Solucionar Problemas de Sincronização do Conector AD de Acesso Seguro

Contents

Problema

O Conector AD instalado em um controlador de domínio não está sincronizando corretamente com o Cisco Secure Access. O conector sofre várias falhas de sincronização, incluindo:

- Falhas de sincronização delta com erros de "Acesso negado" (COMException 0x80070005).
- Falhas de leitura do log de eventos do DC com "UnauthorizedAccessException: "Tentativa de executar uma operação não autorizada".
- Problemas de registro na nuvem mostrando "Formato de URI inválido" ao baixar o manifesto.
- HTTP 404 erros "object_not_found" para AssetID específico durante tentativas de sincronização.

O conector parece ter conectividade com o serviço de nuvem do Cisco Secure Access, mas falha no lado das permissões do Ative Diretory e na configuração do registro de nuvem.

Ambiente

- Cisco Secure Access com conector AD
- Conector AD versão 1.15.2
- Conector AD instalado no controlador de domínio
- Conta de serviço personalizada (svcCiscoUmbrella) em vez da conta padrão Cisco_Connector
- Configuração do ambiente de teste/piloto

Resolução

A resolução envolvia resolver problemas de permissões do Ative Diretory e problemas de registro na nuvem por meio de um processo completo de reinstalação:

Passo 1: Verifique e limpe as entradas existentes do conector AD

No painel Acesso seguro, verifique a entrada do Conector AD para o host e remova todas as entradas obsoletas ou duplicadas para o mesmo servidor, se houver.

Passo 2: Certifique-se de que a desinstalação foi concluída

Desinstale completamente o serviço do Conector do AD existente para garantir que nenhuma configuração restante possa causar problemas de registro.

Passo 3: Executar Scripts do Controlador de Domínio

Antes de reinstalar o conector, execute os scripts de configuração apropriados do controlador de domínio para garantir que as permissões apropriadas sejam definidas. O script precisa ser executado em cada controlador de domínio aplicável, embora o próprio conector possa residir fora do controlador de domínio em outro computador associado a um domínio.

Passo 4: Configurar Permissões de Conta de Serviço

Conceda as permissões necessárias do Ative Diretory à conta de serviço:

- Permissões de sincronização do AD (domínio/escopo raiz conforme apropriado):
    - Ler
    - Replicando Alterações de Diretório

    - Replicando todas as alterações de diretório (se necessário no ambiente)
    - Replicando Alterações de Diretório no Conjunto Filtrado (se necessário no ambiente)
- Acesso ao log de eventos no Controlador de Domínio:
    - Adicione a conta de serviço ao grupo Leitores de Log de Eventos.
    - Garanta uma permissão equivalente baseada em política para ler o log de segurança.

Passo 5: Reinstalar o Conector AD

Reinstale o serviço do Conector do AD para gerar um manifesto novo e uma AssetID válida, garantindo o registro apropriado na nuvem.

Passo 6: Reiniciar e validar

Após a instalação e a configuração de permissão:

1. Reinicie o serviço do Conector AD.
2. Monitore os registros do conector para confirmar o acesso negado e a interrupção de erros não autorizados.
3. Verifique se as entradas de sincronização bem-sucedidas aparecem nos logs (por exemplo, "ADSync LDIF RESPONSE: 200 Success").

Causa

Os problemas de sincronização foram causados por dois fatores principais:

1. Permissões Insuficientes do Ative Diretory: A conta de serviço personalizada (svcCiscoUmbrella) não tinha as permissões do AD necessárias para sincronização delta e acesso ao log de eventos do DC, resultando em erros de "Acesso negado" e "UnauthorizedAccessException".
2. Problemas de registro na nuvem: A instância do conector estava registrada incorretamente

ou apontando para um AssetID inválido/antigo, causando erros de "Formato de URI inválido" ao baixar o manifesto e erros HTTP 404 "object_not_found" durante tentativas de sincronização.

Esses problemas foram agravados por procedimentos de instalação incompletos em que os scripts de configuração do controlador de domínio não foram executados corretamente antes da instalação do conector.

Conteúdo relacionado

- Configuração do Conector AD do Cisco Secure Access
- Requisitos de permissões do conector AD
- Guia de Instalação do Conector AD
- Solução de problemas do conector AD
- Configuração da Conta de Serviço do Conector do AD
- Suporte técnico e downloads da Cisco

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.