

Erfassen der Protokolle für CUIC-Leistungsprobleme

Inhalt

[Einführung](#)

[Erfassen der Protokolle für CUIC-Leistungsprobleme](#)

[Allgemeine Richtlinien](#)

[Typische Gruppe von Protokollen](#)

[Definieren eines Problems](#)

[Beispiel 1. Fehler oder Timeout](#)

[Beispiel 2. Große Verzögerung](#)

[Vom Kunden bereitgestellte Ressourcen](#)

[Vorbereitung der Reproduktion](#)

[1. Name und Adresse der Client-Schnittstelle](#)

[2. HTTP-Paketerfassung für Clients](#)

[3. F12-Protokolle des Client-Browsers](#)

[4. Server-RTMT-Protokolle](#)

[5. HTTP-Paketerfassung für Server](#)

[6. Sitzungsaufzeichnung](#)

[Reproduzieren des Problems](#)

[Erfassen der Protokolle nach der Reproduktion](#)

[1. Erfassung von HTTP-Paketen des Clients](#)

[2. Sammeln von Client-Browser-F12-Protokollen](#)

[3. Server-RTMT-Protokolle sammeln](#)

[4. Aufzeichnung der Sitzung](#)

[Änderungen rückgängig machen](#)

Einführung

Dieses Dokument beschreibt einen Prozess zur Konfiguration und Erfassung von Cisco Unified Intelligence Center (CUIC)-Protokollen bei der Behebung von Leistungsproblemen. Die Behebung von CUIC-Leistungsproblemen könnte aufgrund der Vielzahl der beteiligten Technologien, Produkte und Komponenten eine Herausforderung darstellen. Auch Leistungsprobleme manifestieren sich auf verschiedene Weise, daher ist es wichtig, ein klares Bild während der Fehlerbehebung zu haben.

In diesem Dokument soll nicht der Fehlerbehebungsprozess detailliert beschrieben, sondern die wichtigsten Punkte beim Sammeln der vom Cisco TAC oder Cisco Engineering benötigten Protokolle hervorgehoben werden.

Erfassen der Protokolle für CUIC-Leistungsprobleme

Allgemeine Richtlinien

Das Sammeln aller Protokolle in einem einzigen Vorgang ist eine Herausforderung und zeitaufwendig. Die gesamte Prozedur sollte 1 bis 4 Stunden dauern. Es hängt davon ab, wie gut ein Kunde oder Partner die Umgebung vorbereitet.

Hinweis: Es sind keine Ausfallzeiten für diese Aktivität erforderlich, obwohl ein Kunde möglicherweise einige Änderungsanträge einreichen muss.

Es wird dringend empfohlen, die Tests speziell mit dem Firefox-Browser durchzuführen, da die Entwickler-Tools (F12) umfangreicher sind.

Sie müssen wissen, welche IP-Adressen der CUIC-Client und -Server für die Kommunikation verwendet.

Diese IP-Adressen werden für den CUIC-Client und den Server in diesem Artikel verwendet.

Client-IP-Adresse: 10.111.16.157

Server-IP-Adresse: 10.222.6.29

Tipp: Zur Fehlerbehebung der CUIC-Leistung wird dringend empfohlen, das Problem mithilfe eines Clients in der UCCE-LAN-Umgebung zu reproduzieren. Dadurch werden die Auswirkungen der Netzwerkverbindung zwischen CUIC-Client und Server eliminiert.

Da es mehrere Protokollauflistungsversuche geben kann, ist es wichtig, die eindeutige Benennung der gesammelten Dateien beizubehalten. Erstellen Sie auf dem Desktop Ihres Kunden einen Ordner mit dem Namen **tac<date>_<time>** (z. B. tac27feb17_1334) oder **tac_<date>_<Verbindungsversuch>** (z. B. tac27feb17_take3). Nachdem Sie die Protokolle gesammelt haben, legen Sie sie alle in diesen Ordner, archivieren Sie sie und fügen Sie sie an das Gehäuse an.

Versuchen Sie, einen Knoten im Cluster zu finden, der aus Sicht von CPU, Speicher und ioWait-Status die beste Leistung liefert und trotzdem Leistungsprobleme aufweist. Führen Sie Tests mit diesem Knoten durch, und vermeiden Sie ggf. den Load Balancer.

