Solucionar problemas de integração do Umbrella Insights AD sem detectar o tráfego do usuário

Contents

Introdução

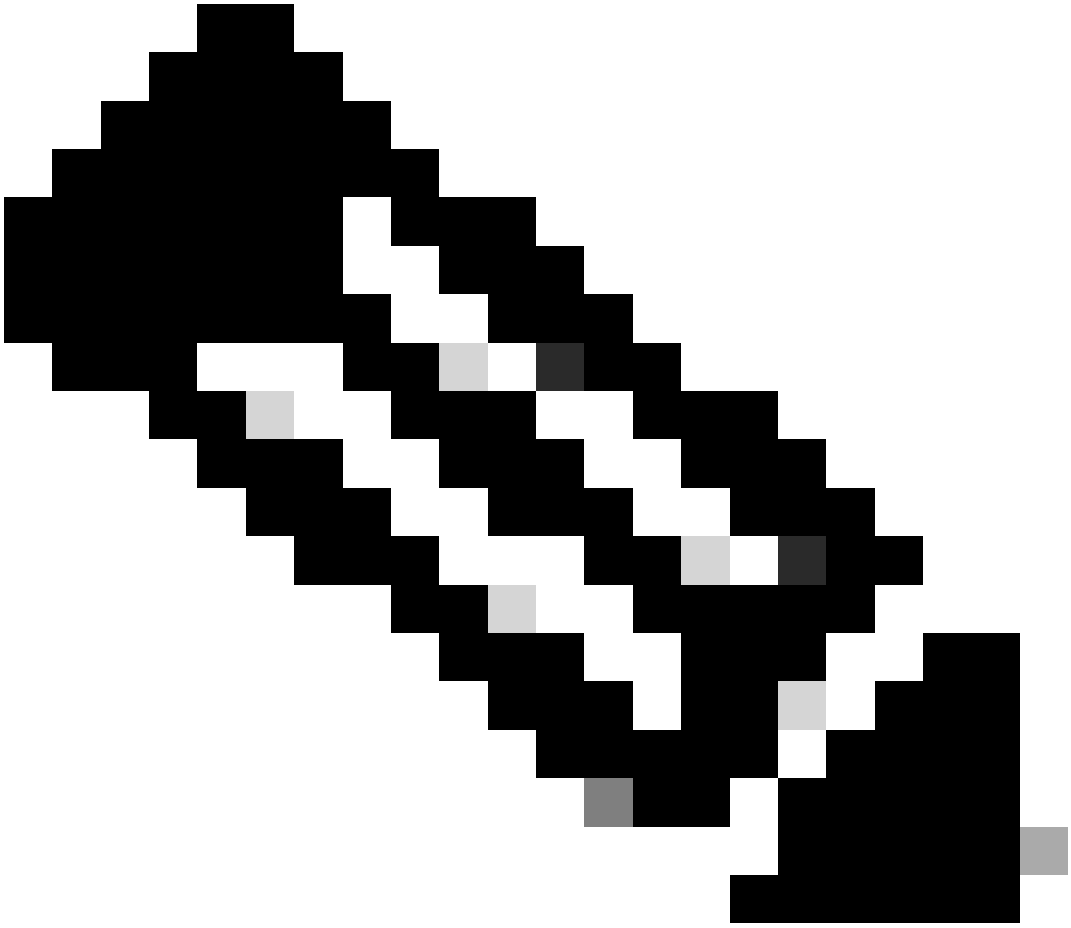
Este documento descreve como solucionar problemas da integração do AD do Umbrella Insights que não detecta o tráfego do usuário.

Overview

Você instalou o Umbrella Insights, configurou um conector e Virtual Appliances e registrou seus controladores de domínio. Todos os seus componentes são exibidos em verde e estão funcionando no painel em `implantações -> Sites e Ative Diretory`. No entanto, você tem uma política configurada para usar usuários do AD ou objetos de grupo, mas ainda não vê a atividade do usuário relatada no painel ou na política que está sendo aplicada corretamente.

Você também pode observar que nesta entrada se repete no arquivo OpenDNSAuditClient.log

`Último evento recebido em 1970-01-01 00:00:00`



Note: O arquivo de log está localizado em C:\Program Arquivos (x86)\OpenDNS\OpenDNS Connector\<VERSION>\
VERSION = a versão real instalada do serviço Connector, como v1.1.22

Explicação

O principal motivo para isso é que os eventos de logon de auditoria podem não estar configurados no domínio do Ative Diretory. A mensagem de log indica que o conector não viu um único evento de usuário desde que foi instalado. No momento, isso não é algo que gera um erro no painel.

