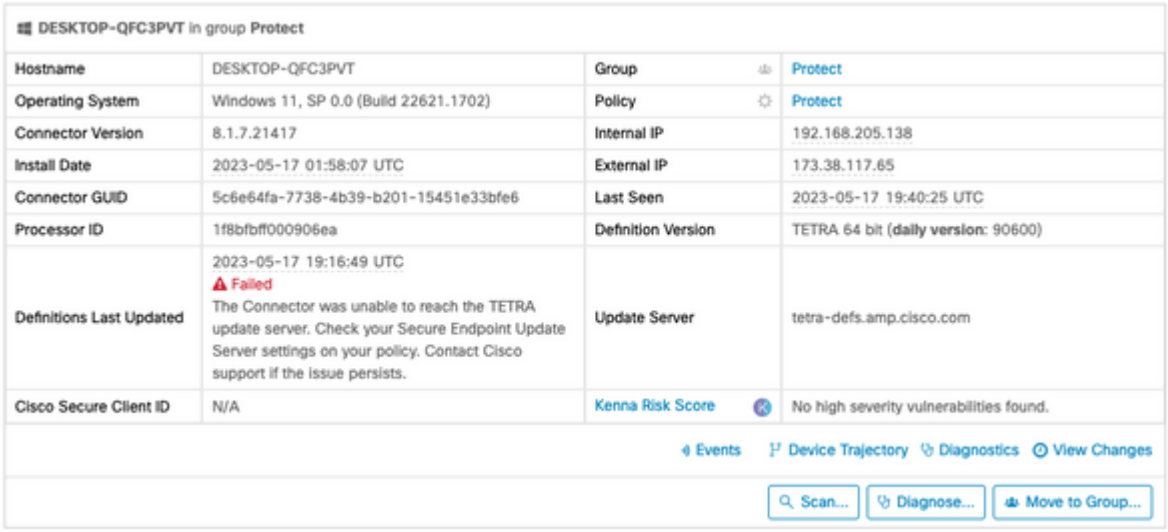
Probleemoplossing TETRA definities update fouten

Inhoud

Inleiding

Dit document beschrijft de stappen die moeten worden gevolgd om de reden te onderzoeken waarom er eindpunten zijn die de TETRA-definities niet kunnen bijwerken vanaf Cisco TETRA-definities update servers.

Definitions Laatst bijgewerkt fout gezien op de Secure Endpoint console verschijnt onder de Computer details zoals hieronder te zien.



â€ƒ

Probleemoplossing

Cisco Secure Endpoint voor Windows vereist een duurzame verbinding met de TETRA-definitieserver om updates te kunnen downloaden.

Veel voorkomende fouten in het downloaden van de TETRA-definities zijn:

- Geen oplossing voor serveradres
- Geen validering van het SSL-certificaat (inclusief controle van de certificaatintrekkingslijst)
- Onderbreking tijdens de download
- Geen verbinding met de proxyserver
- Niet verifiëren bij de proxyserver

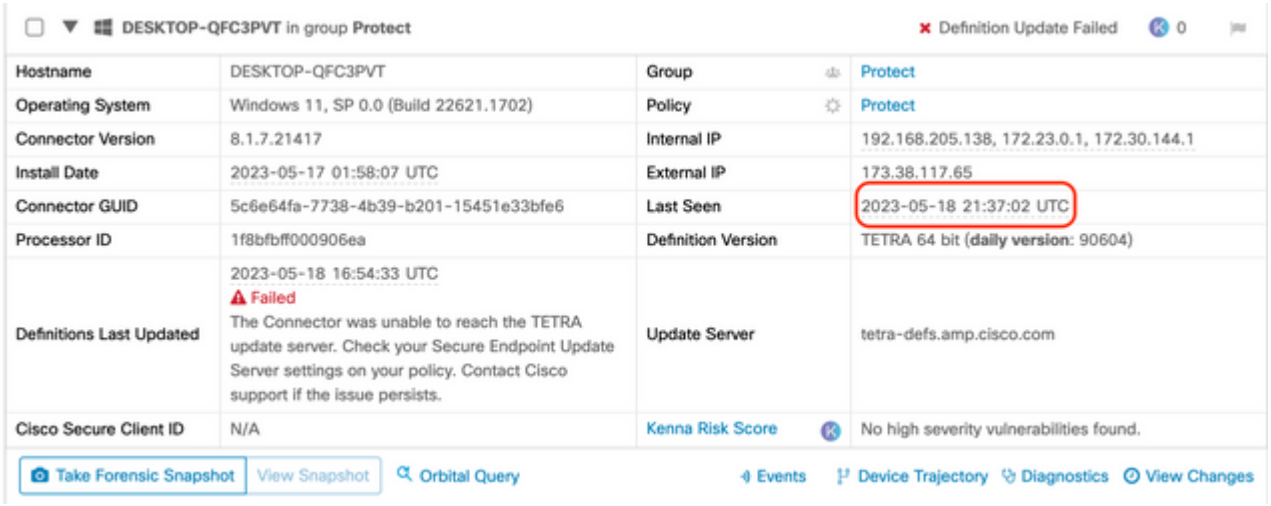
Als er een fout optreedt tijdens het downloaden van de TETRA-definities, zal de volgende poging plaatsvinden op het volgende update-interval of als een handmatige update wordt gestart door de gebruiker.

