Configurar usuários, grupos e computadores do Ative Diretory para sincronização com o serviço OpenDNS Connector

Contents

Introdução

Overview

- Permissões padrão
- Exibir acesso efetivo
- Definindo permissões LDAP do OpenDNS_Connector
- script userPerms

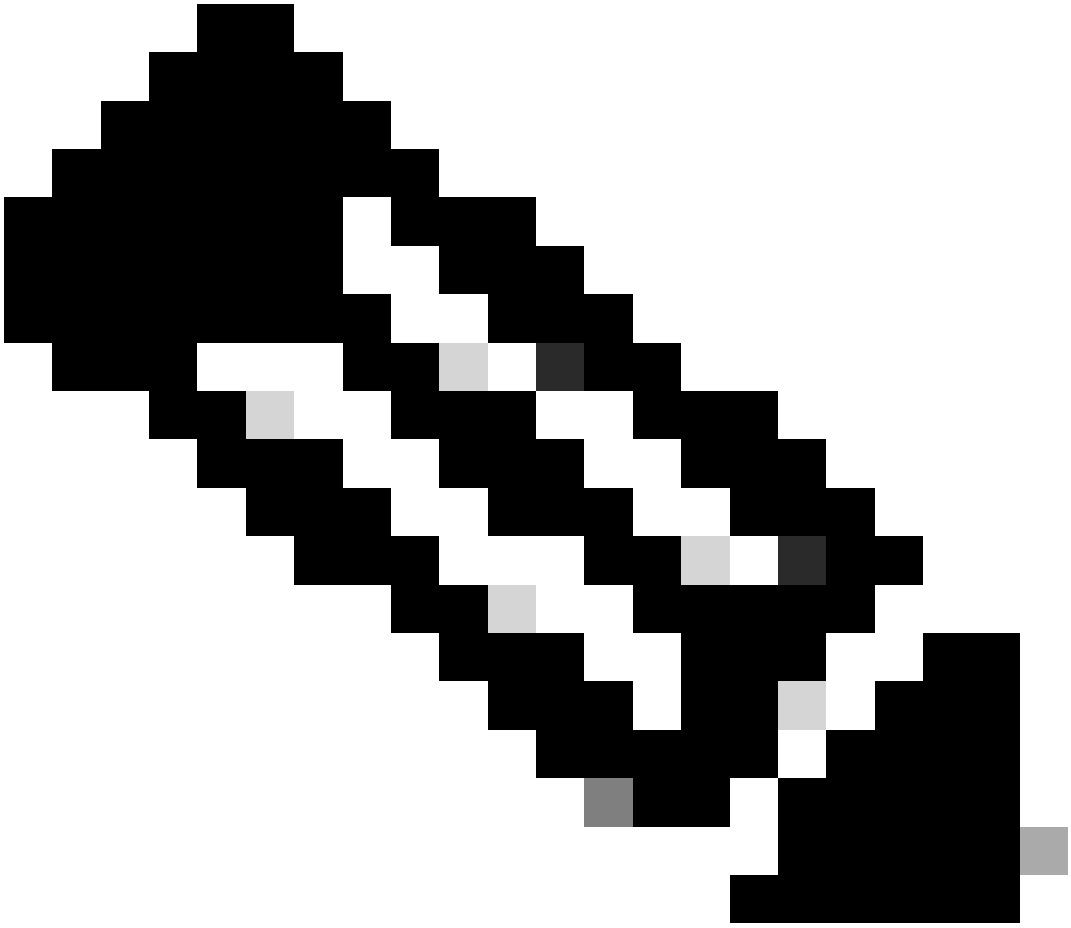
Introdução

Este documento descreve como sincronizar usuários, grupos e computadores do Ative Diretory com o serviço OpenDNS Connector.

Overview

Como parte de sua operação, o serviço OpenDNS Connector sincroniza uma lista de usuários, grupos e computadores do Ative Diretory usando o protocolo LDAP. Este artigo descreve como verificar se a conta OpenDNS_Connector tem as permissões corretas para ler esses objetos.

Cada objeto (usuários/grupos/computadores) no Ative Diretory tem permissões de segurança ACL associadas a ele, e cada objeto deve permitir que a conta de usuário do OpenDNS_Connector leia seus atributos.