Typische Gruppe von Protokollen

1. Client-Browser F12-Protokolle
2. Client-HTTP-Paketerfassung
3. HTTP-Paketerfassung für Server
4. CUIC-Server Intelligence Center Reporting ServiceCisco Informix-DatenbankserviceCisco RIS Data Collector PerfMonLogCisco TomcatEreignisanzeige-AnwendungsprotokollEreignisanzeige - SystemprotokollPaketerfassungsprotokolle

Definieren eines Problems

Beispiel 1. Fehler oder Timeout

Während der Spitzenzeiten meldet der CUIC Benutzer auf allen Knoten im Cluster mehrere Fehler für Echtzeitberichte.

E1: "Retrieve dataset information java.lang.IllegalStateException"

E2: "Letzte Aktualisierung mit Zeitüberschreitung (getDataSetMaxReached), klicken Sie auf Aktualisierung, um neu zu laden."

E3: "Letzte Aktualisierung hat Zeitüberschreitung (reportRefreshRetry). Bitte warten Sie auf die nächste automatische Aktualisierung oder klicken Sie auf "Aktualisieren"."

Das Problem begann am 27. Februar morgens, nachdem diese spezifischen Änderungen in Netzwerk, Sicherheit und Rechenzentrum am Wochenende implementiert wurden. Wir haben diese Dimensionierungsrichtlinien für unser CUIC-Cluster überprüft.

[Cisco Unified Intelligence Center Solution Reference Network Design \(SRND\), Version 11.0\(1\)](#)

Beispiel 2. Große Verzögerung

Bei CUIC, der nur Benutzer auf dem ersten Subscriber-Knoten meldet, treten bei der Anzeige von Echtzeitberichten Verzögerungen von 30-40 Sekunden auf.

Das Problem begann am 26. Februar nach der Aktualisierung der Firmware unserer SAN-Netzwerkgeräte. Wir haben diese Dimensionierungsrichtlinien für unser CUIC-Cluster überprüft.

[Cisco Unified Intelligence Center Solution Reference Network Design \(SRND\), Version 11.0\(1\)](#)

Vom Kunden bereitgestellte Ressourcen

Im Folgenden finden Sie eine Zusammenfassung der Tools/Anwendungen, die Kunden oder Partner bei der Erfassung der Protokolle für CUIC-Leistungsprobleme verwenden müssen.

- Kunde: Windows-Eingabeaufforderung (CMD)
- Kunde: Wireshark
- Kunde: Firefox-Browser
- Kunde: Real-Time Monitoring Tool (RTMT) oder ein Secure File Transfer Protocol (SFTP)-Server
- CUIC Server-Befehlszeile (CLI)

Hinweis: In einigen Fällen kann es kompliziert sein, CUIC-Protokolle mit RTMT zu sammeln. Daher müssen Sie die Protokolle von der CUIC CLI auf einen SFTP-Server herunterladen.

Vorbereitung der Reproduktion

1. Name und Adresse der Client-Schnittstelle

Verwenden Sie CMD, um alle CUIC-Client-IP-Adressen zu sammeln.

Ermitteln Sie die Netzwerkschnittstelle und die IP-Adresse, die für die Kommunikation mit dem CUIC-Server verwendet werden. Sie müssen diese bei der Erfassung einer Paketerfassung von

der Serverseite aus verwenden.

```
C:\Users\Administrator>route print -4 | findstr 222
10.222.6.0    255.255.254.0    On-link    10.111.16.157    1
```

Bestimmen Sie mit diesem Befehl den richtigen Schnittstellennamen, der später in Wireshark ausgewählt werden muss. Der Schnittstellename und seine IP-Adresse sind kursiv.

```
c:\tmp>ipconfig
Windows IP Configuration

Wireless LAN adapter wifi0:
    IPv4 Address. . . . . : 10.111.16.157

Ethernet adapter Local Area Connection 2:
    IPv4 Address. . . . . : 192.168.123.1

<output omitted for brevity>
```

2. HTTP-Paketerfassung für Clients

Stellen Sie sicher, dass die Anwendung Wireshark installiert ist und einwandfrei funktioniert. Wählen Sie die im vorherigen Schritt festgelegte richtige Schnittstelle aus, aber beenden Sie jetzt die Paketerfassung.

Tip: Wenn in Wireshark keine Schnittstellen gefunden werden, ist eine gängige Lösung, die darin besteht, die Pcap-Software, die mit Wireshark gebündelt wird, neu zu installieren.

