Finesse BOSH-implementatie begrijpen en problemen oplossen

Inhoud

Inleiding

Dit document beschrijft de architectuur achter Finesse-verbindingen die BOSH gebruiken en hoe BOSH-verbindingsproblemen kunnen worden gediagnosticeerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Finesse

- Unified Contact Center Enterprise (UCCE)
- Unified Contact Center Express (UCCX)
- Ontwikkelaarstools voor webbrowsers
- Windows- en/of Mac-beheer

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Finesse 9.0(1) â€“ 11.6(1)
- UCCX 10.0(1) â€“ 11.6(2)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

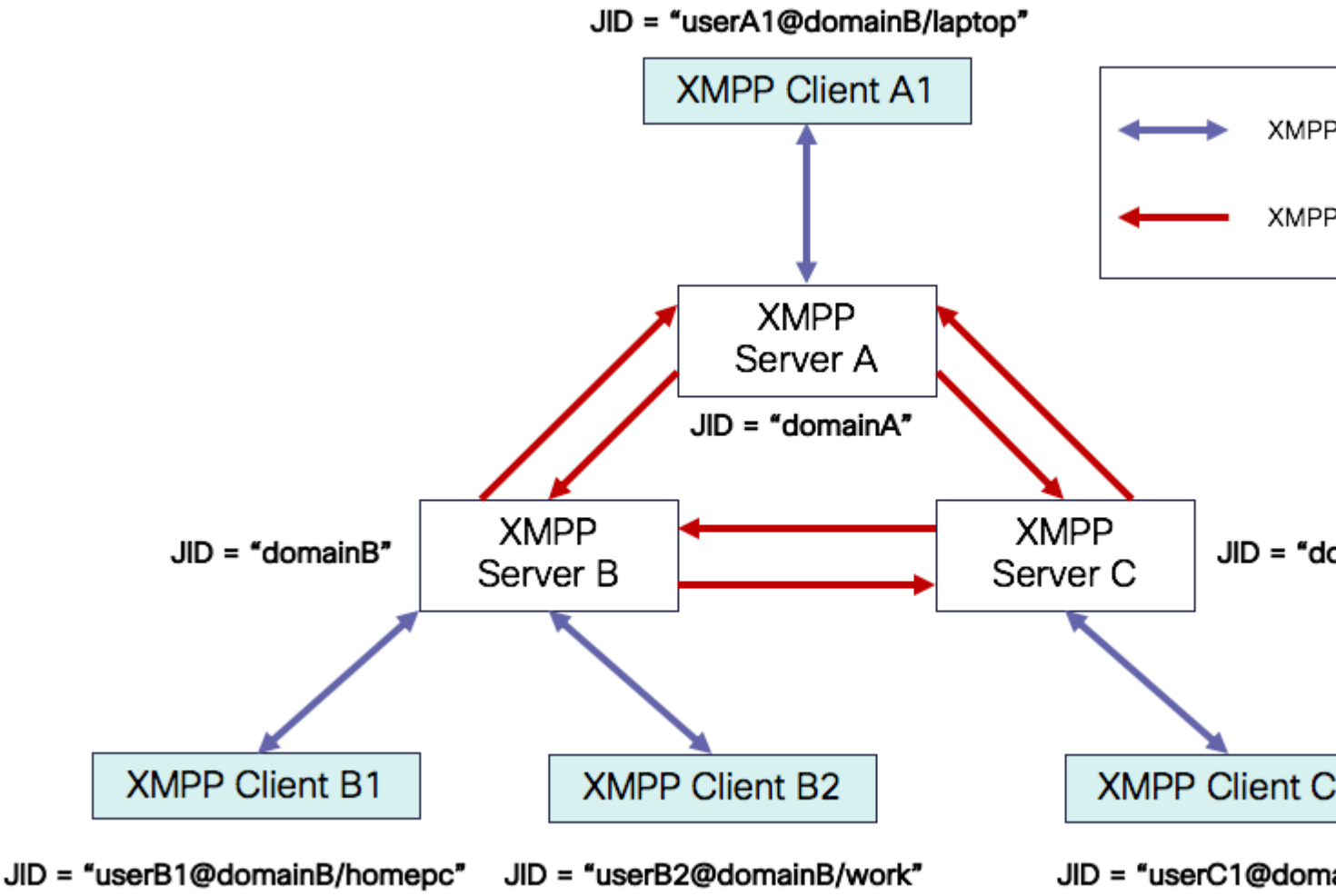
De verbindingen die Bidirectionele-stromen over synchrone HTTP gebruiken worden genoemd BOSH.

Finesse BOSH-implementatie begrijpen

XMPP begrijpen

Extensible Messaging and Presence Protocol (XMPP) (ook bekend als Jabber) is een stateful protocol in een clientservermodel. Met XMPP kunnen kleine stukjes gestructureerde XML-data (eXtensible Markup Language) worden verzonden tussen entiteiten. XMPP/Jabber wordt uitvoerig gebruikt voor instant messaging (IM) en aanwezigheidstoepassingen.

Alle XMPP-entiteiten worden geïdentificeerd op basis van hun Jabber-ID (JID).



JID-adresseringsschema: user@domain/resource

gebruiker	gebruikersnaam van client op de XMPP-server of de naam van de vergaderruimte
domein	Volledig gekwalificeerde domeinnaam van XMPP-server (FQDN)
bron	identificatie van de specifieke entiteit/het specifieke eindpunt van de gebruiker (bijvoorbeeld laptop, smartphone, enz.), een sessie-identificatiecode of naam van het openbare knooppunt

---

> **Opmerking**: Alle drie JID-componenten worden niet in alle gevallen gebruikt. Een server zou typisch enkel door het domein, een conferentieruimte bepaald door user@domain, en een cliënt door user@domain/resource worden bepaald.

XMPP-berichten worden ook wel stanzaâ€™s genoemd. Er zijn drie belangrijke stanzaâ€™s in XMPP:

1. <bericht>: één richting, één ontvanger

2. <Presence>: één richting, publiceren naar velen

3. <iq>: info/query - verzoek/antwoord

Alle stanzaâ€™s moeten adressen van afkomst en bestemming bevatten. De meeste stanzaâ€™s bevatten ook kenmerken voor type, id en xml:lang.

Kenmerk van stanza	**Doel**
in	JID van bestemming
van	JID van bron
type	doel van bericht
id	unieke identificatie om een verzoek te koppelen aan een respons voor <iq> stanzaâ€™s
xml:lang	definieert de standaardtaal van de voor mensen leesbare XML in de stanza

Voorbeeld van XMPP-bericht

```
<message to='person1@example' from='person2@example' type='chat'>
  <subject> Team meeting </subject>
  <body>Hey, when is our meeting today? </body>
  <thread>A4567423</thread>
</message>
```

XMPP-implementatie met Finesse

Als een webtoepassing met XMPP moet werken, brengt dit meerdere problemen met zich mee. Browsers bieden geen native ondersteuning voor XMPP via Transmission Control Protocol (TCP). Daarom moet al het XMPP-verkeer worden verwerkt door een programma binnen de browser. Webservers en browsers communiceren via Hypertext Transfer Protocol (HTTP) en dus plaatsen Finesse en andere webapps XMPP-berichten binnen HTTP-berichten.

Het eerste probleem met deze benadering is dat HTTP een stateless protocol is. Dit betekent dat elk HTTP-verzoek niet gerelateerd is aan een ander verzoek. Dit probleem kan echter worden aangepakt met toepassingsgerichte middelen, bijvoorbeeld met het gebruik van cookies en/of post-data.

De tweede uitdaging is het feit dat HTTP in één richting werkt. Alleen de client kan verzoeken verzenden, en de server kan alleen reageren. Het feit dat de server data niet kan pushen betekent dat het onnatuurlijk is om XMPP via HTTP te implementeren.

Dit probleem bestaat niet in de oorspronkelijke XMPP Core-specificatie (RFC 6120), waar XMPP aan TCP is gebonden. Als u het probleem wilt oplossen met XMPP gebonden aan HTTP, bijvoorbeeld omdat

JavaScript HTTP-aanvragen kan verzenden, zijn er twee mogelijke oplossingen. Voor beiden is een brug tussen HTTP en XMPP nodig.

De voorgestelde oplossingen zijn:

1. Polling (legacy protocol): herhaalde HTTP-verzoeken om nieuwe gegevens zoals gedefinieerd in XEP-0025: Jabber HTTP Polling

2. Lange opiniepeiling is ook bekend als BOSH: transportprotocol dat de semantiek van een langdurige, tweerichtingsTCP-verbinding tussen twee entiteiten emuleert door efficiënt gebruik te maken van meerdere synchrone HTTP-verzoek/respons paren zonder het gebruik van frequente opiniepeilingen gedefinieerd in XEP-0124: HTTP Binding en uitgebreid door XEP-0206: XMPP over BOSH

Finesse implementeert BOSH omdat het efficiënt is qua taakverdeling voor servers en qua verkeer. De reden om BOSH te gebruiken is om het feit te verdoezelen dat de server niet hoeft te reageren zodra er een verzoek is. De respons wordt vertraagd tot een specifiek moment wanneer de server data heeft voor de client, die dan als respons wordt verzonden. Zodra de client de respons krijgt maakt de client een nieuw verzoek, enzovoorts.

De desktopclient van Finesse (webtoepassing) zet elke 30 seconden een inactieve BOSH-verbinding op via TCP-poort 7443. Als er na 30 seconden geen updates zijn van de Notification Service van Finesse, zal deze een HTTP-respons met 200 OK en een (vrijwel) lege responstekst verzenden. Als de Notification Service een update heeft over bijvoorbeeld de aanwezigheid van een medewerker of dialooggebeurtenis (gesprek), worden de gegevens onmiddellijk naar de Finesse-webclient verzonden.