Note: Este artigo supõe que os pré-requisitos normais para a conta 'OpenDNS_Connector' já foram verificados. Se usuários/grupos do AD não estiverem presentes no painel, consulte este artigo primeiro: Usuários/grupos do AD ausentes no Painel do Umbrella.

Permissões padrão

Por padrão, todos os usuários autenticados podem ler as propriedades de usuários/grupos/computadores, de modo que o usuário do OpenDNS_Connector não requer nenhuma permissão extra para fazer a sincronização LDAP.

As permissões padrão são normalmente definidas da seguinte forma:

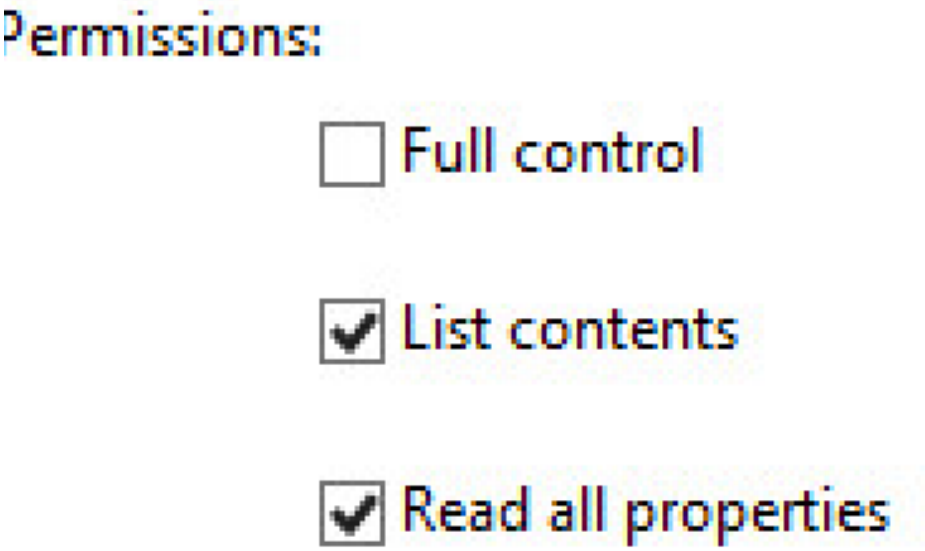
1) O grupo 'Acesso Compatível com Versões Anteriores ao Windows 2000' recebe permissões de leitura (ler todas as propriedades) no domínio para 'Objetos de Usuário Descendentes', 'Objetos de Grupo Descendentes' e 'Objetos de Computador Descendentes'.

Você pode verificar isso duas vezes da seguinte maneira:

- Abrir Usuários e Computadores do Ative Diretory
- Clique em 'Exibir' e marque a opção 'Recursos avançados'.
- Clique com o botão direito do mouse no objeto Domínio e selecione 'Propriedades' e, em seguida, 'Segurança > Avançado'
- Selecione a entrada 'Pre Windows 2000 Compatible Access' com permissões 'Special':

115011616667

- Clique em 'Editar' para ver essas permissões em detalhes.
- Selecione 'Objetos de usuário descendentes' na seção Aplica-se a
- Procure estas permissões:

