Resolver falhas incompletas de perfil CTS e de download SGACL em dispositivos IOS-XE integrados com o Cisco ISE

Contents

Problema

Você observa perfis parciais ou incompletos do Cisco TrustSec (CTS) em dispositivos de rede mesmo quando a lista de servidores CTS e os dados do ambiente estão presentes. O dispositivo de rede não consegue fazer o download das entradas de controle de acesso (ACEs) da lista de controle de acesso do grupo de segurança (SGACL).

Esse problema afeta as implantações que usam dispositivos de rede Cisco IOS® XE, como switches da série Catalyst 9000, controladores Wireless LAN (WLC) e roteadores com Identity Services Engine (ISE).

Este erro aparece nos logs de dispositivo de rede:

```
%CTS-2-AUTHZ_POLICY_SGACL_ACE_FAILED: Failed to download ACEs for SGACL '<ACLname>' for SGT='<SGTnumber>
```

Ambiente

- Patch 2 do ISE 3.5
- Patch 8 do ISE 3.3
- Patch 9 do ISE 3.2
- ambiente CTS
- Dispositivos de rede IOS-XE como Cat9k, WLC e roteadores

Resolução

Opção A: Atualizar ISE (recomendado)

Para resolver permanentemente esse problema, atualize o Cisco ISE para uma versão fixa onde o bug da Cisco ID CSCws51319 é resolvido.

- Versões fixas:
    - ISE 3.5 Patch 3 ou mais recente
    - ISE 3.3 Patch 9 ou mais recente
    - ISE 3.2 Patch 10 ou mais recente

Opção B: Atualização manual de políticas (solução alternativa)

Se uma atualização não for possível imediatamente, você deverá disparar manualmente uma atualização de política no dispositivo de rede sempre que uma alteração de política for feita no ISE.

1. Acesse o CLI do dispositivo de rede afetado.

2. Execute este comando para verificar o status da PAC CTS.

```
show cts pac
```

3. Para verificar se os dados do ambiente CTS estão presentes, execute o comando:

```
show cts environment data
```

4. Para verificar as permissões atuais da política, execute:

```
show cts role-based permissions
```

5. Execute o comando para atualizar a política:

```
cts refresh policy
```

6. Aguarde alguns minutos para que o download seja concluído.

7. Verifique a condição da política atual e confirme se todas as permissões foram baixadas usando este comando:

```
show cts role-based permissions
```

Causa

Esse problema é devido à ID de bug Cisco CSCws51319.

Conteúdo relacionado

- ID de bug Cisco CSCws51319
- 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.