Voorbeeld van Finesse XMPP-verzoek/respons

Dit voorbeeld toont het eerste XMPP-bericht met verzoek en respons tussen de Finesse-client en Finesse-server voor het opzetten van de BOSH-verbinding.

```
Finesse client request:
<body xmlns="http://jabber.org/protocol/httpbind" xml:lang="en-US" xmlns:xmpp="urn:xmpp:xbosh" hold="1"

Finesse server response:
<body xmlns="http://jabber.org/protocol/httpbind" xmlns:stream="http://etherx.jabber.org/streams" authic
```

Kort samengevat:

1. De Finesse-webclient heeft een inactieve HTTP-verbinding (http-bind) met de Finesse-server via TCP-poort 7443. Dit wordt ook wel een BOSH long poll genoemd.

2. De Finesse Notification Service is een aanwezigheidsdienst die updates post met betrekking tot de staat van een agent, vraag, etc.

3. Als de Notification Service een update heeft, reageert deze op het http-bind-verzoek met de toestandsupdate als een XMPP-bericht in de tekst van de HTTP-respons.

4. Als er 30 seconden na ontvangst van het http-bind-verzoek geen statusupdates zijn, antwoordt de Notification Service zonder toestandsupdates zodat de Finesse-webclient nog een http-bind-verzoek kan verzenden. Dit is een manier voor de Notification-service om te weten dat de Finesse-webclient nog steeds in staat is om verbinding te maken met de Notification Service en dat de agent hun browser niet heeft gesloten of hun computer niet in de slaapstand heeft gezet, enzovoort.

Finesse XMPP-berichten en XMPP-knooppunten begrijpen

Finesse implementeert ook XMPP specificatie XEP-0060: Publish-Subscribe. Met deze specificatie kan de XMPP-server (Notification Service) informatie verzenden naar XMPP-knooppunten (onderwerpen) en vervolgens XMPP-gebeurtenissen versturen naar entiteiten die zijn geabonneerd op het knooppunt. In het geval van Finesse verstuurt de CTI-server (Computer Telephony Integration) CTI-berichten naar de Finesse-webservice om Finesse te informeren over configuratie-updates zoals, maar niet beperkt tot, het aanmaken van een medewerker of contactservicewachtrij (CSQ) of informatie over een gesprek. Deze informatie wordt vervolgens omgezet in een XMPP-bericht dat de Finesse-webservice naar de Notification Service van Finesse verzendt. De Notification Service van Finesse verzendt vervolgens XMPP Over BOSH-berichten naar medewerkers die zijn geabonneerd op bepaalde XMPP-knooppunten.

Enkele API-objecten van Finesse die in de Cisco Finesse Web Services Developer Guide (Ontwikkelaarsgids voor webservices van Cisco Finesse) zijn gedefinieerd, zijn XMPP-knooppunten. Agent en supervisor Finesse webclients kunnen zich abonneren op gebeurtenisupdates voor een aantal van deze XMPP-knooppunten om actuele informatie te hebben over real-time gebeurtenissen (zoals call-gebeurtenissen, state-gebeurtenissen, enzovoort). Deze tabel toont de XMPP-knooppunten die geschikt zijn voor publish-subscribe.

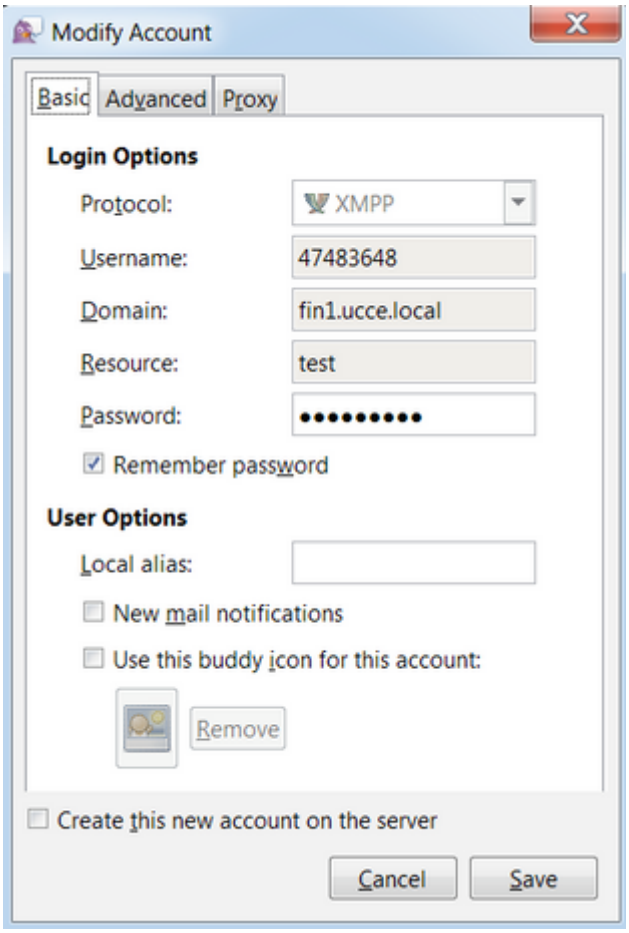
Finesse API-object	**Doel**	**Abonnement**
/finesse/api/User/<LoginID>	Toont de toewijzing van toestand en team van de medewerker	Medewerkers en supervisors
/finesse/api/User/<LoginID>/Dialogs	Toont de vraag (en) die door de agent wordt (worden) behandeld	Medewerkers en supervisors
/finesse/api/User/<LoginID>/ClientLog	Wordt gebruikt om clientlogboeken van de knop **Send Error Report** (Foutrapport verzenden) te verzamelen	Medewerkers en supervisors
/finesse/api/User/<LoginID>/Queue/<queueID>	Toont statistische gegevens voor wachtrijen (indien ingeschakeld)	Medewerkers en supervisors
/finesse/api/Team/<TeamID>/Users	Toont de medewerkers die tot een bepaald team behoren, inclusief statusinformatie	Supervisors
/finesse/api/SystemInfo	Toont de status van de Finesse-server. Hiermee wordt bepaald of failover nodig is	Medewerkers en supervisors

Voorbeeld 1: Gebruik Pidgin om Finesse XMPP-knooppunten te bekijken

Stap 1. Download en installeer de XMPP client Pidgin.

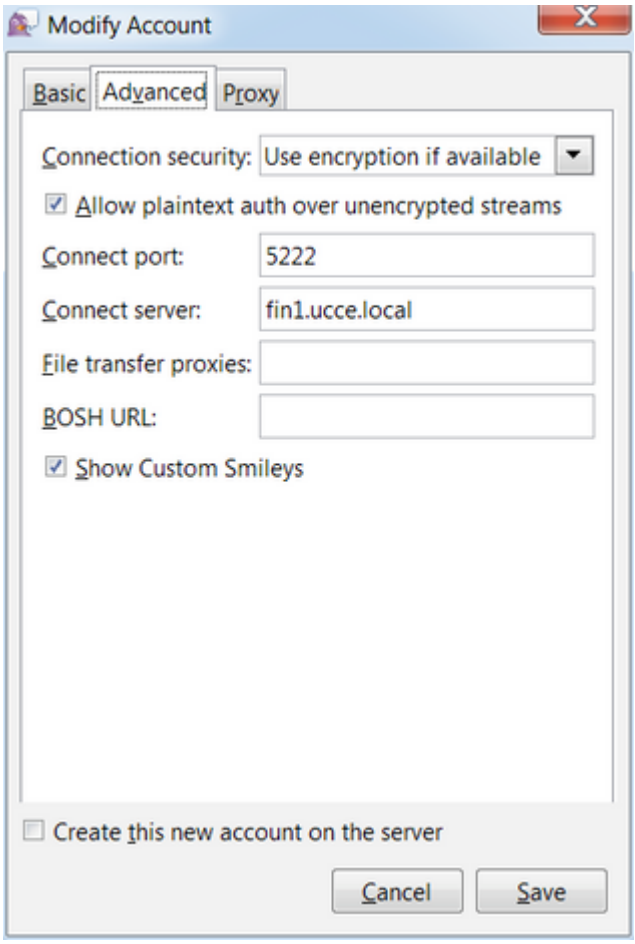
Stap 2. Navigeer naar **accounts** > **Wijzigen** > **Basis** en configureer de **inlogopties**:

- Protocol: XMPP
- Gebruikersnaam: LoginID voor elke agent
- Domain: FQDN van Finesse-server
- Resource: Plaatsaanduiding - elke waarde kan worden gebruikt, bijvoorbeeld test
- Wachtwoord: Agent-wachtwoord
- Schakel het selectievakje **Remember password** (Wachtwoord onthouden) in



