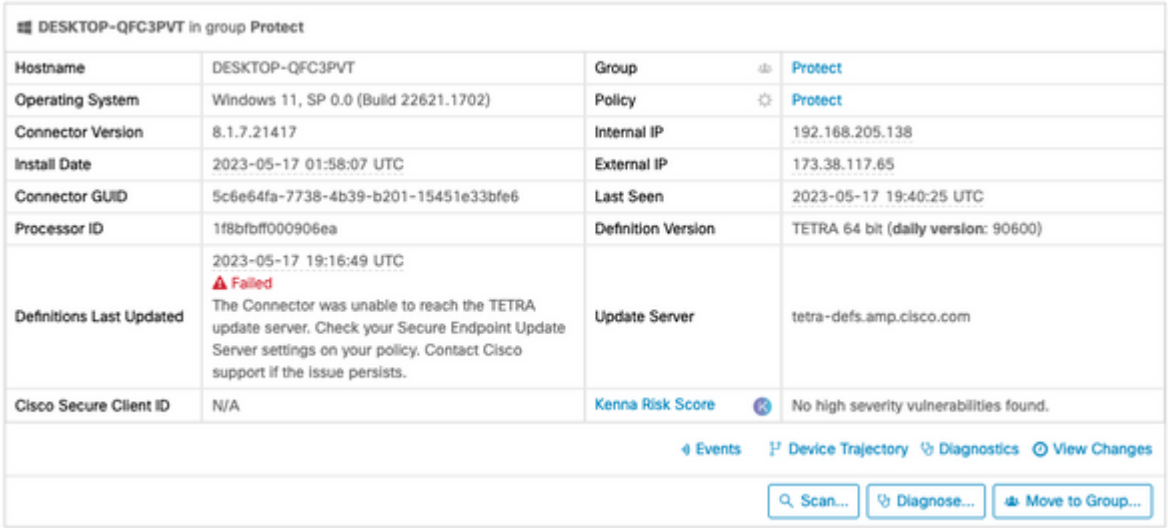
Risoluzione dei problemi relativi agli errori di aggiornamento delle definizioni TETRA

Sommario

Introduzione

Questo documento descrive i passaggi da seguire per indagare il motivo per cui gli endpoint non sono in grado di aggiornare le definizioni TETRA dai server di aggiornamento delle definizioni Cisco TETRA.

L'errore Ultimo aggiornamento delle definizioni visualizzato in Secure Endpoint Console viene visualizzato sotto i dettagli Computer come illustrato di seguito.



â€f

Risoluzione dei problemi

Cisco Secure Endpoint per Windows richiede una connessione continua al server di definizione TETRA per il download degli aggiornamenti.

Errori comuni nel download delle definizioni TETRA includono:

- Impossibile risolvere l'indirizzo del server

- Errore durante la convalida del certificato SSL (incluso il controllo dell'elenco di revoche di certificati)
- Interruzione durante il download
- Impossibile connettersi al server proxy
- Errore di autenticazione al server proxy

