

ISE 3.2 MDM Compliance Query non riuscita a causa di soppressione del client e problemi software

Sommario

Problema

Alcuni endpoint autenticati tramite EAP-TLS su Cisco Identity Services Engine (ISE) non ricevono a intermittenza uno stato di conformità da Microsoft Intune, anche se vengono visualizzati come conformi nel dashboard di Intune. Di conseguenza, tali endpoint hanno utilizzato un criterio di autorizzazione wireless predefinito anziché il criterio Posture Compliant o Posture Non Compliant previsto. Gli endpoint interessati non mostrano gli attributi di conformità MDM (Mobile Device Management) nei log ISE in tempo reale o nei report MDM esterni e il problema interessa solo un sottoinsieme di client nella distribuzione.

I sintomi specifici osservati includono:

- I client anormali non dispongono di log in ISE Report in External Mobile Device Management Report.
- I client anormali non dispongono di attributi quali lo stato di conformità MDM o lo stato di conformità del dispositivo nei dettagli di log attivi.
- I client anormali utilizzano il criterio di autorizzazione wireless 802.1x_EAP-TLS_toyotawi anziché il criterio di conformità alla postura.
- Nei log vengono visualizzati messaggi di errore indicanti "Impossibile connettersi al server MDM: 404 Non Trovato".

Ambiente

- Cisco ISE multi-node cluster versione 3.2 patch 6

- 8 nodi ISE nel cluster, tutti con stato verde
- 11.000 client wireless/cablati integrati con Microsoft Intune
- I client utilizzano l'autenticazione EAP-TLS (certificato computer)
- ISE utilizza l'indirizzo MAC del client per le query su Intune
- Tutti i client hanno lo stato di conformità nel dashboard di Microsoft Intune
- Il problema riguarda alcuni client ma non tutti

Risoluzione

Il problema è stato risolto attraverso questi passaggi.

Passaggio 1: Identificazione della root cause

L'analisi dei log ISE ha rilevato che gli endpoint interessati dispongono di un ID server MDM non aggiornato che impedisce l'esecuzione delle query MDM.

I registri riportavano:

```
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MDMUtil -:::::- M
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MdmServersCache -
2026-06-15 13:35:14,344 ERROR [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.pip.MdmPartnerPIPHandl
```

È stato inoltre rilevato che la distribuzione ha raggiunto l>ID bug Cisco CSCwv51917, il che influisce sulle ricerche di conformità MDM quando l'indirizzo MAC contiene un ID server MDM non aggiornato.

Passaggio 2: Soluzione temporanea

Come soluzione temporanea:

1.- Eliminare l'endpoint da Visibilità contesto e rieseguire l'autenticazione. È stato osservato per risolvere il problema relativo all'esecuzione di query sul server MDM e all'acquisizione dello stato di conformità.

2.- Passare a Visibilità contesto.

3.- Selezionare l'indirizzo MAC dell'endpoint ed eliminarlo.

4.- Autenticare nuovamente l'endpoint.

Passaggio 3: Risoluzione permanente - Aggiornamento software

La risoluzione permanente è tracciata con l'ID bug Cisco CSCwv51917.

Causa

Durante l'autenticazione, ISE tenta di eseguire una query sul riferimento al server MDM non aggiornato, ma l'oggetto server MDM corrispondente non esiste più o non è attivo. Di conseguenza, ISE non recupera gli attributi di conformità MDM da Intune.

Contenuto correlato

- [ID bug Cisco CSCwv519173134](#)
- [Note sulla release di ISE 3.2 - Avvertenze risolte](#)
- [Avviso di fine del ciclo di vita per ISE 3.2](#)
- [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).