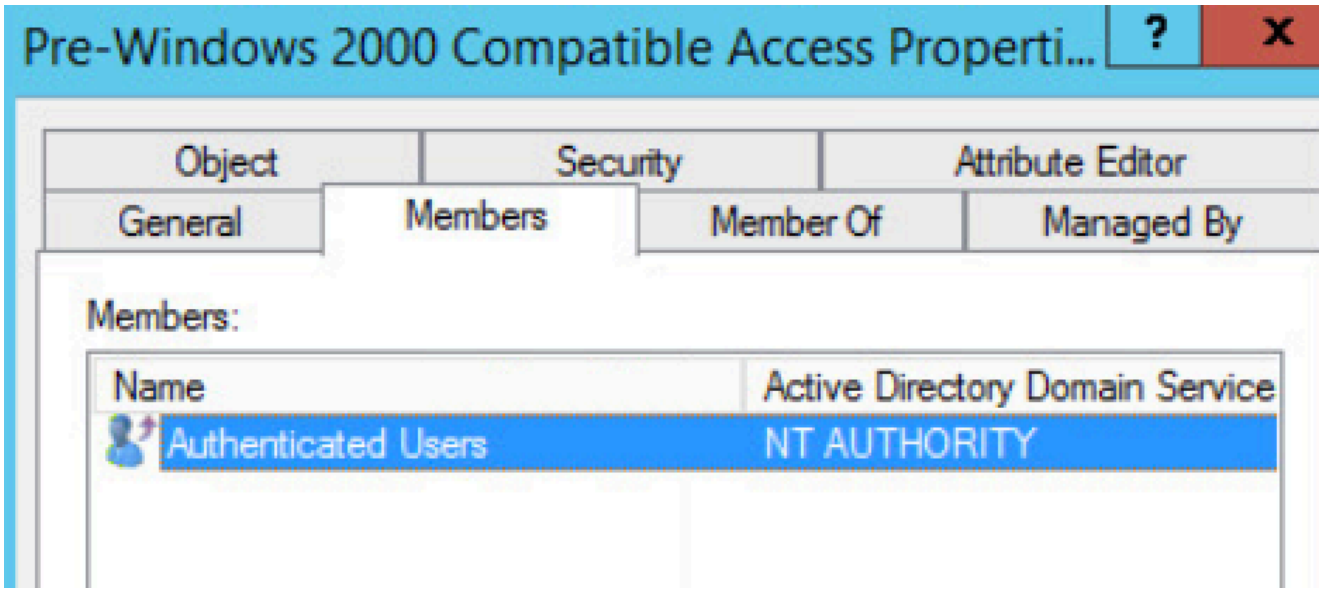


115011616687

- Repita essas etapas para 'objetos do grupo de descendentes' e 'objetos do computador de destino'

2) O grupo Todos os 'Usuários Autenticados' é membro do grupo 'Acesso Compatível com Versões Anteriores ao Windows 2000' que fornece essas configurações a todos os usuários.

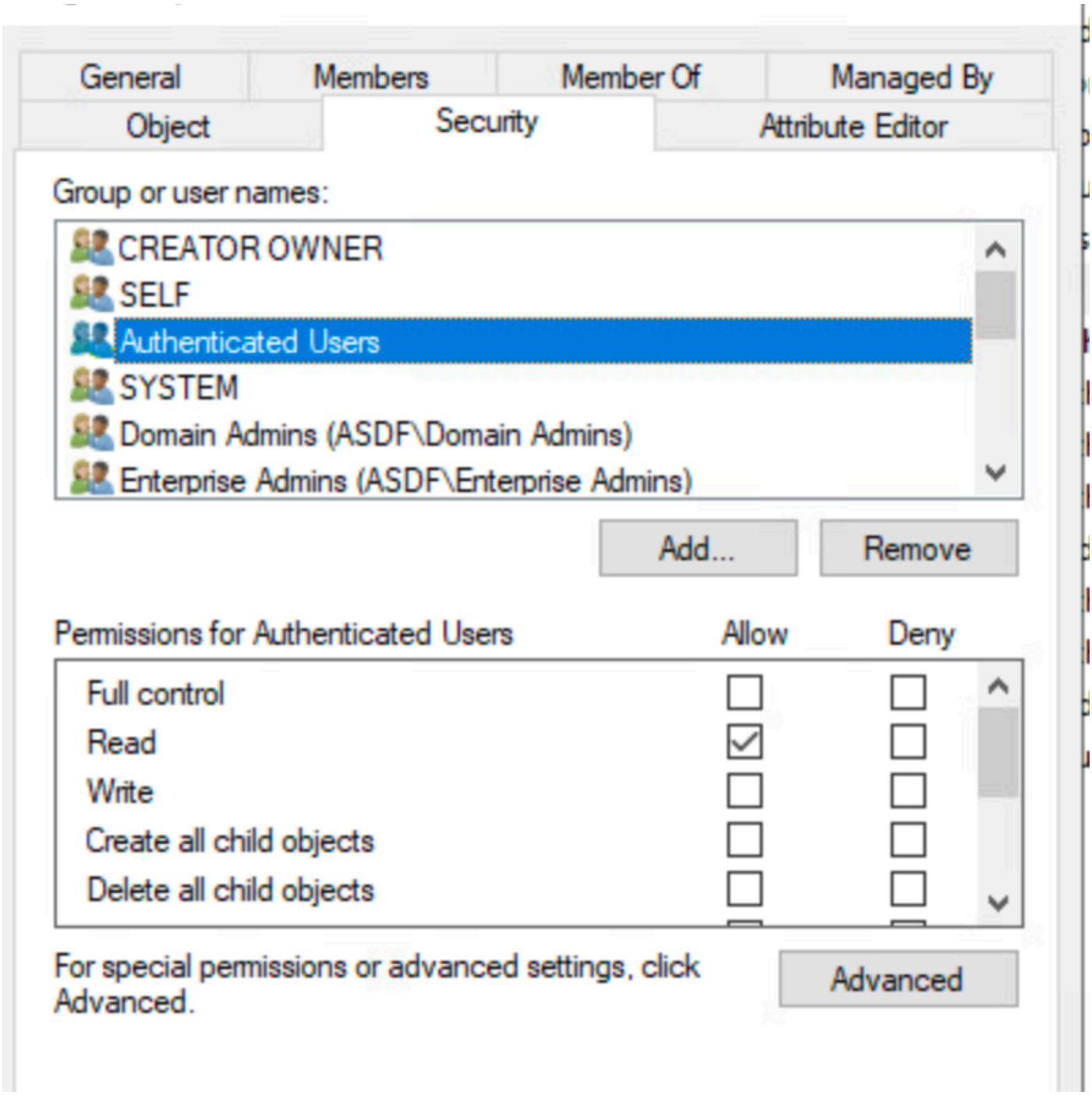
- Clique com o botão direito no grupo Pre-Windows 2000 Compatible Access, que normalmente está no contêiner de AD interno.
- Selecione 'Propriedades' e vá para a guia 'Membros'.
- Verifique se 'Usuários autenticados' está listado.