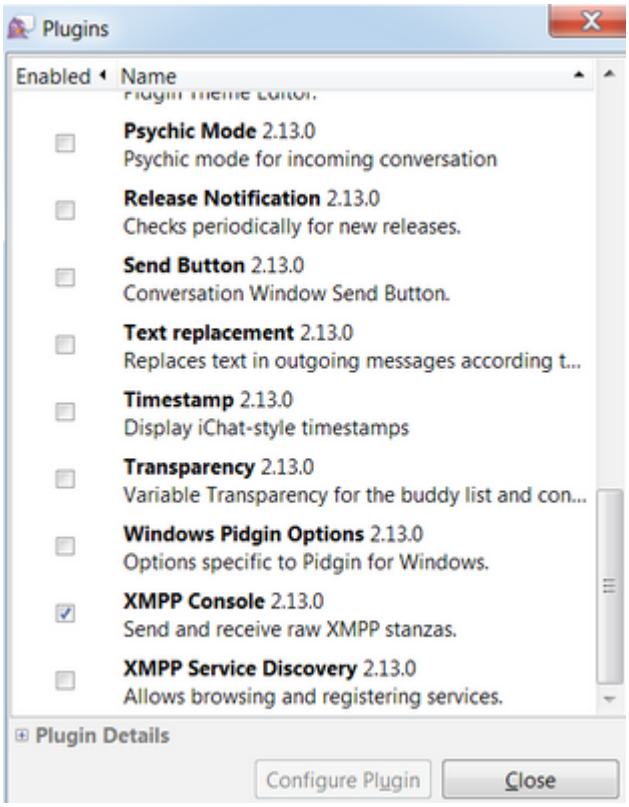
Stap 3. Navigeer naar **accounts** > **Wijzigen** > **Geavanceerd** en configureer:

- Connection security (Security van verbinding): Gebruik encryptie indien beschikbaar
- Controleer de **optie Plaintext auth toestaan bij andere niet-versleutelde stromen**.
- Verbindingshaven: 522. Gebruik de standaardpoort 5222. Deze poort is vereist voor externe XMPP-clients. Desktopclients van Finesse gebruiken 7443. Gebruik poort 7443 niet.
- Verbindingsserver: Finesse server FQDN

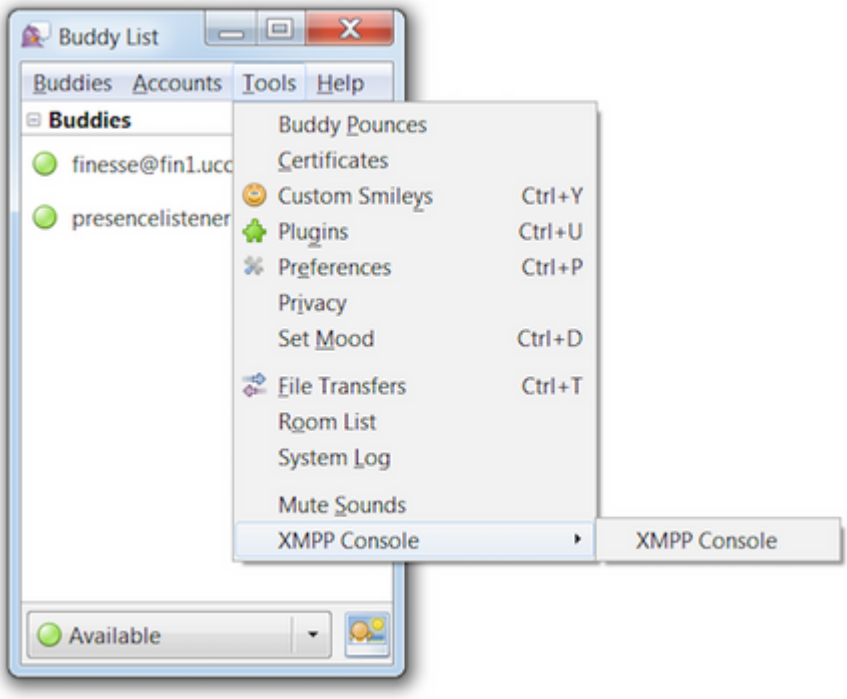


Opmerking: poort 5222 wordt alleen gebruikt omdat Finesse-webclients poort 7443 kunnen gebruiken om verbinding te maken met de meldingsdienst.

Stap 4. Navigeer naar **Gereedschappen > Plugins** en schakel de XMPP-console in.

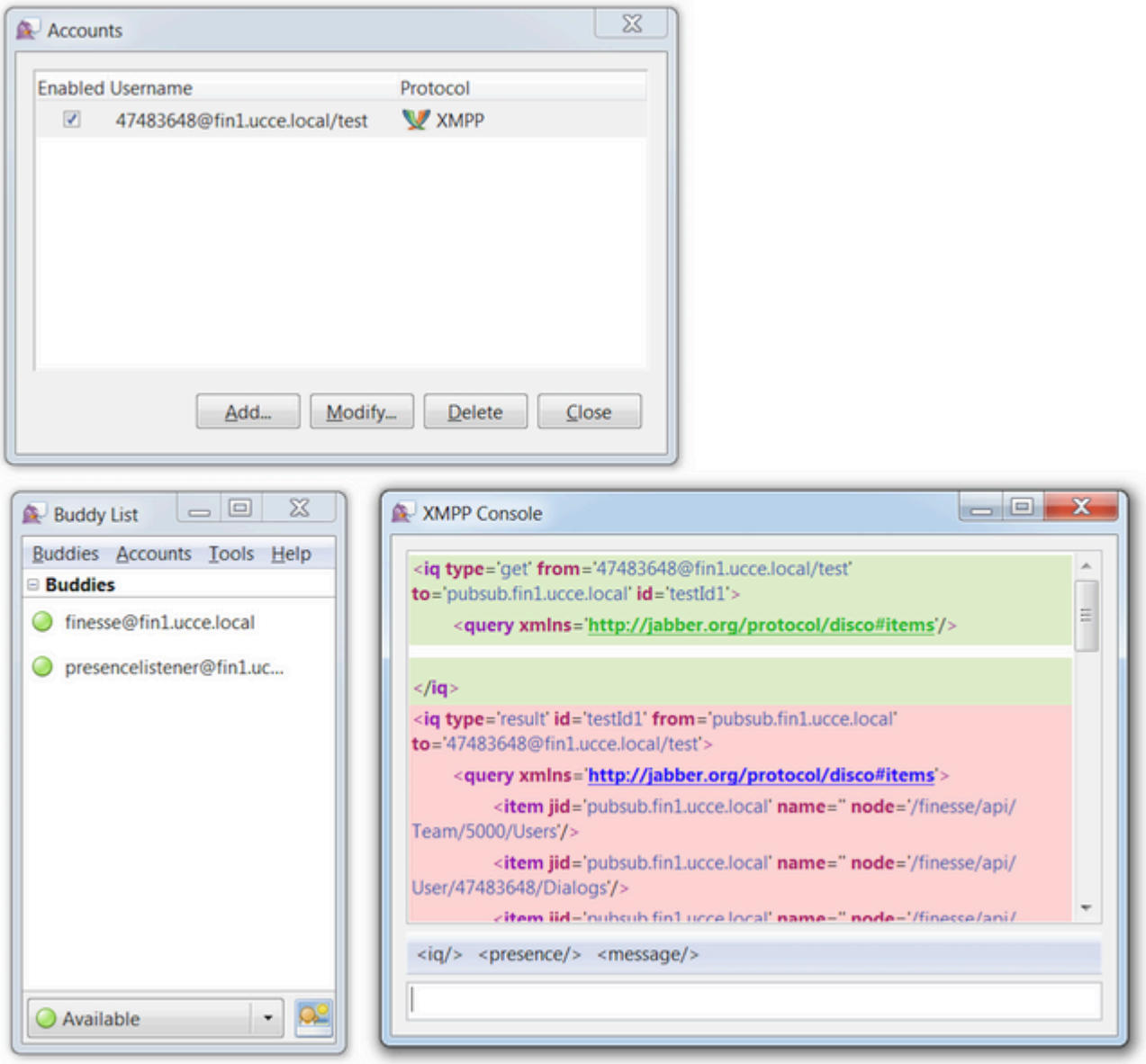


Stap 5. Ga naar **Gereedschappen > XMPP-console > XMPP-console** om de XMPP-console te openen.



Stap 6. Voer dit **<iq>**-bericht uit om alle XMPP-knooppunten te zien die bestaan.

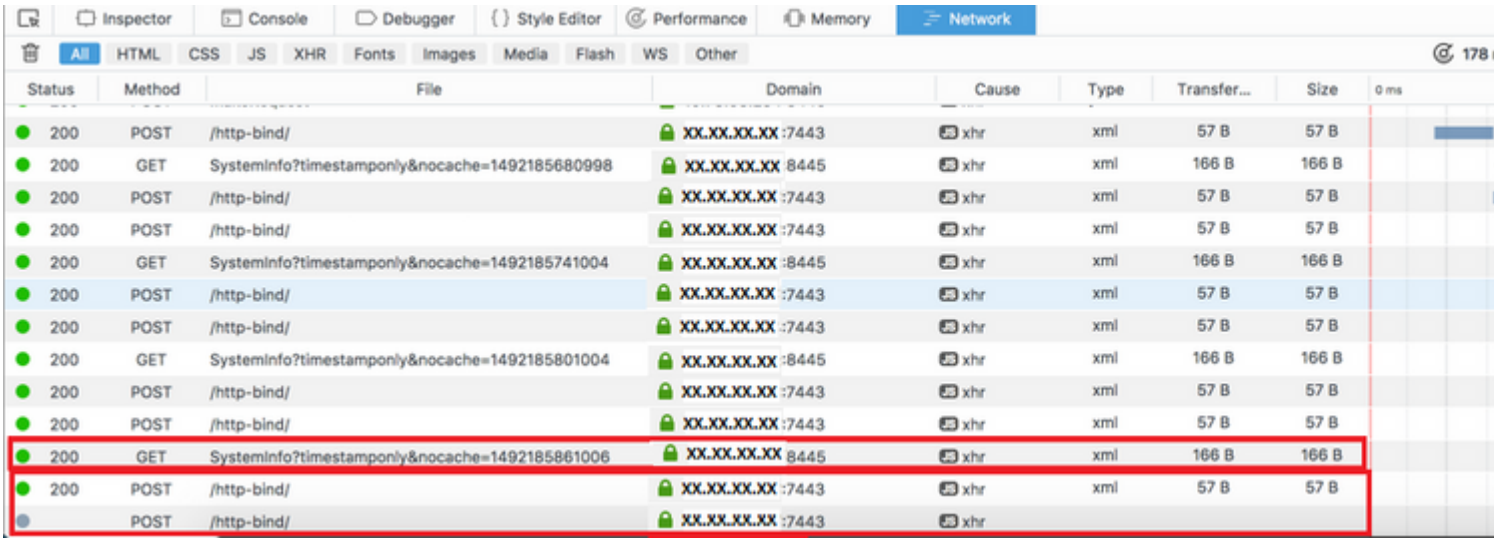
Voorbeeld:



In een laboratoriumomgeving waarin twee medewerkers en twee CSQâ€™s zijn geconfigureerd, bevat de Finesse-respons deze uitvoer:

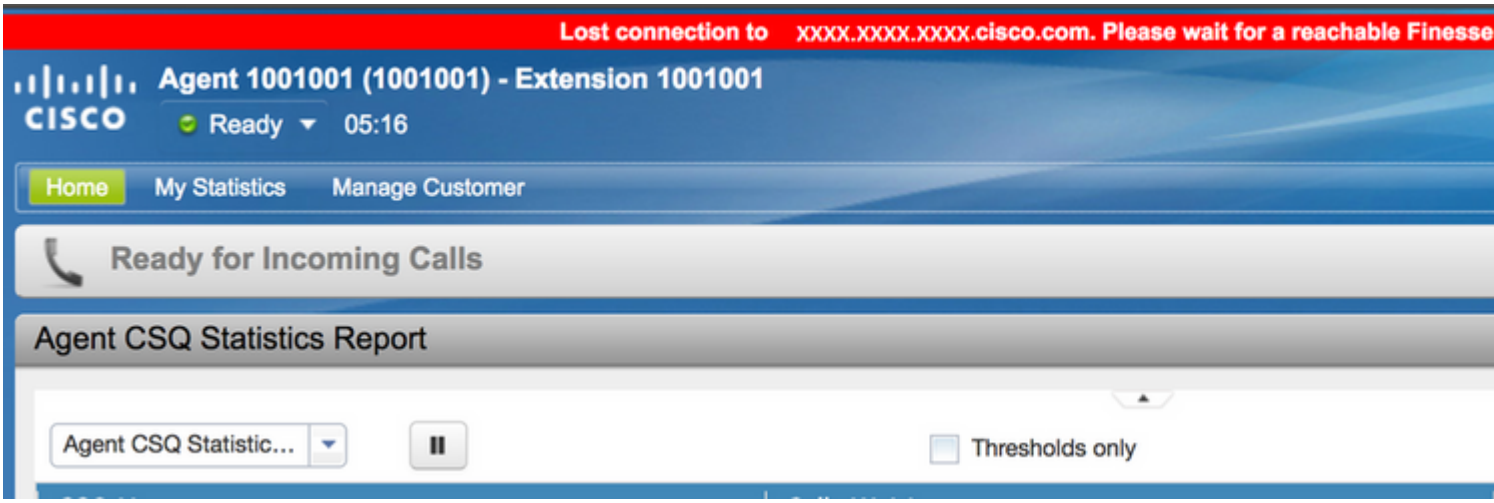
Voorbeeld 2: Gebruik Browser Developer Tools Network Tab om HTTP-berichten te bekijken

Elke browser heeft ontwikkelaarstools. Het tabblad Network (Netwerk) van de ontwikkelaarstools toont de HTTP-berichten die zijn ontvangen en verzonden door de Finesse-webclient (browser). Deze afbeelding laat bijvoorbeeld zien hoe de Finesse-webclient een SystemInfo-verzoek verzendt dat de status van Finesse Tomcat elke minuut controleert ter controle op failover. Daarnaast worden ook http-bind-berichten van de BOSH-verbinding getoond. Als er geen updates zijn op de XMPP-knooppunten waarop de webclient is geabonneerd, zal de Finesse-server binnen 30 seconden een respons verzenden.



Foutmelding voor BOSH-verbinding oplossen

Wanneer een BOSH losmaakt, de fout Verloren verbinding aan {Finesse Server FQDN}. Wacht tot een bereikbare Finesse Server gevonden is... wordt weergegeven in een rode banner bovenaan het bureaublad van Finesse.



Dit bericht wordt getoond omdat er op dit moment geen XMPP-abonnementsgebeurtenissen kunnen worden ontvangen van de Cisco Finesse Notification Service. Daarom kunnen er geen toestandsinformatie en gespreksdetails worden getoond op de medewerkersdesktop.

Voor UCCX wordt de status van de medewerker 60 seconden nadat de verbinding met de browser wordt verbroken, veranderd in Logout. Dit gebeurt ongeacht of de status van de medewerker Ready of Not Ready is.

Voor UCCE kan het Finesse tot 120 seconden kosten om te detecteren dat een medewerker de browser heeft gesloten of dat de browser is gecrasht. Finesse wacht 60 seconden voordat het een aanvraag voor gedwongen afmelden verzendt naar de CTI-server, waarna de CTI-server de status van de medewerker op Not Ready wordt gezet. Onder deze omstandigheden kan Finesse tot 180 seconden nodig hebben om de medewerker af te melden. In tegenstelling tot in UCCX wordt de status van de medewerker op Not Ready gezet in plaats van Logout.

Opmerking: de CTI heeft de verbinding niet klaar vs. Het gedrag van de logout staat in UCCE wordt

---

gecontroleerd door de parameter PG/LOAD. Zoals aangegeven in de Release-opmerkingen voor Unified Contact Center Enterprise & Hosted Release 10.0(1) is de parameter /LOAD afgeschaft vanaf UCCE 10.0.

Raadpleeg de sectie Desktop Behavior (Desktopgedrag) in het hoofdstuk Cisco Finesse Failover Mechanisms (Failover-mechanismen van Cisco Finesse) in de Cisco Finesse Administration Guide (Beheerhandleiding voor Cisco Finesse) voor meer informatie over het gedrag van UCCE Finesse voor desktop.

Opmerking: de timer-waarden kunnen in de toekomst veranderen al naar gelang de productbehoefte.

Analyse van logboeken

De logboeken van de Notification Services van Finesse en UCCX kunnen verzameld worden via RTMT of de CLI:

file get activelog /desktop recurs compress

Foutopsporingslogboeken van Notification Service

Opmerking: stel debug level logs in terwijl u een probleem reproduceert. Schakel de debug-informatie uit nadat u het probleem heeft gereproduceerd.

Opmerking: Finesse 9.0(1) heeft geen debug level logging. Logboekregistratie voor debugs is geïntroduceerd in Finesse 9.1(1). Het proces om de logboekregistratie in te schakelen is anders in 9.1(1) dan in Finesse 10.0(1) â€“ 11.6(1). Raadpleeg voor dit proces de handleiding Finesse Administration and Serviceability (Beheer en service van Finesse).

Schakel de foutopsporingslogboeken van de Notification Service van Unified Contact Center Express (UCCX) in, zoals getoond:

<#root>

admin:

utils uccx notification-service log enable

WARNING! Enabling Cisco Unified CCX Notification Service logging can affect system performance and should be disabled when logging is not required.

Do you want to proceed (yes/no)? yes

Cisco Unified CCX Notification Service logging enabled successfully.

NOTE: Logging can be disabled automatically if Cisco Unified CCX Notification Service is restarted.

Schakel de foutopsporingslogboeken van de Notification Service van Unified Contact Center Enterprise (UCCE) (Finesse Standalone) in, zoals getoond:

<#root>

admin:

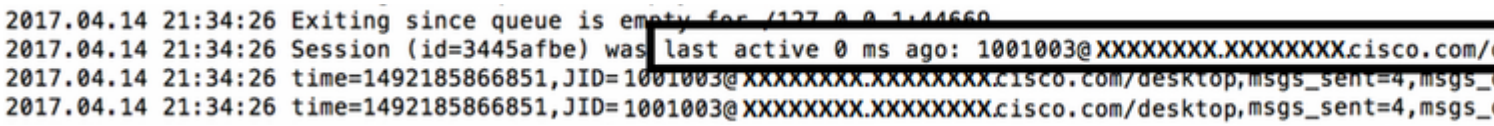
utils finesse notification logging enable

```
Checking that the Cisco Finesse Notification Service is started...
The Cisco Finesse Notification Service is started.

Cisco Finesse Notification Service logging is now enabled.

WARNING! Cisco Finesse Notification Service logging can affect system performance
and should be disabled when logging is not required.

Note: Logging can be disabled automatically if you restart the Cisco Finesse Notification Service
```

Deze logboeken bevinden zich in de map /desktop/logs/openfire en hebben de naam debug.log.

Zoals te zien in de afbeelding toont het bestand debug.log van de Notification Service (Openfire) de http-binding met de desktop samen met het IP-adres en de poort van de pc van de medewerker.

Zoals te zien in de afbeelding, geeft het bericht last active 0 ms aan dat de sessie nog actief is.



Openfire sluit de ongebruikte sessie geeft aan dat de agent logout kan starten in 60 seconden, waar Finesse een gedwongen logout met een rede code van 255 kan sturen naar de CTI-server. Het daadwerkelijke gedrag van de desktop in deze omstandigheden hangt af van de instelling voor Logout on Agent Disconnect (LOAD) in UCCE. In UCCX is dit altijd het gedrag.

