Risoluzione dei problemi di download di CTS Profile e SGACL incompleti sui dispositivi IOS-XE integrati con Cisco ISE

Sommario

Problema

È possibile osservare profili Cisco TrustSec (CTS) parziali o incompleti sui dispositivi di rete anche quando sono presenti l'elenco dei server CTS e i dati dell'ambiente. Il dispositivo di rete non riesce a scaricare le voci di controllo di accesso (ACE, Access Control List) SGACL (Security Group Access Control List).

Questo problema interessa le implementazioni che utilizzano dispositivi di rete Cisco IOS® XE, quali switch Catalyst serie 9000, Wireless LAN Controller (WLC) e router con Identity Services Engine (ISE).

Questo errore viene visualizzato nei registri dei dispositivi di rete:

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

Ambiente

- ISE 3.5 patch 2
- ISE 3.3 patch 8
- ISE 3.2 patch 9
- ambiente CTS
- Dispositivi di rete IOS-XE come Cat9k, WLC e router

Risoluzione

Opzione A. Aggiorna ISE (scelta consigliata)

Per risolvere definitivamente il problema, aggiornare Cisco ISE a una versione fissa in cui è stato risolto l'ID bug Cisco CSCws51319.

- Versioni fisse:
  - ISE 3.5 Patch 3 o versione successiva
  - ISE 3.3 Patch 9 o versione successiva
  - ISE 3.2 Patch 10 o versione successiva

Opzione B. Aggiornamento manuale dei criteri (soluzione alternativa)

Se l'aggiornamento non è immediatamente possibile, è necessario attivare manualmente un aggiornamento dei criteri sul dispositivo di rete ogni volta che viene apportata una modifica ai criteri in ISE.

1. Accedere alla CLI del dispositivo di rete interessato.

2. Eseguire questo comando per verificare lo stato della PAC CTS.

```
show cts pac
```

3. Per verificare la presenza dei dati dell'ambiente CTS, eseguire il comando:

```
show cts environment data
```

4. Per verificare le autorizzazioni correnti per i criteri, eseguire:

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

5. Eseguire il comando per aggiornare il criterio:

```
cts refresh policy
```

6. Attendere alcuni minuti per il completamento del download.

7. Controllare la condizione del criterio corrente e verificare se tutte le autorizzazioni vengono scaricate utilizzando questo comando:

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

Causa

il problema è dovuto all'ID bug Cisco CSCws51319.

Contenuto correlato

- Cisco ID bug CSCws51319
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).