

ISE 3.2 MDM Compliance Query mislukt door onderdrukking van client en softwaredefect

Inhoud

uitgifte

Sommige eindpunten die via EAP-TLS op Cisco Identity Services Engine (ISE) zijn geverifieerd, krijgen van Microsoft Intune af en toe geen nalevingsstatus, hoewel ze in het Intune-dashboard als conform worden weergegeven. Als gevolg daarvan hebben deze eindpunten een standaard beleid voor draadloze autorisatie in plaats van het verwachte beleid voor Posture Compliant of Posture Non-Compliant. De betreffende eindpunten tonen geen compatibiliteitskenmerken voor Mobile Device Management (MDM) in ISE-livlogs of externe MDM-rapporten en het probleem heeft alleen invloed op een subset van clients in de implementatie.

Specifieke symptomen die zijn waargenomen zijn:

- Abnormale clients hebben geen logs in ISE Report bij External Mobile Device Management Report.
- Abnormale clients hebben geen kenmerken zoals MDM-compatibele status of apparaatcompatibele status in live loggegevens.
- Abnormale clients hebben het beleid voor draadloze 802.1x_EAP-TLS_toyotawifi goedgekeurd in plaats van het beleid voor naleving van de houding.
- Foutberichten in logboeken tonen "Kan geen verbinding maken met MDM Server: 404 niet gevonden".

milieu

- Cisco ISE multi-node cluster versie 3.2 patch 6
- 8 ISE-nodes in het cluster, die allemaal de groene status weergeven
- 11.000 draadloze/bekabelde clients geïntegreerd met Microsoft Intune

- Clients gebruiken EAP-TLS-verificatie (Machine Certificate)
- ISE gebruikt het MAC-adres van de client voor query's naar Intune
- Alle clients hebben de status 'compliant' op het Microsoft Intune-dashboard
- Probleem treft sommige klanten, maar niet allemaal

resolutie

Het probleem is via deze stappen opgelost.

Stap 1: Identificeer de oorzaak

Analyse van de ISE-logs toonde aan dat de getroffen eindpunten een verouderde MDM-server-ID hebben die voorkomt dat MDM-query's worden uitgevoerd.

De logboeken toonden aan:

```
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
```

Bovendien bleek de implementatie Cisco bug ID CSCwv51917 te raken, wat van invloed is op MDM compliance lookups wanneer het gebruik van een MAC-adres een verouderde MDM server-ID heeft.

Stap 2: Tijdelijke workaround

Als tijdelijke workaround:

1.- Verwijder het eindpunt uit Context Visibility en authentickeer opnieuw. Dit werd waargenomen om het probleem van het vragen naar de MDM-server en het verkrijgen van de nalevingsstatus op te lossen.

2.- Navigeer naar Context Visibility.

3.- Selecteer het MAC-adres van het eindpunt en verwijder het.

4.- Verifieer het eindpunt opnieuw.

Stap 3: Permanente resolutie - Software-upgrade

De permanente resolutie wordt gevolgd onder Cisco bug ID CSCwv51917.

Oorzaak

Tijdens de verificatie probeert ISE de verouderde MDM-serverreferentie te bevragen, maar het corresponderende MDM-serverobject bestaat niet meer of is inactief. Bijgevolg haalt ISE geen MDM-conformiteitskenmerken op van Intune.

Gerelateerde inhoud

- [Cisco bug ID CSCwv519173134](#)
- [ISE 3.2 Release Notes - Opgeloste voorbehouden](#)
- [ISE 3.2 Mededeling betreffende het einde van de levensduur](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.