3. F12-Protokolle des Client-Browsers

3.1 Öffnen Sie den Firefox-Browser, und überprüfen Sie dessen Version. Es muss unterstützt werden.

Drücken Sie F12, und navigieren Sie zur Registerkarte **Network (Network Monitor, STRG+Umschalt+Q)**. Wählen Sie **All** (oder **HTML, JS, XHR, Media, Flash, WS, Other**) aus.



4. Server-RTMT-Protokolle

Melden Sie sich bei CUIC mit RTMT an, und wählen Sie diese Dienste für alle Knoten aus.

- Intelligence Center Reporting Service
- Cisco Informix-Datenbankservice
- Cisco RIS Data Collector PerfMonLog
- Cisco Tomcat
- Ereignisanzeige-Anwendungsprotokoll
- Ereignisanzeige - Systemprotokoll
- Paketerfassungsprotokolle

Wählen Sie **Absolute Range** oder **Relative Range** und geben Sie einen aussagekräftigen Namen für den Ordner mit diesen Protokollen an.

5. HTTP-Paketerfassung für Server

Um den Fehlerbehebungsprozess zu vereinfachen, muss es eine einfache Möglichkeit geben, einzelne Abfragen von Client zu Server nachzuverfolgen. Standardmäßig wird ein HTTPS-verschlüsselter Transport verwendet, der solche Details nicht preisgibt. Aus diesem Grund sollte HTTP für die Zeit der Problemreproduktion vorübergehend aktiviert werden.

Um die HTTP-Kommunikation zu aktivieren, geben Sie diesen Befehl in der CUIC CLI ein. Sie sollte auf dem Knoten aktiviert werden, der für den Test verwendet wird.

```
admin:set cuic properties http-enabled on
Value has been successfully set
```

```
admin:show cuic properties http-enabled
http_enabled
=====
on
```

Hinweis: Sie müssen den Cisco Tomcat-Dienst nicht neu starten. Die einzige Auswirkung ist eine unverschlüsselte Kommunikation zwischen CUIC-Client und -Server.

Starten Sie eine Paketerfassung mit Wireshark auf dem CUIC-Client.

Starten Sie eine Paketerfassung mit diesem Befehl auf dem CUIC-Serverknoten. Stellen Sie sicher, dass die richtige IP-Adresse des Clients angegeben ist.

```
admin:utils network capture file packetcapture count 100000 size all host ip 10.111.16.157
Executing command with options:
size=ALL count=100000 interface=eth0
src=dest= port=
ip=10.111.16.157
```

6. Sitzungsaufzeichnung

Es wird dringend empfohlen, zusammen mit den Protokollen eine Bildschirmaufzeichnung der Wiedergabe zu erstellen, um die CUIC-Benutzerfreundlichkeit insbesondere bei Zeitüberschreitungen und Verzögerungen bei der Berichtsanzeige zu zeigen.

Es kann eine beliebige Bildschirmaufzeichnungssoftware verwendet werden. Die Cisco WebEx-Aufzeichnungsfunktion stellt diese Funktion ebenfalls bereit.

Reproduzieren des Problems

Versuchen Sie, das Problem mit der geringsten Anzahl von durchgeführten Schritten zu reproduzieren. Versuchen Sie, während der Wiedergabe unnötige Aufgaben zu vermeiden. Dadurch wird die Protokollanalyse durch das Cisco TAC erheblich beschleunigt.

Ein Beispiel für einen sehr einfachen Test wäre die Anmeldung bei der **CUIC Main Administration-Seite** -> **Security** -> **User List** (oder **User Groups** oder **User Permissions**).

Wenn der obige Test die Verzögerung nach mehreren Versuchen nicht anzeigt, kann ein Kunde versuchen, das Problem durch Ausführen eines Berichts oder Dashboards zu reproduzieren. In diesem Fall ist es sehr wichtig, den Bericht oder den Dashboard-Namen aufzuschreiben.

Während des Reproduktionstests klicken Sie auf Windows Clock und öffnen Sie **Datum und Uhrzeit ändern** ... rechts unten. Die Zeit muss genau auf die Sekunden überwacht werden.

Protokollieren Sie alle durchgeführten Aktionen. Es ist hilfreich, zwischen den Aktionen zeitliche Lücken zu schließen. Sie können dieses Beispiel verwenden.