Connectiviteit met gerapporteerde endpoints controleren op de beveiligde endpointconsole

De Secure Endpoint Console toont of het eindpunt regelmatig verbinding maakt. Zorg ervoor dat uw endpoints actief zijn en een recente status hebben die â€˜Laatst gezienâ€™ is. Als de eindpunten niet inchecken met de Secure Endpoint Console, dan geeft dit aan dat het eindpunt niet actief is of bepaalde connectiviteitsproblemen heeft.

Cisco geeft dagelijks gemiddeld vier definitie-updates uit en als dat op enig moment van de dag het geval is, als het eindpunt de update niet kan downloaden, dan geeft de connector een foutmelding. Gezien deze frequentie, slechts als de eindpunten constant worden verbonden, en een stabiele netwerkverbinding aan de server van TETRA door hebben, dan zullen de eindpunten als "binnen Beleid"rapporteren.

De status "Laatst gezien" staat op de pagina Computergegevens, zoals hieronder wordt weergegeven:

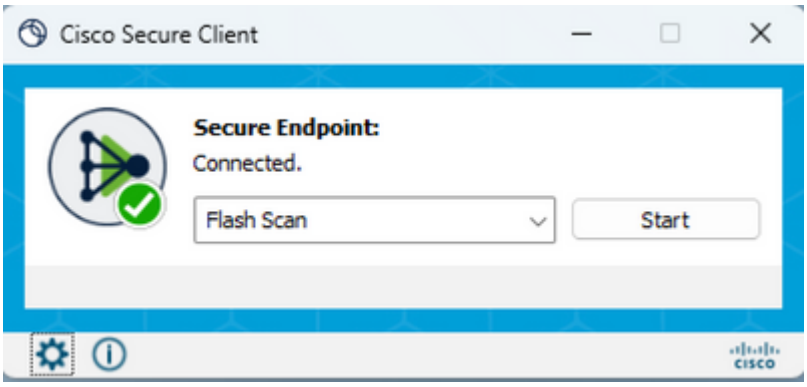


Als het eindpunt verbinding maakt en er een fout wordt gemeld dat de definities niet worden gedownload maar door de console worden gezien, dan kan het probleem intermitterend zijn. Verder onderzoek is mogelijk als er grote tijdsverschillen zijn tussen "Laatst gezien" en "Definitions Laatst bijgewerkt".

Connectiviteit op het eindpunt controleren

Eindgebruikers kunnen de connectiviteit controleren met de UI-interface.

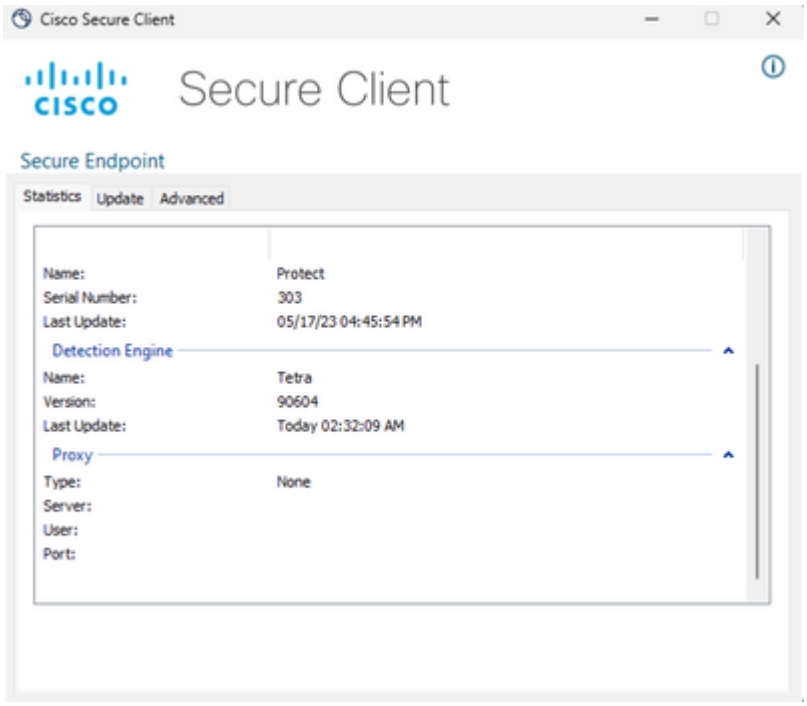
Wanneer u de beveiligde Cisco-client opent, wordt de connectiviteitsstatus weergegeven.