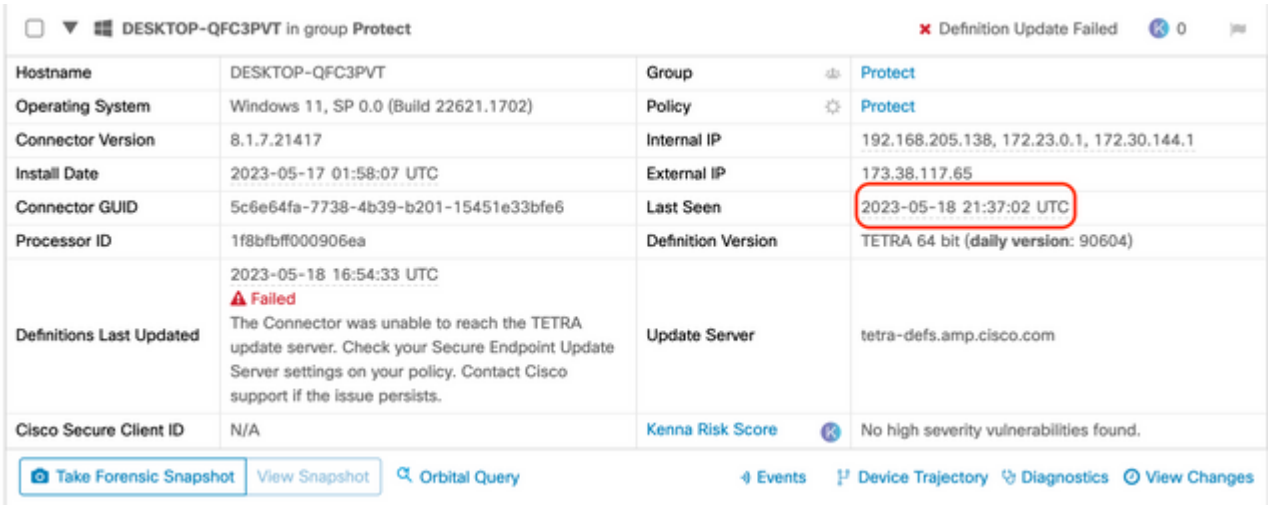
Se si verifica un errore durante il tentativo di scaricare le definizioni TETRA, il tentativo successivo verrà eseguito durante il successivo intervallo di aggiornamento o se l'utente avvia un aggiornamento manuale.

Verifica della connettività segnalata per l'endpoint in Secure Endpoint Console

Secure Endpoint Console visualizza se l'endpoint si connette regolarmente. Verificare che gli endpoint siano attivi e che abbiano uno stato "Ultima visualizzazione" recente. Se gli endpoint non vengono archiviati con Secure Endpoint Console, significa che l'endpoint non è attivo o presenta alcuni problemi di connettività.

Cisco rilascia in media 4 aggiornamenti delle definizioni al giorno e, se in qualsiasi momento del giorno l'endpoint non riesce a scaricare l'aggiornamento, il connettore invia un errore. Considerando questa frequenza, solo se gli endpoint sono costantemente connessi e hanno una connessione di rete stabile al server TETRA in tutto, allora, gli endpoint si presenteranno come "All'interno del criterio".

Lo stato "Ultima vista" si trova nella pagina dei dettagli del computer, come indicato di seguito:

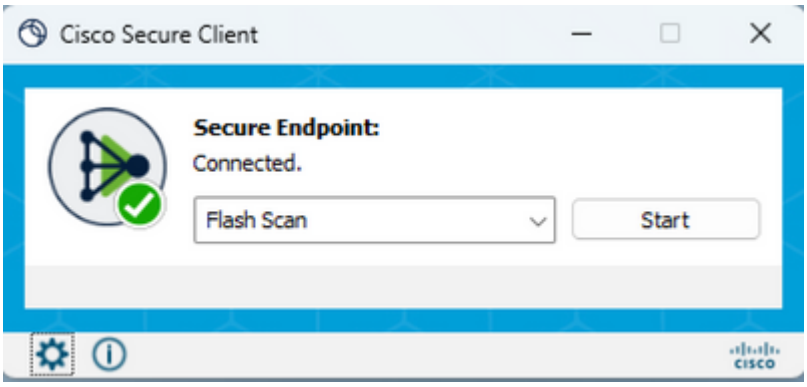


Se l'endpoint è connesso e viene segnalato un errore che indica che le definizioni non sono state scaricate ma sono visualizzate dalla console, il problema potrebbe essere intermittente. Ulteriori indagini possono essere condotte se le differenze temporali tra "Ultimo visto" e "Ultimo aggiornamento delle definizioni" sono notevoli.

Controllo della connettività sull'endpoint

Gli utenti finali possono verificare la connettività utilizzando l'interfaccia utente.

