

Problemas de desempenho de consulta de grupos externos do ISE 3.5 EntraID e resolução de permissão da API do Microsoft Graph

Contents

Problema

A configuração do Cisco ISE 3.5 patch2 com EntraID REST ID Store sofre atrasos significativos de autenticação durante a autenticação EAP-TLS ao consultar EntraID.ExternalGroups. A fase PIP consultado - EntraID.ExternalGroups leva mais de 30 segundos para ser concluída, fazendo com que os clientes EAP expirem e reiniciem a autenticação, impedindo a conclusão bem-sucedida da sessão.

Além disso, ao tentar salvar atributos de grupo na configuração do armazenamento de ID ENTRAID REST, esta mensagem de erro é exibida:

```
java.rmi.RemoteException: null; nested exception is: java.lang.NullPointerException
```

Os logs de autenticação mostram erros PIP assíncronos e suspensão do mecanismo de política durante o processo de pesquisa de grupos externos. O problema se manifesta como fluxos de trabalho de autenticação com falha em que os clientes não podem concluir sessões EAP devido aos tempos de consulta estendidos.

Ambiente

- Cisco Identity Services Engine (ISE) versão 3.5.0.527 com Patch 2
- Integração do Microsoft EntraID (Azure Ative Directory) via Repositório de ID REST
- Autenticação EAP-TLS configurada

- Origem REST configurada para EntraID com recuperação de atributo de grupo
- Problema observado no ISE 3.4 patch4/patch5 e ISE 3.5 patch2/patch3

Resolução

A resolução envolve a concessão das permissões corretas da API do Microsoft Graph para o aplicativo Azure usado pela integração do ISE EntraID REST ID Store.

Passo 1: Conceder Permissões de API do Microsoft Graph Necessárias

Navegue até o portal do Azure e localize o registro do aplicativo usado para integração do ISE. Conceder esta permissão de API do tipo Aplicativo:

`Directory.Read.All`

Verifique se o consentimento do administrador foi concedido para esta permissão.

Passo 2: Reinicie os serviços do ISE

Após conceder a permissão `Directory.Read.All`, reinicie os serviços em todos os nós do ISE para garantir que as novas permissões sejam aplicadas.

Passo 3: Verificar resolução

Teste o processo de autenticação para confirmar se a fase PIP consultado - `EntraID.ExternalGroups` é concluída dentro de prazos aceitáveis e se os atributos do grupo podem ser salvos sem erros.

Os logs de resolução devem mostrar a conclusão bem-sucedida sem o `AsynchronousPIPError`:

2026-05-26 14:21:47,981 DEBUG [I/O dispatcher 1][[]] cisco.ise.ropc.utilities.HttpClientWrapper -:::-

Causa

O problema é causado pelo bug da Cisco ID CSCwu13703, que afeta o ISE 3.5 patch 3 e versões relacionadas. O bug está relacionado a permissões insuficientes da API do Microsoft Graph para a integração do EntraID. Sem a permissão Directory.Read.All adequada, o ISE não pode consultar grupos externos de forma eficiente da EntraID, resultando em condições de tempo limite e suspensão do mecanismo de política por meio de exceções AsynchronousPIPEError.

O processo de autenticação falha porque cada avaliação malsucedida faz com que o mecanismo de política acione AsynchronousPIPEError e suspenda o fluxo de trabalho de autenticação, levando aos tempos de consulta estendidos e ao eventual tempo limite do cliente.

Conteúdo relacionado

- [ID de bug Cisco CSCwu13703](#)
- [Guia de Configuração do Cisco ISE com Microsoft Ative Directory Entra ID e Intune](#)

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.