De Connectivity Tool kan worden gebruikt wanneer het eindpunt niet is verbonden en verbindingsproblemen worden gemeld. Dit is opgenomen in de IPS Support Tool die het ondersteuningspakket genereert.

De TETRA-definities op het eindpunt bekijken

Cisco Secure Client biedt informatie over de huidige TETRA-definities die door de endpointconnector zijn geladen. De eindgebruiker kan de client openen en de instellingen voor Secure Endpoint controleren. Op het tabblad Statistieken is de huidige definitie van TETRA beschikbaar.



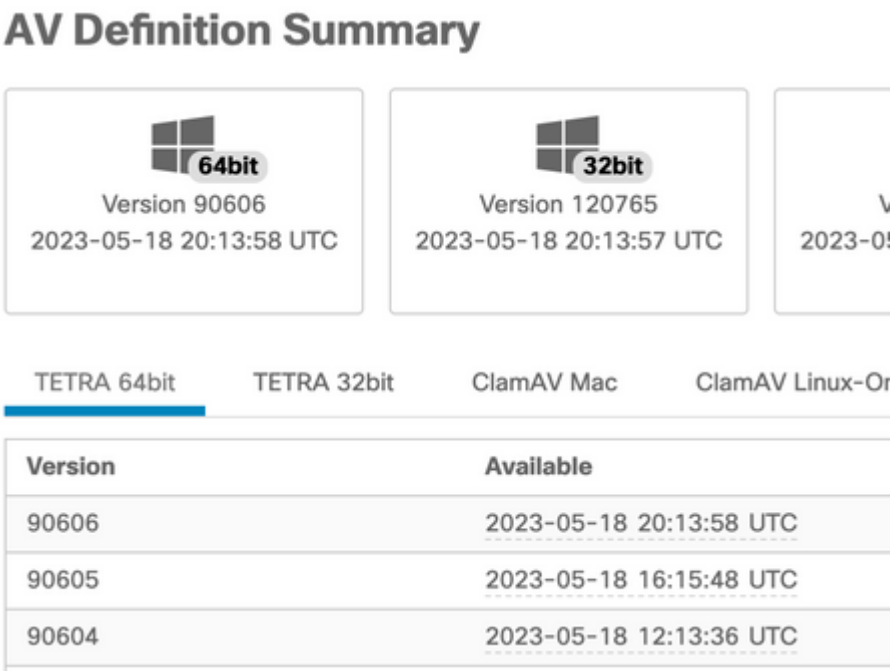
â€f

Ook worden de huidige TETRA-definitiedetails gerapporteerd door de AmpCLI-tool op het eindpunt. Een voorbeeld van de opdracht is:

```
PS C:\Program Files\Cisco\AMP\8.1.7.21417> .\AmpCLI.exe posture
{"agent_uuid":"5c6e64fa-7738-4b39-b201-15451e33bfe6","connected":true,"connector_version":"8.1.7","engir
```

De definitieversies worden weergegeven voor elk van de motoren, inclusief TETRA. In deze output hierboven, is het versie 90604. Dit kan worden vergeleken met de Secure Endpoint Console onder:

Management > AV Definition Samenvatting. Een voorbeeld van de pagina is zoals hieronder.