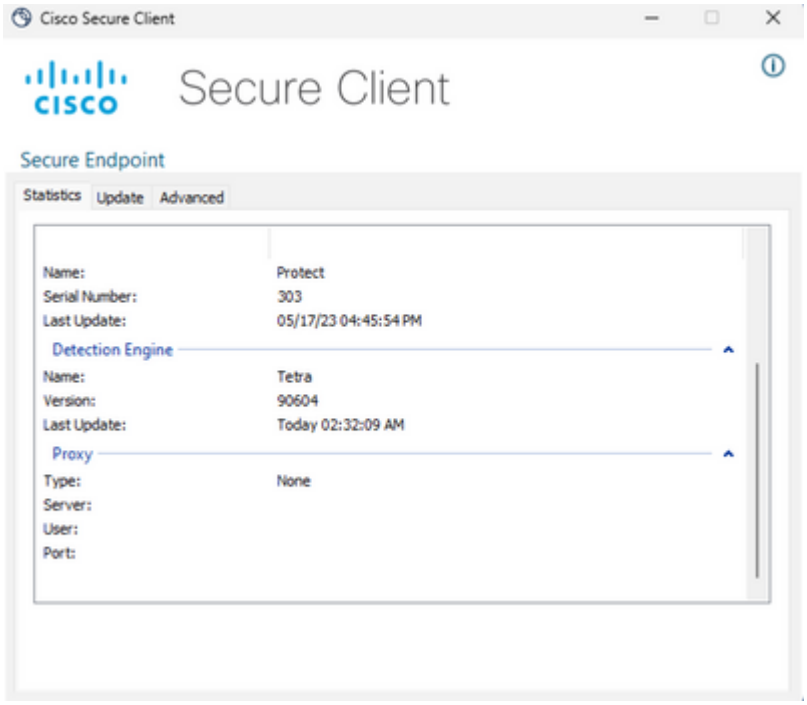
Se si apre Cisco Secure Client, viene visualizzato lo stato della connettività.



ConnectivityTool può essere utilizzato quando l'endpoint non è connesso e segnala problemi di connessione. È incluso in IPSupportTool che genera il pacchetto di supporto.

Controllo delle definizioni TETRA sull'endpoint

Cisco Secure Client fornisce informazioni sulle definizioni TETRA correnti caricate dal connettore dell'endpoint. L'utente finale può aprire il client e controllare le impostazioni per Secure Endpoint. Nella scheda Statistiche è disponibile la definizione corrente di TETRA.