115011616707

No entanto, em alguns ambientes do AD, esse modelo de permissões pode ter sido alterado e os usuários autenticados foram removidos. Isso pode se manifestar porque alguns usuários estão ausentes do Umbrella Dashboard ou porque as associações de grupo estão incorretas. Se esse for o caso, adicione o usuário do OpenDNS_Connector a esse grupo, reinicie o serviço do conector e os itens ausentes aparecerão no Umbrella.

Em alguns casos raros, isso ainda não resolve o problema. Se você achar que esse é o caso, verifique a guia de segurança de grupos no ative diretory, certifique-se de ver usuários autenticados listados aqui com um check-in de acesso de leitura. Se essa opção não estiver marcada, marque-a e reinicie o serviço do conector para ver se os membros do grupo aparecem. Além disso, se a configuração de segurança não estiver presente em todos os grupos, será necessário aplicar as alterações a todos os grupos globalmente em massa.



28728163336852

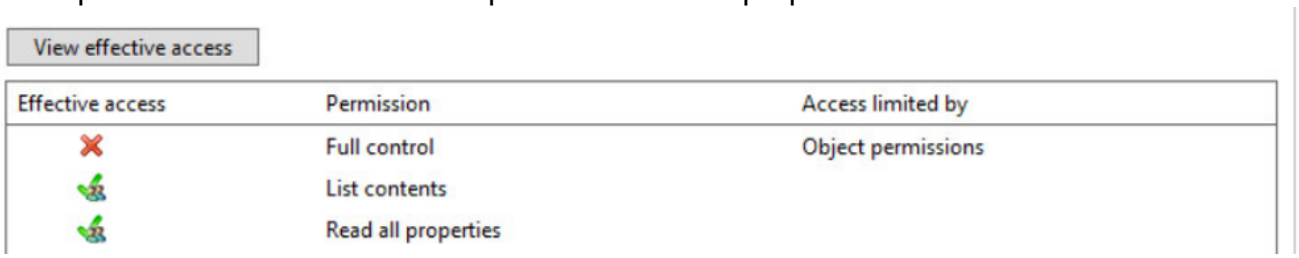
Exibir acesso efetivo

Você pode usar a ferramenta 'Acesso efetivo' do Windows para ver se o usuário do OpenDNS_Connector pode ler um objeto específico que está ausente (ou que tem associação de grupo incorreta).