14:16:30 - Eingabe der CUIC-Adresse im Firefox-Browser

14:17:42 - **Eingabe** nach Eingabe der Anmeldeinformationen gedrückt

14:20:20 - Das System lud die Webseite Main.html ein.

14:21:02 - Auf **Benutzerliste** geklickt und CUIC hat mit dem Laden begonnen

14:28:15 - **Benutzerliste** wurde erfolgreich geladen (Verzögerung: 7,10 m)

Lassen Sie ein Notizblock geöffnet, und kopieren Sie die Vorlage oben. Ersetzen Sie dann im Idealfall einfach die Zeit- oder Schrittbeschreibung.

Erfassen der Protokolle nach der Reproduktion

1. Sammeln von HTTP-Paketerfassung für Clients

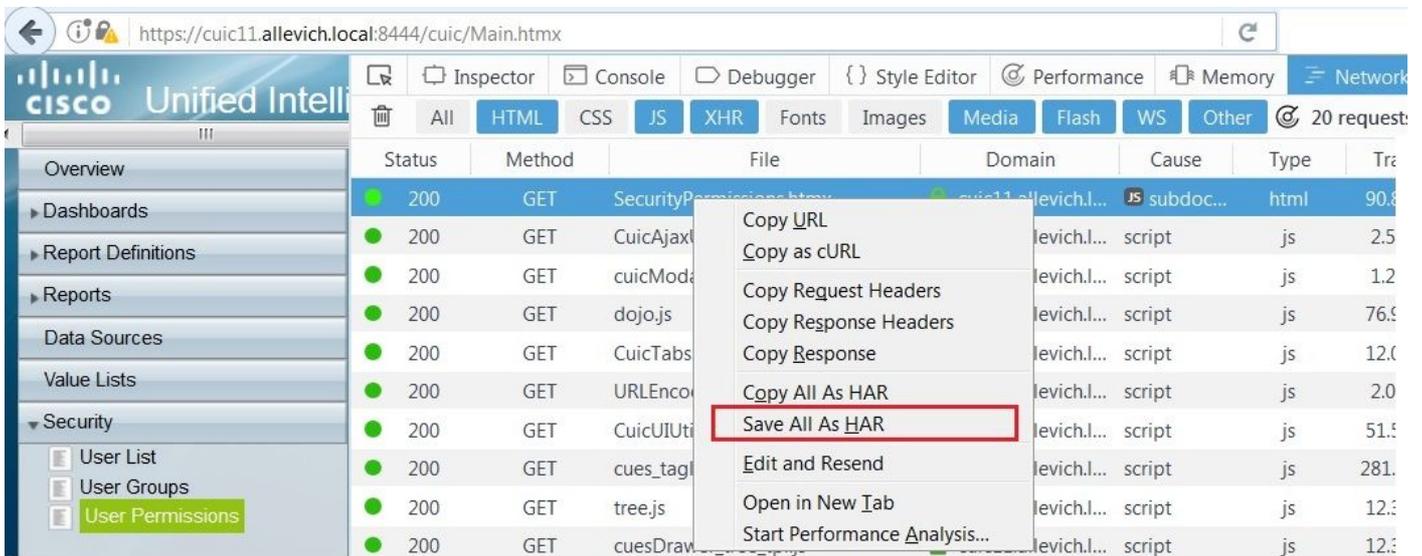
Beenden Sie die Paketerfassung auf dem Client (Wireshark).

Stoppen Sie die Paketerfassung auf dem CUIC-Knoten, indem Sie **STRG+C drücken**.

Speichern Sie in Wireshark die Client-Paketerfassung, und verschieben Sie sie in den TAC-Ordner.