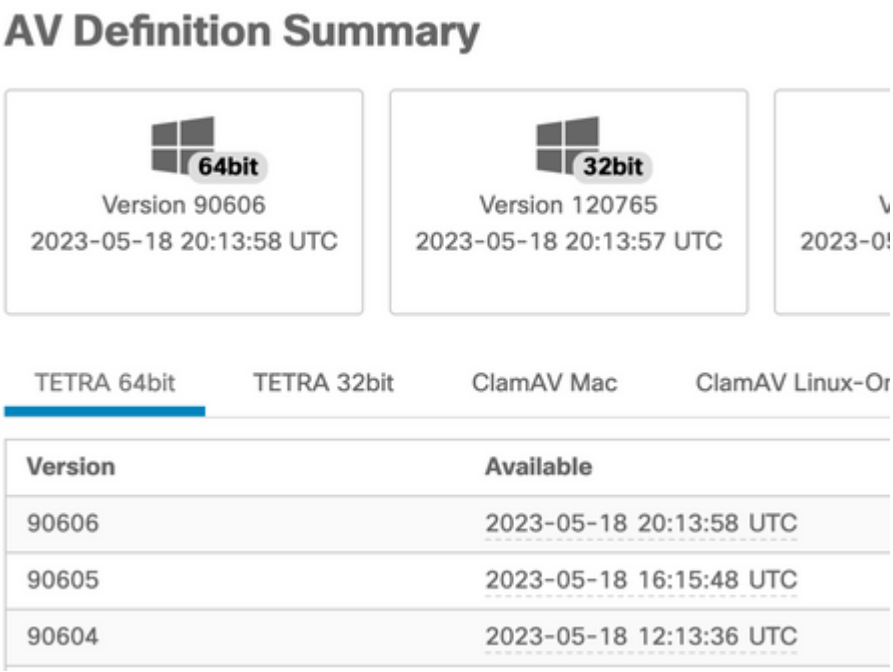


â€f

Inoltre, i dettagli correnti della definizione TETRA vengono riportati dallo strumento AmpCLI sull'endpoint. Di seguito è riportato un esempio del comando:

```
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
```

Le versioni delle definizioni vengono visualizzate per ciascun motore, incluso TETRA. Nell'output precedente, è la versione 90604. La differenza può essere confrontata con Secure Endpoint Console in: **Gestione > Riepilogo delle definizioni AV**. Di seguito è riportato un esempio della pagina.



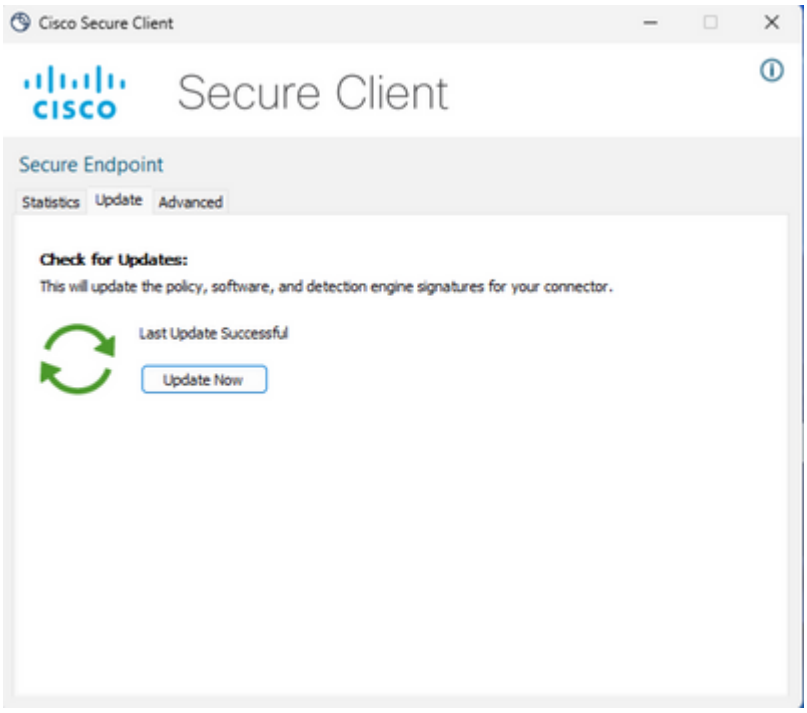
â€ƒ

Se la versione è ancora in ritardo e lo stato del connettore è connesso, è possibile eseguire un aggiornamento delle definizioni o il controllo della connettività dell'endpoint al server TETRA.

Forzatura dell'aggiornamento delle definizioni TETRA sull'endpoint

Gli utenti finali possono avviare e controllare lo stato di avanzamento del download di TETRA. Affinché l'utente attivi l'aggiornamento, è necessario impostare l'opzione nel criterio. Nella pagina **Impostazioni avanzate >** Impostazioni criterio **interfaccia utente client**, è necessario attivare le impostazioni **Consenti all'utente di aggiornare le definizioni TETRA** affinché l'utente possa attivarle.

In Cisco Secure Client, l'utente finale può aprire il client e verificare le impostazioni di Secure Endpoint. L'utente può fare clic su "Aggiorna ora" per attivare l'aggiornamento della definizione TETRA come mostrato di seguito:



Se si esegue AMP for Endpoints Connector versione 7.2.7 e successive, è possibile utilizzare un nuovo switch "-forceupdate" per forzare il connettore a scaricare le definizioni TETRA.