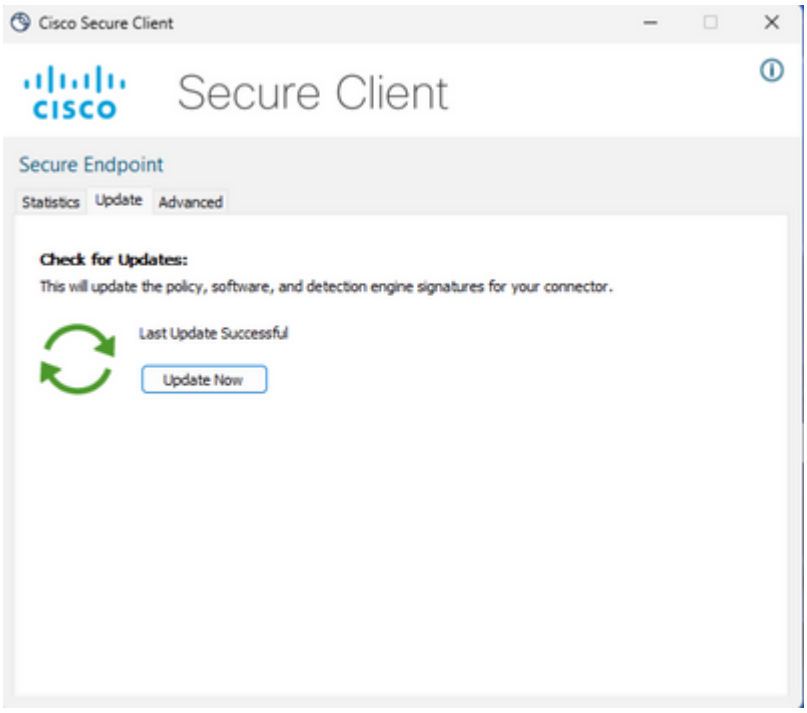
â€ƒ

Als de versie nog achterloopt en de status van de connector is aangesloten, kan er een update van de definities of een controle van de eindpuntverbinding met de TETRA-server worden uitgevoerd.

Forceren van een TETRA definities update op het Endpoint

Eindgebruikers kunnen de TETRA download voortgang inhuren en controleren. De gebruiker kan de update alleen activeren als de optie in het beleid is ingesteld. Onder de pagina **Geavanceerde instellingen > Clientgebruikersinterface** beleidsinstellingen, moeten de instellingen **Gebruiker toestaan om TETRA-definities bij** te **werken** ingeschakeld zijn om de definities door de gebruiker te activeren.

In de beveiligde client voor Cisco kan de eindgebruiker de client openen en de instellingen voor beveiligde endpoints controleren. De gebruiker kan op "Update nu" klikken om de TETRA definitie update te activeren zoals hieronder getoond:



Als u AMP for Endpoints Connector versie 7.2.7 en hoger uitvoert, kunt u een nieuwe switch "-forceupdate" gebruiken om de connector te dwingen de TETRA-definities te downloaden.

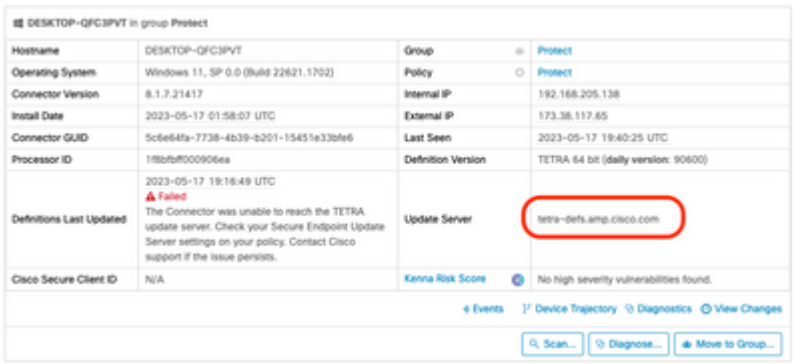
```
C:\Program Files\Cisco\AMP\8.1.7.21417\sfc.exe -forceupdate
```

Nadat de update wordt gedwongen, kan de definitie van TETRA opnieuw worden gecontroleerd om te zien of een update voorkomt. Als er nog steeds geen update plaatsvindt, moet de verbinding met de TETRA-server worden gecontroleerd.

De connectiviteit van de TETRA-definitieserver op het endpoint controleren

Het beleid van het eindpunt omvat de definitieserver dat het eindpuntcontact om de definities te downloaden.

