解決與思科ISE整合的IOS-XE裝置上的不完整CTS配置檔案和SGACL下載故障

目錄

問題

即使存在CTS伺服器清單和環境資料，您仍會觀察到網路裝置上的部分或不完整的Cisco TrustSec(CTS)配置檔案。網路裝置無法下載安全組訪問控制清單(SGACL)訪問控制條目(ACE)。

此問題會影響使用Cisco IOS® XE網路裝置(例如Catalyst 9000系列交換機、無線LAN控制器(WLC)和具備身份服務引擎(ISE)的路由器)的部署。

此錯誤出現在網路裝置日誌中：

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

環境

- ISE 3.5補丁2
- ISE 3.3補丁8
- ISE 3.2補丁9
- CTS環境
- IOS-XE網路裝置，如Cat9k、WLC和路由器

解析

選項 A：升級ISE（推薦）

若要永久解決此問題，請將Cisco ISE升級至已解決思科錯誤ID CSCws51319的固定版本。

- 已修復版本：
  - ISE 3.5補丁3或更高版本
  - ISE 3.3補丁9或更高版本
  - ISE 3.2補丁10或更高版本

選項 B：手動策略刷新（解決方法）

如果無法立即進行升級，則在ISE中更改策略時，必須手動觸發網路裝置上的策略刷新。

1.訪問受影響網路裝置的CLI。

2.運行此命令以驗證CTS PAC狀態。

```
show cts pac
```

3.要驗證CTS環境資料是否存在，請運行命令：

```
show cts environment data
```

4.要檢查當前策略許可權，請運行：

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

5.運行命令以刷新策略：

```
cts refresh policy
```

6.請等待幾分鐘以使下載完成。

7.檢查當前策略條件並確認是否使用以下命令下載了所有許可權：

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

原因

此問題是由思科錯誤ID CSCws51319導致的。

相關內容

- 思科錯誤ID CSCws51319
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。