- Abrir Usuários e Computadores do Ative Diretory
- Clique em 'Exibir' e marque a opção 'Recursos avançados'.
- Localize o objeto de usuário e clique com o botão direito do mouse para selecionar

'Propriedades'

- Vá para 'Segurança > Avançado > Acesso efetivo' (isso pode dizer 'Permissões efetivas')
- Clique em "Selecionar um usuário" e selecione a conta de usuário 'OpenDNS_Connector'.
- Clique em 'OK' e depois em 'Exibir acesso efetivo'
- Verifique se o usuário do conector pode ler todas as propriedades:

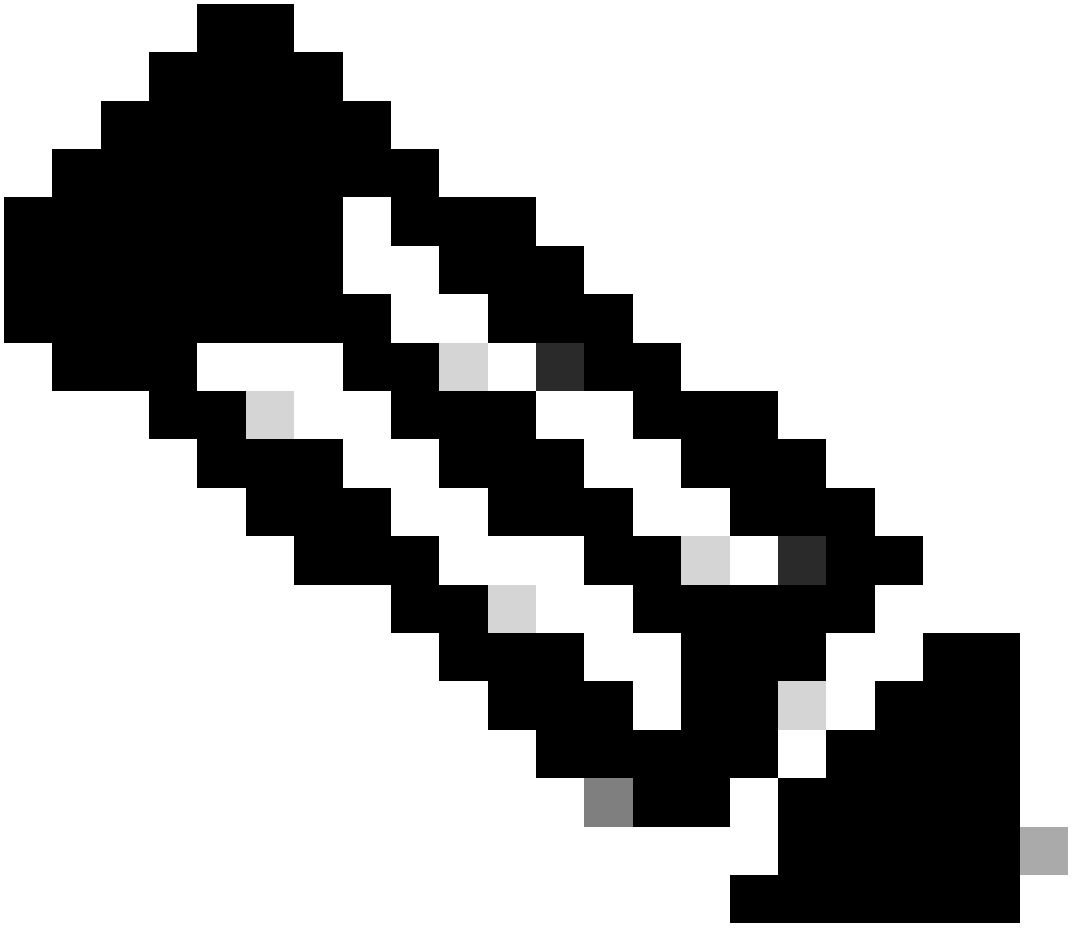


115011616727

Definindo permissões LDAP do OpenDNS_Connector

O assistente 'Delegar Controle' no AD é uma forma rápida de atribuir as permissões necessárias ao usuário 'OpenDNS_Connector':

1) Vá para Ferramentas Administrativas e abra o snap-in Usuários e Computadores do Ative Diretory.
2) Clique com o botão direito do mouse no domínio que inclui o OpenDNS_Connector e selecione "Delegate Control...", depois clique em Next.
3) Adicione o usuário OpenDNS_Connector e clique em Avançar.
4) Selecione "Ler todas as informações do usuário" e clique em Avançar. [Veja a figura 3.]
7) Clique em Finish. [Veja a figura 6.]



Note: Essas etapas podem falhar se a herança for desabilitada em alguns objetos. Para esses objetos, você precisa definir as permissões manualmente.

script userPerms

O script do PowerShell anexado é outro método para obter as permissões de um objeto específico (por exemplo, usuário) no AD. Inclua a saída deste script ao entrar em contato com o suporte técnico da Umbrella.

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.