínios ou várias florestas. Consulte o anúncio do Suporte a domínios multi-AD no Umbrella. Você também pode entrar em contato com o Umbrella Support sobre a sua configuração para obter assistência se tiver esses problemas.

Para verificar as Permissões WMI:

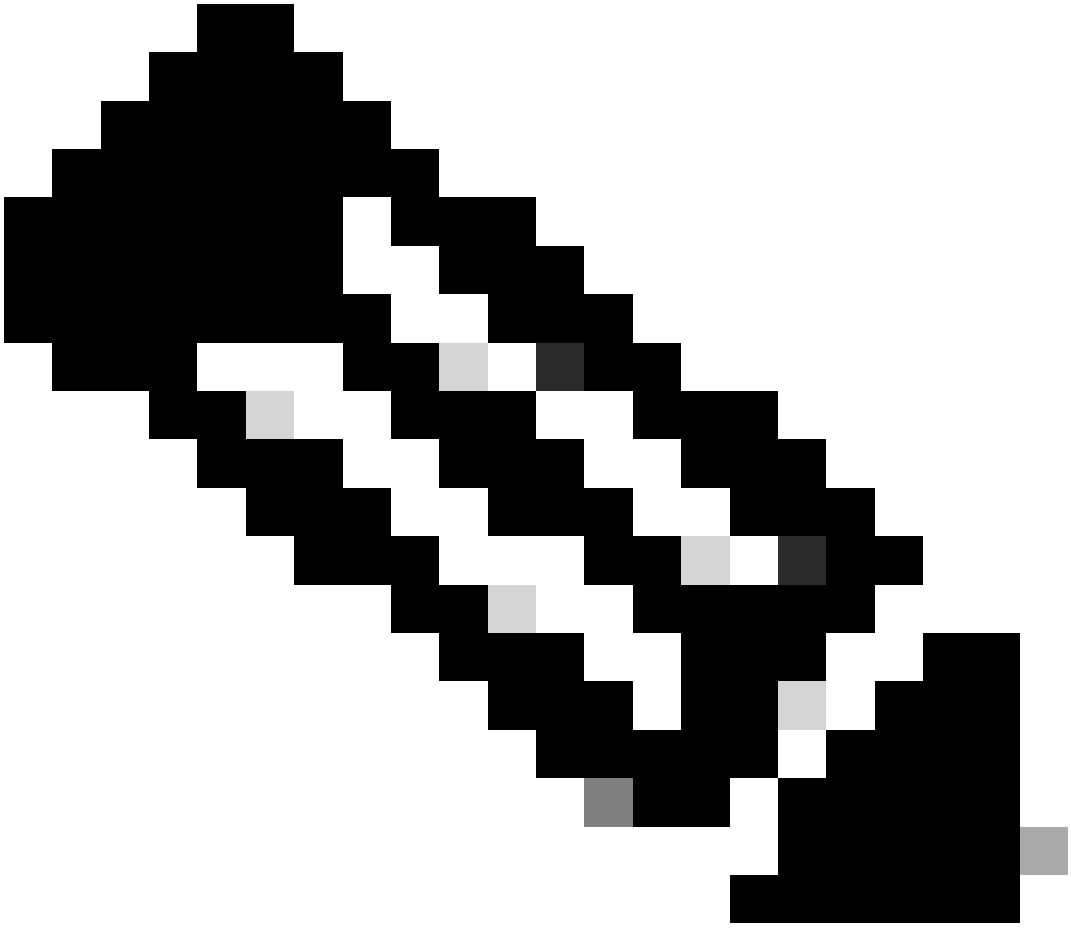
1. Selecione Start > Run > wmimgmt.msc para acessar o console do Controle de Infraestrutura de

Gerenciamento do Windows.
2. Clique com o botão direito do mouse em Controle WMI > Propriedades > guia Segurança.
3. Selecione Raiz > namespace CIMV2 e selecione o botão Segurança.
4. Adicione o usuário OpenDNS_Connector e Permita estas permissões:

- Habilitar conta
- Ativação remota
- Ler Segurança

Para verificar Permissões DCOM:

1. Em uma linha de comando, execute dcomcnfg.
2. Navegue até Raiz do Console > Serviços de Componentes > Computadores.
3. Clique com o botão direito do mouse em Meu Computador e selecione Propriedades.
4. Em Propriedades do Meu Computador, selecione a guia Segurança COM.
5. Na seção Permissões de Inicialização e Ativação, selecione Editar Limites.
6. Adicione o usuário do OpenDNS_Connector e permita as permissões de Início Remoto e Ativação Remota.
7. Selecione OK para confirmar e fechar as Propriedades do Meu Computador.



Note: Na maioria dos casos, se forem feitas alterações no DCOM, será necessário reinicializar esse DC para que as alterações entrem em vigor.

Para verificar "Gerenciar logs de auditoria e segurança" nos servidores Windows 2003:

1. Em um Controlador de Domínio, abra um prompt de comando e digite este comando (se estiver executando o Windows 2003, substitua /r por /v):

```
gpresult /scope computer /r
```

2. Procure a linha Applied Group Policy Objects (Objetos de Diretiva de Grupo Aplicados). Abaixo está uma lista de políticas aplicadas a esse controlador de domínio. Anote um que possa ser aplicado a todos os controladores de domínio.
(como "Política de controladores de domínio padrão"). Se não houver nenhum, você precisará criar um e aplicá-lo.

Para editar a política apropriada:

3. Abra o painel Gerenciamento de Diretiva de Grupo (através das Ferramentas Iniciar/Administrativas). Selecione a política desejada. Algo na pasta "Controladores de domínio" provavelmente é um candidato.

4. Clique com o botão direito do mouse nessa política e selecione Editar para exibir o Editor de Gerenciamento de Política de Grupo.

5. Navegue até a pasta Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment e selecione Manage audit and security log para exibir suas propriedades.

6. Selecione Definir estas configurações de política >Adicionar usuário ou grupo. Procure e selecione o usuário OpenDNS_Connector.

7. Execute o comando "gpupdate /force" no Controlador de Domínio para certificar-se de que a diretiva esteja aplicada.

Causa

Esse erro geralmente indica que o usuário do OpenDNS_Connector não tem permissões suficientes para operar.

O script do Conector do Windows normalmente define as permissões necessárias para o usuário do OpenDNS_Connector. No entanto, em ambientes restritos do AD, alguns administradores não têm permissão para executar scripts VB em seus Controladores de Domínio e, portanto, precisam replicar manualmente as ações do script de Configuração do Windows.

Informações adicionais

Para obter mais informações sobre como resolver esse problema, visite Tópicos completos para a resolução de acesso negado.

Se, após confirmar/alterar as configurações mencionadas acima, você ainda estiver vendo mensagens de "Acesso negado" no Painel, envie ao Suporte os logs do conector conforme descrito neste artigo: Forneça suporte com logs do conector do AD.

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.