Als de Fineese client geen http-bind-berichten naar de Finesse-server stuurt, kunnen de logbestanden de sessie-up-tijd tonen en de sessie-afsluiting tonen.

```
2017.06.17 00:14:34 Session (id=f382a015) was last active 0 ms ago: 1001003@xxxxx.xxxx.xxx.cisco.com/des
2017.06.17 00:15:04 Session (id=f382a015) was last active 13230 ms ago: 1001003@xxxxx.xxxx.xxx.cisco.com
2017.06.17 00:15:34 Session (id=f382a015) was last active 43230 ms ago: 1001003@xxxxx.xxxx.xxx.cisco.com
2017.06.17 00:16:04 Session (id=f382a015) was last active 63231 ms ago: 1001003@xxxxx.xxxx.xxx.cisco.com

2017.06.17 00:17:04 Unable to route packet. No session is available so store offline. <message from="pub
```

Informatielogboeken van Notification Service

Deze logboeken zijn in de map /desktop/logs/openfire en worden info.log genoemd. Als de Fineese client geen http-bind-berichten naar de Finesse-server stuurt, kunnen de logbestanden tonen dat de sessie inactief wordt.

```
2017.06.17 00:16:04 Closing idle session (id=f382a015): 1001003@xxxxx.xxxx.xxx. cisco.com/desktop
after inactivity for more than threshold value of 60
2017.06.17 00:16:04 A session is closed for 1001003@xxxxx.xxxx.xxx. cisco.com/desktop
```

Logboeken van webservices

Deze logboeken zijn in de map /desktop/logs/webservices en worden Desktop-webservices.YYYY-MM-DDTHH-MM-SS.sss.log genoemd. Als de Fineese client geen http-bind-berichten naar de Finesse-server verstuurt binnen de opgegeven tijd, kunnen de logbestanden tonen dat de agent-presense niet beschikbaar wordt en 60 seconden later kan een presense gedreven logout optreden.

```
0000001043: XX.XX.XX.XXX: Jun 17 2017 00:16:04.630 +0530: %CCBU_Smack Listener Processor (1)-6-PRESENCE_
0000000417: XX.XX.XX.XXX: Jun 17 2017 00:16:04.631 +0530: %CCBU_Smack Listener Processor (1)-6-UNSUBSCRI
0000001044: XX.XX.XX.XXX:  Jun 17 2017 00:16:04.631 +0530: %CCBU_Smack Listener Processor (1)-6-AGENT_PR
0000001051: XX.XX.XX.XXX:  Jun 17 2017 00:16:35.384 +0530: %CCBU_pool-8-thread-1-6-AGENT_PRESENCE_MONITO
0000001060: XX.XX.XX.XXX:: Jun 17 2017 00:17:04.632 +0530: %CCBU_CoreImpl-worker12-6-PRESENCE DRIVEN LOG
0000001061: XX.XX.XX.XXX:: Jun 17 2017 00:17:04.633 +0530: %CCBU_CoreImpl-worker12-6-MESSAGE_TO_CTI_SERV
1, workmode : 0, reason code: 255, forceflag :1, agentcapacity: 1, agentext: 1001003, agentid: 1001003,
0000001066:  XX.XX.XX.XXX:: Jun 17 2017 00:17:04.643 +0530: %CCBU_CTIMessageEventExecutor-0-6-DECODED_ME
skillGroupNumber=-1, skillGroupPriority=0, agentState=1 (LOGOUT), eventReasonCode=255, numFltSkillGroups
duration=null, nextAgentState=null, fltSkillGroupNumberList=[], fltSkillGroupIDList=[], fltSkillGroupPri
msgID=30, timeTracker={"id":"AgentStateEvent","CTI_MSG_RECEIVED":1497638824642,"CTI_MSG_DISPATCH":149763
Decoded Message to Finesse from backend cti server
```

Veelvoorkomende redenen voor verbroken BOSH-verbinding

BOSH-verbindingen zijn ingesteld door de webclient en de Finesse-server bepaalt of de medewerker onbeschikbaar is. Deze problemen zijn bijna altijd problemen aan de clientzijde, zoals problemen gerelateerd aan de browser, het netwerk of de computer van de medewerker, aangezien de client verantwoordelijk is voor het opzetten van de verbinding.

Probleem - Agents verbreken op verschillende tijden (probleem aan clientzijde)

Aanbevolen acties

Controleer op deze problemen:

1. Netwerkkwestie:

- Controleer de firewallregels en -logboeken: TCP-poort 7443 mag niet geblokkeerd of beperkt zijn
- Gebruik een sniffer voor HTTP-webverkeer zoals Fiddler® of Wireshark® om te controleren of de browser http-bind-verzoeken verzendt via TCP-poort 7443 en responsen ontvangt
- Controleer alle netwerkapparaten/interfaces tussen de computer van de medewerker en de Finesse-server op overmatige vertraging of pakketafwijzingen
    - Traceroute kan handig zijn om het pad te bepalen en vertragingen te bepalen
        - Op een pc met Microsoft® Windows®: tracert {IP-adres van Finesse-server | FQDN van Finesse-server}
        - Op een Mac®: traceroute {IP-adres van Finesse-server | FQDN van Finesse-server}
        - Op Cisco IOS®-software kunnen de interfacestatistieken worden gecontroleerd: interfaces weergeven
            - Raadpleeg Afwijzingen in invoerwachtrijen en afwijzingen in uitvoerwachtrijen troubleshooten
- Finesse-clientlogboeken verzamelen voor een testagent. Clientlogboeken kunnen op drie manieren worden verzameld:
    1. Logboeken van webconsoles van browsers
        - Webconsole van Firefox
        - Microsoft Edge-webconsole
        - Webconsole van Chrome
    2. Klik op de knop Send Error Report (Foutenrapport verzenden) op de Finesse-pagina en verzamel de logboeken van de Finesse-server. U kunt de logboeken vinden in **/desktop/logs/clientlogs.**
    3. Meld u aan via https://<Finesse-FQDN>/desktop/locallog en verzamel de logboeken nadat het probleem optreedt.

De client maakt elke minuut verbinding met de Finesse-server om afwijkingen en netwerklatentie te berekenen:

```
<PC date-time with GMT offset>: : <Finesse FQDN>: <Finesse server date-time with offset>:
Header : Client: <date-time>, Server: <date-time>, Drift: <drift> ms, Network Latency (round trip): <RT

2019-01-11T12:24:14.586 -05:00: : fin1.ucce.local: Jan 11 2019 11:24:14.577 -0600: Header : Client: 2019
```

Raadpleeg Problemen met logboekinzameling oplossen bij problemen met Cisco Finesse Desktop Persistent Logging Probleem

2. Niet-ondersteunde browser en/of versie:

Gebruik ondersteunde browsers/versies en instellingen zoals aangegeven in de compatibiliteitsmatrices:

Compatibiliteitsmatrix voor UCCE

Compatibiliteitsmatrix voor UCCX

3. Browser vastgelopen voorwaarde door inhoud/verwerking van ander tabblad/venster:

Controleer de workflow van de medewerkers en ga na of deze:

- Regelmatig andere tabbladen of vensters open hebben met andere realtime apps zoals muziek-/videostreaming, WebSocket-verbindingen, aangepaste webclients voor Customer Relationship

Management (CRM), enz.
- Een zeer groot aantal tabbladen of vensters open hebben
- Caching in de browser hebben uitgeschakeld
- Hun browser lange tijd open hebben gehouden en deze niet afsluiten aan het einde van de werkdag

4. Computer in stand-by:

Controleer of de medewerkers hun computer op stand-by zetten zonder zich af te melden voor Finesse, of de timer voor de stand-bymodus erg kort is.

5. Probleem met hoog CPU- of geheugengebruik op computer met client:

- Als de browser van de medewerker in een gedeelde omgeving draait, zoals Microsoft Windows Remote Desktop Services, Citrix® XenApp® of Citrix XenDesktop®, ga dan na of de prestaties van de browser afhankelijk zijn van het aantal gebruikers dat tegelijkertijd dezelfde browser gebruikt
    - Zorg er voor dat de juiste bronnen voor CPU en geheugen zijn geconfigureerd op basis van het aantal gebruikers

- Controleer op problemen met bronbenutting:
    - Windows:
        - Windows PowerShell Get-Counter-opdracht die controleert % van de CPU-tijd, Megabytes geheugen beschikbaar, en % van het geheugen in gebruik elke 2 seconden: Get-Counter - Counter "\Processor(_Total)\% Processor Time","\Memory\Available MBytes","\Memory\% Toegewijde bytes in gebruik" -SampleInterval 2 -Continuous
        - In plaats van PowerShell kunt u ook Windows Prestatiemeter gebruiken
        - Taakbeheer kan worden gebruikt om live statistieken van CPU en geheugen te bekijken, zowel algemeen als per proces
    - Mac:
        - Terminal Top commando dat live totale CPU en geheugen controleert: top
            - Controleer processen en sorteer op CPU-gebruik: top -o CPU
            - Controleer processen en sorteer op geheugengebruik: top -o MEM
        - Activiteitenweergave kan worden gebruikt om live statistieken van CPU en geheugen te bekijken, zowel algemeen als per proces

6. Gadgets van derden die onverwachte, problematische activiteiten op de achtergrond uitvoeren:

Test het gedrag van Finesse op de desktop als alle gadgets van externe partijen zijn verwijderd.