De pagina met computergegevens bevat de updateserver. De onderstaande afbeelding toont waar de updateserver wordt weergegeven:



â€ƒ

Op Public Cloud wordt de vereiste servernaam waarmee het eindpunt verbinding kan maken, vermeld onder:

Vereiste serveradressen voor juiste Cisco Secure Endpoint en Malware Analytics Operations

Rechtstreekse aansluitingsvalidatie

Vanaf het eindpunt kan de volgende opdracht worden uitgevoerd om DNS-lookup naar de updateserver te controleren:

```
PS C:\Program Files\Cisco\AMP> Resolve-DnsName -Name tetra-defs.amp.cisco.com
Name                           Type TTL Section IPAddress
----                           ---- --- ------- ---------
tetra-defs.amp.cisco.com       A    5   Answer  192.XXX.X.XX
tetra-defs.amp.cisco.com       A    5   Answer  192.XXX.X.X
tetra-defs.amp.cisco.com       A    5   Answer  192.XXX.X.X
```

Als de IP-verbinding tot stand is gebracht, kan de verbinding met de server worden getest. Een geldig antwoord ziet er als volgt uit:

<#root>

```
PS C:\Program Files\Cisco\AMP> curl.exe -v https://tetra-defs.amp.cisco.com
* Trying 192.XXX.X.X:443...
* Connected to tetra-defs.amp.cisco.com (192.XXX.X.X) port 443 (#0)
* schannel: disabled automatic use of client certificate
* ALPN: offers http/1.1
* ALPN: server did not agree on a protocol. Uses default.
* using HTTP/1.x
> GET / HTTP/1.1
> Host: tetra-defs.amp.cisco.com
> User-Agent: curl/8.0.1
> Accept: */*
>
* schannel: server closed the connection
```

< HTTP/1.1 200 OK

```
< Date: Fri, 19 May 2023 19:13:35 GMT
< Server:
< Last-Modified: Mon, 17 Apr 2023 15:48:54 GMT
< ETag: "0-5f98a20ced9e3"
< Accept-Ranges: bytes
< Content-Length: 0
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
* Closing connection 0
* schannel: shutting down SSL/TLS connection with tetra-defs.amp.cisco.com port 443
```

Als de verbinding niet tot valdate van het certificaat met de CRL server kan worden gemaakt (zoals commercial.ocsp.identrust.com of validation.identrust.com), dan zal een fout als volgt worden gezien:

```
PS C:\Program Files\Cisco\AMP> curl.exe -v https://tetra-defs.amp.cisco.com
```

```
* Trying 192.XXX.X.XX:443...
* Connected to tetra-defs.amp.cisco.com (192.XXX.X.XX) port 443 (#0)
* schannel: disabled automatic use of client certificate
* ALPN: offers http/1.1
* schannel: next InitializeSecurityContext failed: Unknown error (0x80092013) - The revocation function
* Closing connection 0
* schannel: shutting down SSL/TLS connection with tetra-defs.amp.cisco.com port 443
curl: (35) schannel: next InitializeSecurityContext failed: Unknown error (0x80092013) - The revocation
```

Proxy-validatie

Als het eindpunt is geconfigureerd om een proxy te gebruiken, kan de laatste foutstatus worden gecontroleerd. De PowerShell hieronder uitvoeren kan de laatste fout van TETRA update poging teruggeven.

```
PS C:\Program Files\Cisco\AMP> (Select-Xml -Path local.xml -XPath '//tetra/lasterror').Node.InnerText
```

Laatste foutcode	Probleem	Acties
4294965193	Kan geen verbinding met de proxy worden vastgesteld	Controleer netwerkverbinding met de proxy
4294965196	Kan niet authenticeren met proxy	Controleer de verificatie-referenties voor de proxy
4294965187	Verbonden met de proxy en downloaden mislukt	Proxy-logbestanden controleren op downloadproblemen

Aanvullende informatie

- Als u eindpunten ziet die voortdurend de TETRA-definities niet kunnen downloaden ondanks de bovenstaande controles, moet u de Connector in de debug-modus inschakelen voor een tijdsinterval dat gelijk is aan het update-interval zoals gedefinieerd in uw beleid en moet u de ondersteuningsbundel genereren. Wanneer de connector in de debug-modus staat, moet u er rekening mee houden dat het Wireshark-pakket ook wordt opgenomen. De pakketopname moet ook worden uitgevoerd voor een tijdsinterval dat gelijk is aan het updateinterval dat in uw beleid is gedefinieerd. Nadat deze informatie is verzameld, opent u een Cisco TAC-case samen met deze informatie voor verder onderzoek.

Verzameling van diagnostische gegevens via AMP voor Windows Connector

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.