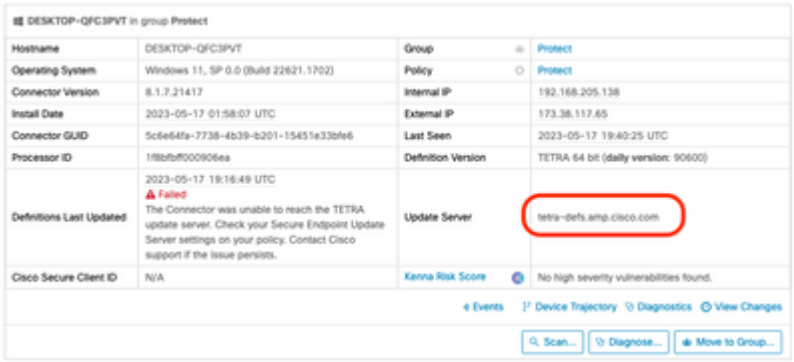
```
C:\Program Files\Cisco\AMP\8.1.7.21417\sfc.exe -forceupdate
```

Una volta forzato l'aggiornamento, è possibile controllare nuovamente la definizione TETRA per verificare se si verifica un aggiornamento. Se l'aggiornamento non è ancora in corso, è necessario controllare la connessione al server TETRA.

Verifica della connettività del server di definizione TETRA sull'endpoint

I criteri degli endpoint includono il server delle definizioni contattato dall'endpoint per il download delle definizioni.

Nella pagina dei dettagli del computer è incluso il server di aggiornamento. L'immagine seguente mostra la posizione del server di aggiornamento:



â€ƒ

Nel cloud pubblico, il nome del server richiesto a cui l'endpoint può connettersi è elencato in: Indirizzi del

server richiesti per le operazioni Cisco Secure Endpoint e Malware Analytics appropriate

Convalida connessione diretta

Dall'endpoint è possibile eseguire il comando seguente per verificare la ricerca DNS nel server di aggiornamento:

```
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
```

Se l'indirizzo IP è risolto, è possibile testare la connessione al server. Una risposta valida avrà il seguente aspetto:

<#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
```

Se non è possibile effettuare la connessione per convalidare il certificato con il server CRL (ad esempio commercial.ocsp.identrust.com o validation.identrust.com), verrà visualizzato il seguente messaggio di errore:

```
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
```

Convalida proxy

Se l'endpoint è configurato per l'utilizzo di un proxy, è possibile controllare lo stato dell'ultimo errore. L'esecuzione di PowerShell seguente può restituire l'ultimo errore restituito dal tentativo di aggiornamento TETRA.

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

Codice ultimo errore	**Problema**	**Azioni**
4294965193	Impossibile stabilire la connessione al proxy	Verificare la connettività di rete al proxy
4294965196	Impossibile eseguire l'autenticazione con il proxy	Controllare le credenziali di autenticazione per il proxy
4294965187	Connessione con il proxy e download non riusciti	Verifica la presenza di problemi di download nei log proxy

Ulteriori informazioni

- Se si notano endpoint che non riescono costantemente a scaricare le definizioni TETRA, nonostante siano stati completati i controlli precedenti, abilitare il connettore in modalità debug per un intervallo di tempo uguale all'intervallo di aggiornamento definito nella policy e generare il bundle di supporto. Quando il connettore è in modalità debug, prendere nota anche di acquisire il pacchetto Wireshark. È inoltre necessario eseguire l'acquisizione del pacchetto per un intervallo di tempo uguale all'intervallo di aggiornamento definito nel criterio. Una volta raccolte queste informazioni, aprire una richiesta TAC Cisco e altre informazioni per ulteriori informazioni.

Raccolta di dati diagnostici da AMP for Windows Connector

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).