7. Probleem met NTP op server of client:

- Gebruik **utils ntp status** op de Finesse publisher-server en controleer dat het stratum van de NTP-server 4 of lager is
- Controleer de client-logboeken op afwijkingen en netwerklatentie

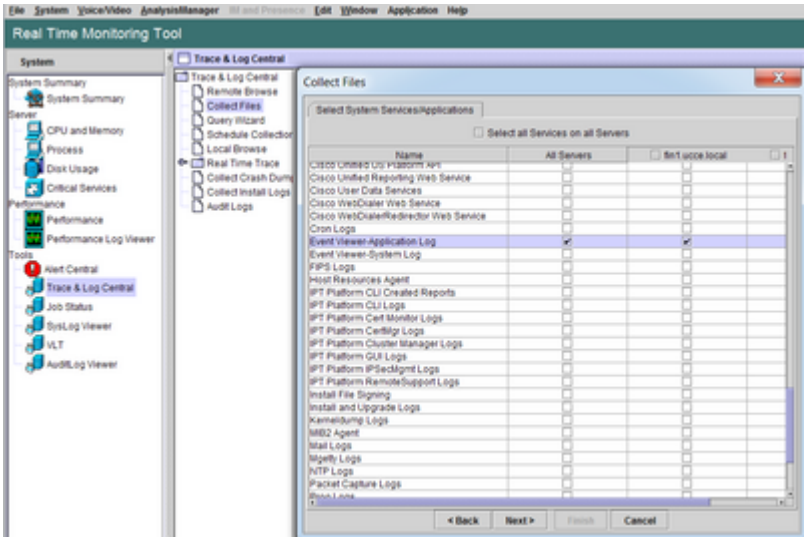
Probleem - Alle agents verbreken tegelijk (serverprobleem)

Aanbevolen acties

Controleer op deze problemen:

1. Cisco Unified Communications Manager CTIM Manager-service - Verbinding verbreken. Als alle CTIManager-providers voor UCCX afsluiten of crashen zijn, zien UCCX-agents de rode banner fout. UCCE-medewerkers krijgen de rode banner niet te zien, maar er kunnen geen oproepen naar hen worden gerouteerd.

- Controleer of de Cisco CTIManager-service is gestart op de CUCM-servers die als CTI-providers worden gebruikt
- Controleer via het Toepassingslogboek in Logboeken op RTMT of de Cisco CTIManager-service is gecrasht
    - Als u gebeurtenisviewer-logbestanden wilt verzamelen op RTMT, gaat u naar **Systeem > Gereedschappen > Trace en Log Central > Bestanden verzamelen > Systeemservices/toepassingen selecteren > Event Viewer-Application Log**.



- Om de Event Viewer-Application logs op CLI te verzamelen: file get activelog/syslog/CiscoSyslog* basis hh:mm:MM/DD/YY hh:mm:MM/DD/YY
- Ga als volgt te werk om coredumps via de opdrachtregelinterface te bekijken: utils core active list

---

Opmerking: Bestandsnamen van coredumps gebruiken de volgende notatie: **core.<ProcessID>.<SignalNumber>.<ProcessName>.<EpochTime>.**
Bijvoorbeeld: core.24587.6.CTIManager.1533441238
Zodoende kan het tijdstip van de crash worden bepaald op basis van de Unix-tijd (epoch).

---

2. De Finesse/UCS Notification Service is gestopt of crasht:

- Controleer de toepassingslogboeken in Event Viewer (Logboeken) op foutmeldingen van de Notification Service om te zien of de service is gestopt
- Controleer of de Notification Service in werking is: utils service list
- Controleer hoe vaak de melddienst is gesloten: bestandszoekactivelog /desktop/logs/openfire "OpenFire gestopt"
- Controleer hoe vaak de Notification-service is gestart: file search activelog /desktop/logs/openfire "HTTP bind service gestart"
- Controleer op geheugenstortplaatsen die het gevolg zijn van een crash: file list activelog /desktop/logs/openfire/*.hprof
- Controleer of de Notification-service op TCP-poort 7443 luistert: toon open poorten regexp 7443.*LISTEN
- Controleer of deze gebreken van toepassing zijn (ze zouden leiden tot inlogfouten voor medewerkers die inloggen en voor medewerkers die al zijn ingelogd; deze medewerkers krijgen de rode banner te zien met het bericht dat de verbinding met Finesse is verbroken):
    - Cisco bug-id CSCva72280 - Finesse Tomcat en Open Fire Crash voor ongeldige XML-tekens
    - Cisco bug-id CSCva72325 - UCCX: Finesse Tomcat en Open Fire Crash voor ongeldige XML-tekens

Start Cisco Finesse Tomcat en de Notification Service opnieuw als u een crash vermoedt. Dit wordt alleen aanbevolen als het netwerk inactief is, anders wordt de verbinding tussen de medewerkers en de Finesse-server verbroken.

Stappen voor UCCE:

- utils service stop Cisco Finesse Tomcat
- utils service stop Cisco Finesse Notification Service
- utils service start Cisco Finesse Tomcat
- utils service start Cisco Finesse Notification Service

Stappen voor UCCX:

- utils service stop Cisco Finesse Tomcat
- utils service stop Cisco Unified CCX Notification Service
- utils service start Cisco Finesse Tomcat
- utils service start Cisco Unified CCX Notification Service

Fiddler gebruiken

Het configureren van Fiddler kan een uitdaging zijn als u niet begrijpt hoe Fiddler werkt en welke stappen er moeten worden genomen. Fiddler is een tussenliggende webproxy tussen de Finesse-client (webbrowser) en Finesse-server. Door de verbindingen tussen de Finesse-client en de Finesse-server, voegt dit een laag van complexiteit toe aan de Fiddler-configuratie om beveiligde berichten te bekijken.

Veelvoorkomend probleem met Fiddler

Aangezien Fiddler zich tussen de Finesse-client en Finesse-server bevindt, moet de Fiddler-app ondertekende certificaten maken voor alle Finesse TCP-poorten die certificaten nodig hebben:

Cisco Finesse Tomcat-servicecertificaten

1. Finesse publisher-server TCP 8445 (en/of 443 voor UCCE)
2. Finesse subscriber-server TCP 8445 (en/of 443 voor UCCE)

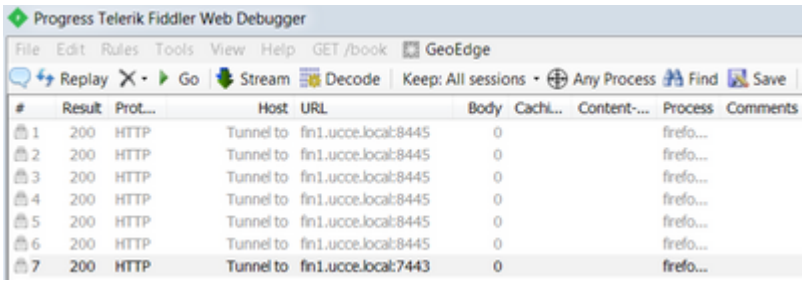
Certificaten van Cisco Finesse (Unified CCX) Notification Service

1. Finesse publisher-server TCP 7443
2. Finesse subscriber-server TCP 7443

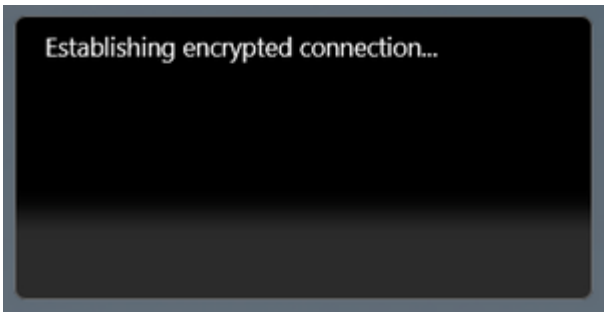
HTTPS-decryptie moet ingeschakeld zijn voordat Fiddler namens de Finesse-server dynamische certificaten kan genereren. Dit is standaard niet ingeschakeld.

Als HTTPS-decryptie niet is geconfigureerd, wordt de initiële tunnelverbinding met de Notification Service gezien, maar het http-bind-verkeer niet. Fiddler toont alleen:

```
Tunnel to <Finesse server FQDN>:7443
```



De Finesse-certificaten die door Fiddler zijn ondertekend, moeten vervolgens door de client worden vertrouwd. Als deze certificaten niet worden vertrouwd, kunt u niet verder dan de fase Establishing encrypted connection... (Bezig met opzetten van versleutelde verbinding ...) van het aanmeldproces van Finesse.