Resolução

O principal a ser acessado é verificar a política de grupo do AD para obter a configuração correta da política de auditoria:

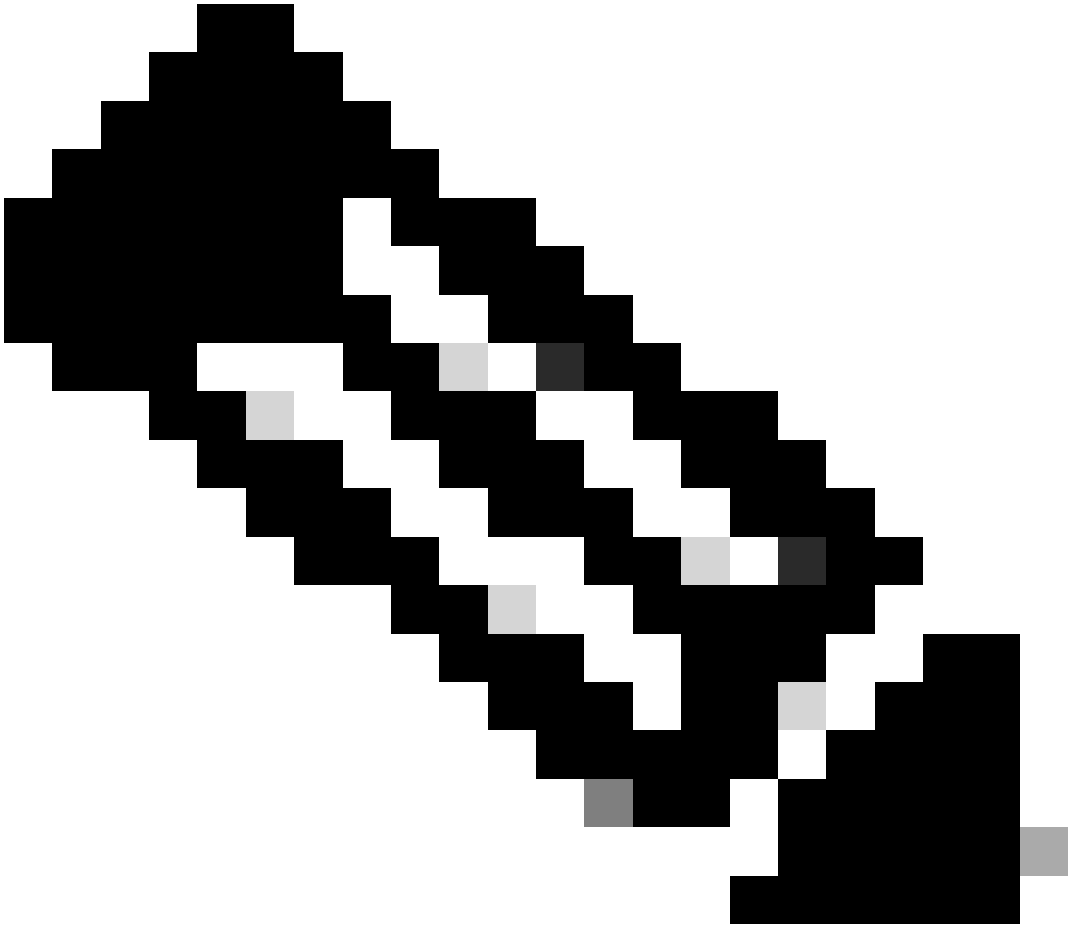
1. No Controlador de Domínio, abra o `painel Gerenciamento de Diretiva de Grupo localizado em *Ferramentas Administrativas*` e selecione uma diretiva que se aplique aos Controladores de Domínio (a Diretiva de Controlador de Domínio Padrão seria o candidato provável).

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

3. Navegue até a pasta `"Configuração do Computador\Políticas\Configurações do Windows\Configurações de Segurança\Políticas Locais\Política de Auditoria"` e selecione Auditoria de eventos de logon para exibir suas propriedades.

4. Esta política deve ser usada para auditar as tentativas de Êxito.

5. Execute o comando gpupdate para aplicar a diretiva.



Note: Há casos em que os "Controladores de domínio padrão e a Política de domínio padrão" talvez precisem ter essa configuração configurada.

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.