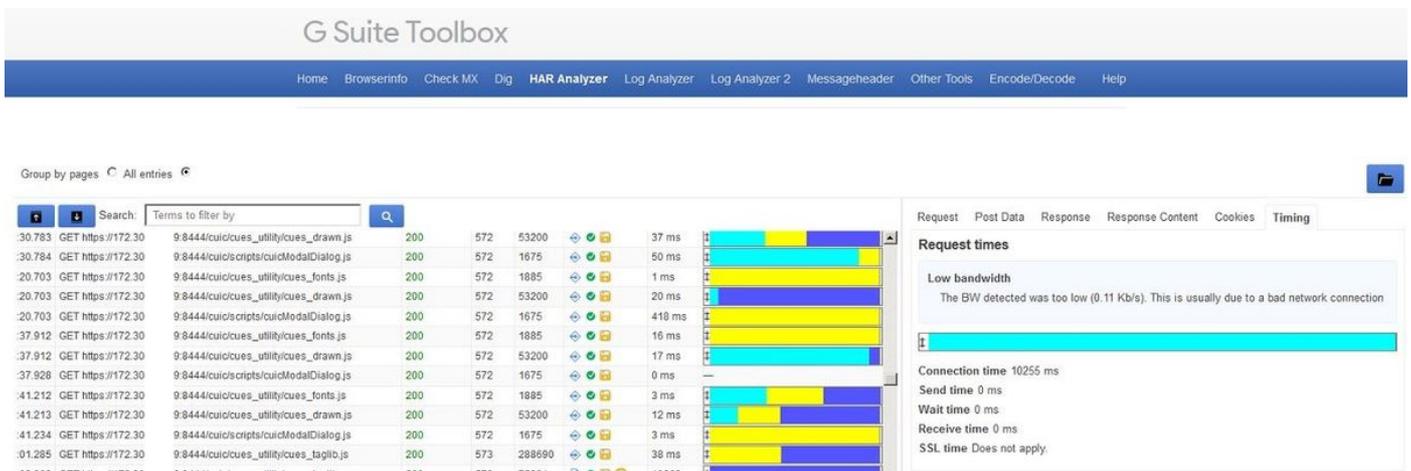
2. F12-Protokolle des Client-Browsers sammeln

Klicken Sie mit der rechten Maustaste auf eine Anfrage, und drücken Sie **Alle speichern als HAR**. Wählen Sie anschließend den TAC-Ordnerspeicherort aus, und klicken Sie auf **Speichern**.



Dieser Dateityp kann mit dem [G Suite HAR Analyser](#) Tool analysiert werden.

Dieses Beispiel zeigt, dass die Ursache für Berichtsverzögerungen eine geringe Netzwerkbandbreite zwischen CUIC-Client und -Server ist.



3. Server-RTMT-Protokolle sammeln

Stellen Sie sicher, dass die Paketerfassung des CUIC-Servers bereits angehalten ist. Falls nicht, drücken Sie in der CLI-Sitzung STRG+C.

Navigieren Sie zu CUIC RTMT, das vor der Einrichtung eingerichtet wurde, und drücken Sie **Fertig stellen**.

Hinweis: Bei Verwendung von RTMT müssen Sie sicherstellen, dass alle nicht vertrauenswürdigen Zertifikataufforderungen akzeptiert werden.

Wenn der Prozess der RTMT-Protokollerfassung langsam ist, können Protokolldateien auf einen SFTP-Server heruntergeladen werden.

Verwenden Sie diese Befehle, um die erforderlichen Protokolle für einen SFTP-Server zu sammeln.

```
file get activelog /cuic/logs/cuic/* retime hours 1
file get activelog /cuic/logs/cuicsrvr/* retime hours 1
file get activelog /cm/log/informix/* retime hours 1
file get activelog /cm/log/ris/csv/PerfMon* retime hours 1
file get activelog /syslog/CiscoSyslog* retime days 1
file get activelog /syslog/AlternateSyslog* retime days 1
file get activelog /syslog/messages* retime days 1
file get activelog /cuic/logs/cuic/* retime hours 1
file get activelog /cuic/logs/cuic/* retime hours 1
file get activelog /tomcat/logs/localhost_access*.txt retime hours 1
file get activelog /platform/cli/*.cap retime hours 1
```

Zusammen mit den Protokollen werden diese CUIC CLI-Ausgaben vom Testknoten bereitgestellt.

```
show status
show tech network hosts
utils ntp status
utils service list
utils dbreplication runtimestate
file list activelog /core/
file dump install system-history.log
show process using-most cpu
show process using-most memory
run sql SELECT COUNT(*) FROM cuic_data:cuicuser
show perf query counter ReportingEngineInfo ReportsUsersLoggedIn
```

4. Aufzeichnung der Sitzung

Beenden und fügen Sie die Bildschirmaufzeichnung zum TAC-Ordner hinzu.

Änderungen rückgängig machen

Deaktivieren Sie die HTTP-Kommunikation auf dem CUIC-Knoten.

```
admin:set cuic properties http-enabled off
Value has been successfully set

admin:show cuic properties http-enabled
http_enabled
=====
off
```