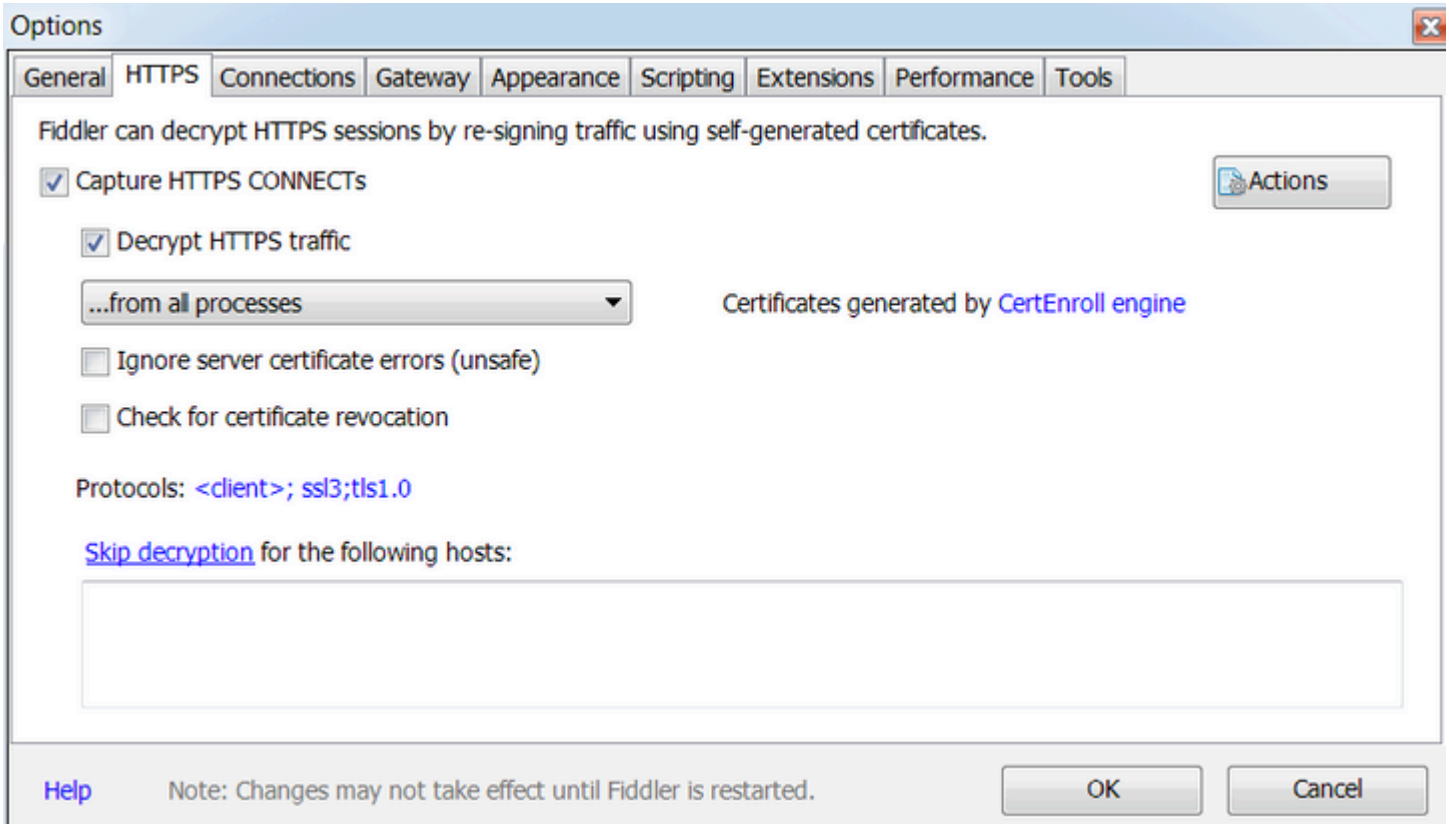
In sommige gevallen volstaat het niet de certificaatuitzonderingen vanuit de login te accepteren, en moeten de certificaten handmatig worden vertrouwd door de browser.

Stappen van voorbeeldconfiguratie

> **Waarschuwing**: de voorbeeldconfiguratie is voor Fiddler v5.0.20182.28034 voor .NET 4.5en Mozilla Firefox 64.0.2 (32-bits) op Windows 7 x64 in een laboratoriumomgeving. Deze procedures kunnen niet generaliseren naar alle versies van Fiddler, alle browsers of alle computer besturingssystemen. Als uw netwerk live is, zorg er dan voor dat u de mogelijke impact van elke configuratie begrijpt. Raadpleeg de officiële documentatie van Fiddler voor meer informatie.

Stap 1. Downloadfilter

Stap 2. HTTPS-decryptie inschakelen. Navigeer naar **Gereedschappen > Opties > HTTPS** en controleer het vakje **HTTPS-verkeer ontsleutelen**.

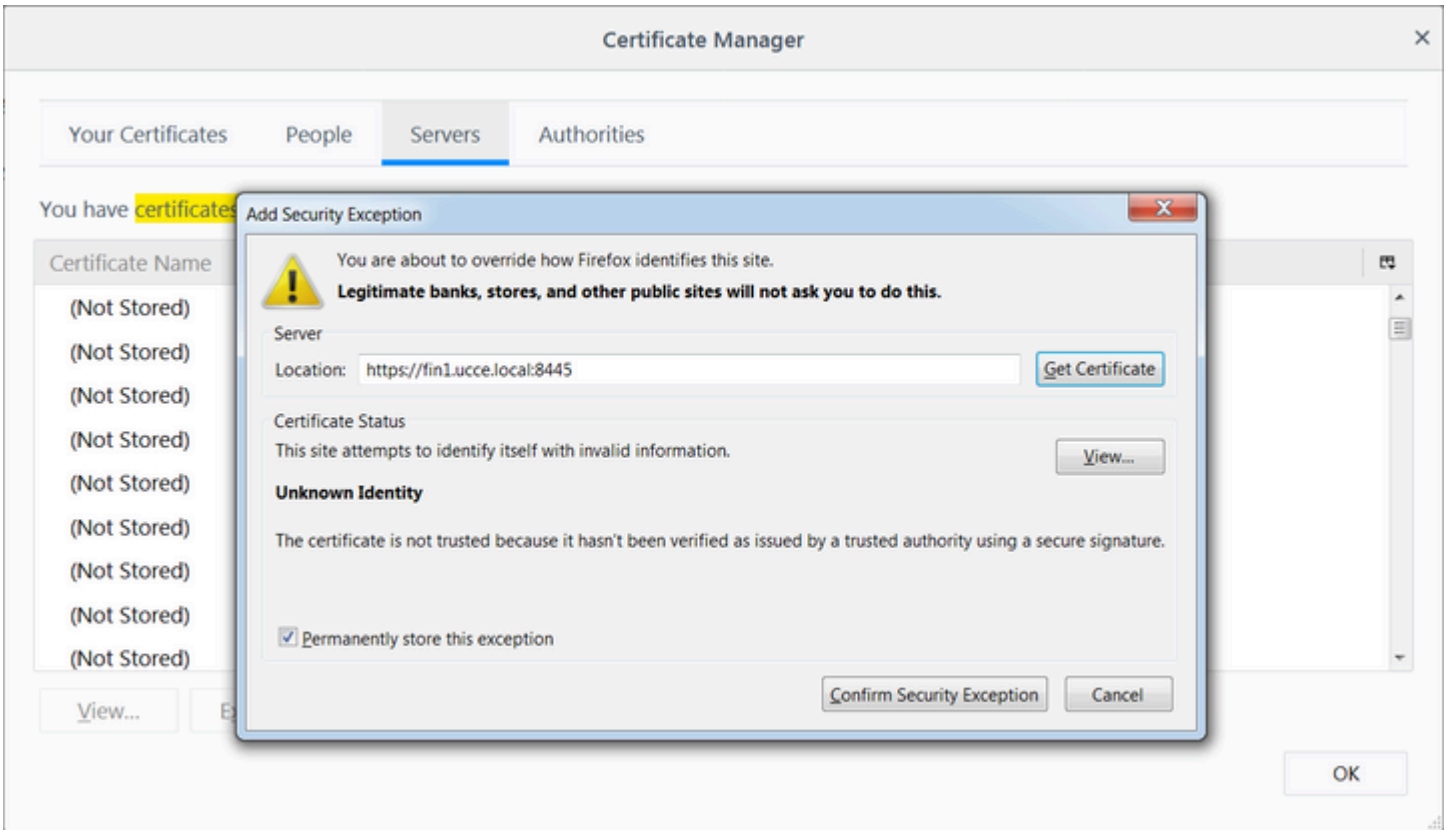


Stap 3. Er wordt een waarschuwingsbericht geopend met de vraag of het basiscertificaat van Fiddler moet worden vertrouwd. Kies Yes.

Stap 4. Een waarschuwingsbericht wordt geopend met het bericht "U staat op het punt om een certificaat te installeren van een certificeringsinstantie (CA) die beweert het volgende te vertegenwoordigen: DO_NOT_TRUST_FiddlerRoot... Do you want to install this certificate?â€ (U staat op het punt om een certificaat van een certificeringsinstantie (CA) te installeren die als vertegenwoordiging optreedt van DO_NOT_TRUST_FiddlerRoot â€¦ Wilt u dit certificaat installeren?). Kies **Yes**.

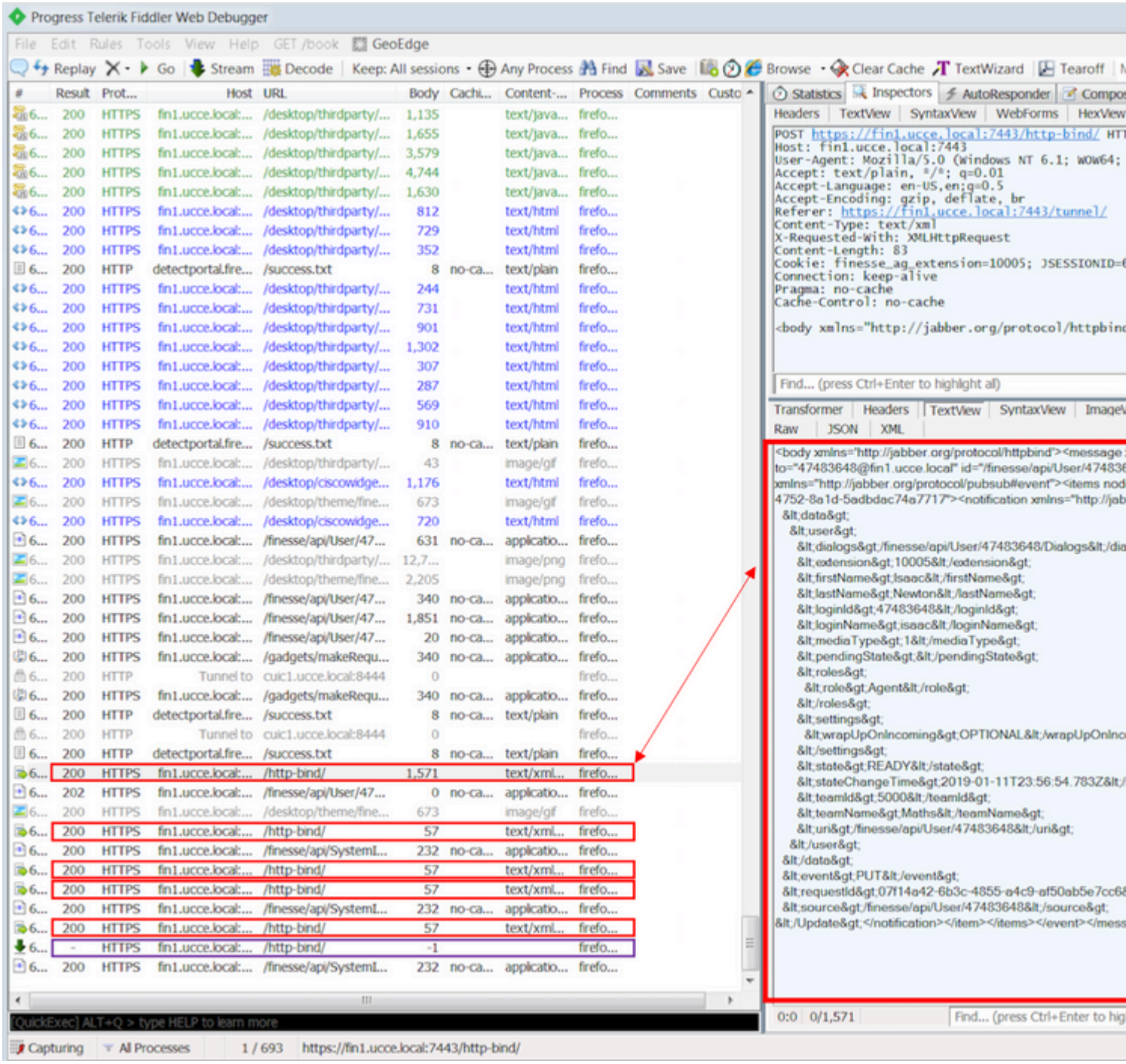
Stap 5. Voeg de Finesse-uitgever en abonneecertificaten handmatig toe aan de computer of browser-certificaattrust. Zorg voor poorten 8445, 7443 en (alleen voor UCS) 443. Op Firefox kan dit bijvoorbeeld eenvoudig worden gedaan zonder certificaten te downloaden van de Finesse Operating System Administration pagina:

Options > Find in Options (search)**> Certificates > Servers > Add Exception > Location (Opties > Zoeken in opties > (zoeken) > Certificaten > Servers > Uitzondering toevoegen > Locatie) en hier https://<Finesse server>:poort in te voeren voor de relevante poorten voor beide Finesse-servers.**

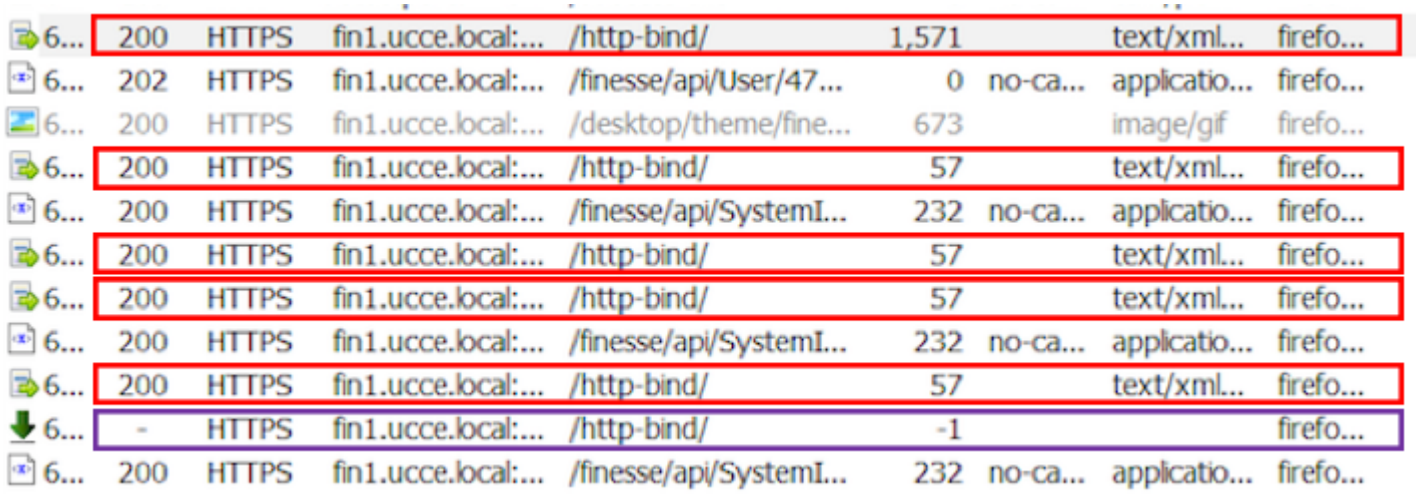


Stap 6. Log in op Finesse en bekijk de http-bind berichten verlaat de Finesse client via Fiddler naar de Finesse Server.

In dit voorbeeld duiden de eerste vijf berichten op http-bind-berichten waarop de Finesse-server heeft gereageerd. Het eerste bericht bevat 1571 bytes aan data die in de berichttekst is geretourneerd. Het lichaam bevat een XMPP update over een medewerkergebeurtenis. Het laatste http-bind-bericht is verzonden door de Finesse-client maar heeft geen respons gekregen van de Finesse-server. Dit kan worden bepaald wanneer u ziet dat het HTTP-resultaat ongeldig is (-) en het aantal bytes in de responsinstantie ongeldig is (-1).



Ingezoomde weergave op de data:



6...	200	HTTPS	fin1.ucce.local:...	/http-bind/	1,571		text/xml...	firefo...
6...	202	HTTPS	fin1.ucce.local:...	/finesse/api/User/47...	0	no-ca...	applicatio...	firefo...
6...	200	HTTPS	fin1.ucce.local:...	/desktop/theme/fine...	673		image/gif	firefo...
6...	200	HTTPS	fin1.ucce.local:...	/http-bind/	57		text/xml...	firefo...
6...	200	HTTPS	fin1.ucce.local:...	/finesse/api/SystemI...	232	no-ca...	applicatio...	firefo...
6...	200	HTTPS	fin1.ucce.local:...	/http-bind/	57		text/xml...	firefo...
6...	200	HTTPS	fin1.ucce.local:...	/http-bind/	57		text/xml...	firefo...
6...	200	HTTPS	fin1.ucce.local:...	/finesse/api/SystemI...	232	no-ca...	applicatio...	firefo...
6...	200	HTTPS	fin1.ucce.local:...	/http-bind/	57		text/xml...	firefo...
6...	-	HTTPS	fin1.ucce.local:...	/http-bind/	-1			firefo...
6...	200	HTTPS	fin1.ucce.local:...	/finesse/api/SystemI...	232	no-ca...	applicatio...	firefo...

Responstekst voor XMPP-bericht:


```
<body xmlns='http://jabber.org/protocol/httpbind'><message xmlns="jabber:client" from="pubsub.fin1.ucce.local"
to="47483648@fin1.ucce.local" id="/finesse/api/User/47483648__47483648@fin1.ucce.local__K7hYF"><event
xmlns="http://jabber.org/protocol/pubsub#event"><items node="/finesse/api/User/47483648"><item id="26a3e421-
4752-8a1d-5adbdac74a7717"><notification xmlns="http://jabber.org/protocol/pubsub">&lt;Update&gt;
 &lt;data&gt;
  &lt;user&gt;
   &lt;dialogs&gt;/finesse/api/User/47483648/Dialogs&lt;/dialogs&gt;
   &lt;extension&gt;10005&lt;/extension&gt;
   &lt;firstName&gt;Isaac&lt;/firstName&gt;
   &lt;lastName&gt;Newton&lt;/lastName&gt;
   &lt;loginId&gt;47483648&lt;/loginId&gt;
   &lt;loginName&gt;isaac&lt;/loginName&gt;
   &lt;mediaType&gt;1&lt;/mediaType&gt;
   &lt;pendingState&gt;&lt;/pendingState&gt;
   &lt;roles&gt;
    &lt;role&gt;Agent&lt;/role&gt;
   &lt;/roles&gt;
   &lt;settings&gt;
    &lt;wrapUpOnIncoming&gt;OPTIONAL&lt;/wrapUpOnIncoming&gt;
   &lt;/settings&gt;
   &lt;state&gt;READY&lt;/state&gt;
   &lt;stateChangeTime&gt;2019-01-11T23:56:54.783Z&lt;/stateChangeTime&gt;
   &lt;teamId&gt;5000&lt;/teamId&gt;
   &lt;teamName&gt;Maths&lt;/teamName&gt;
   &lt;uri&gt;/finesse/api/User/47483648&lt;/uri&gt;
  &lt;/user&gt;
 &lt;/data&gt;
 &lt;event&gt;PUT&lt;/event&gt;
 &lt;requestId&gt;07f14a42-6b3c-4855-a4c9-af50ab5e7cc6&lt;/requestId&gt;
 &lt;source&gt;/finesse/api/User/47483648&lt;/source&gt;
&lt;/Update&gt;</notification></item></items></event></message></body>
```


Wireshark gebruiken

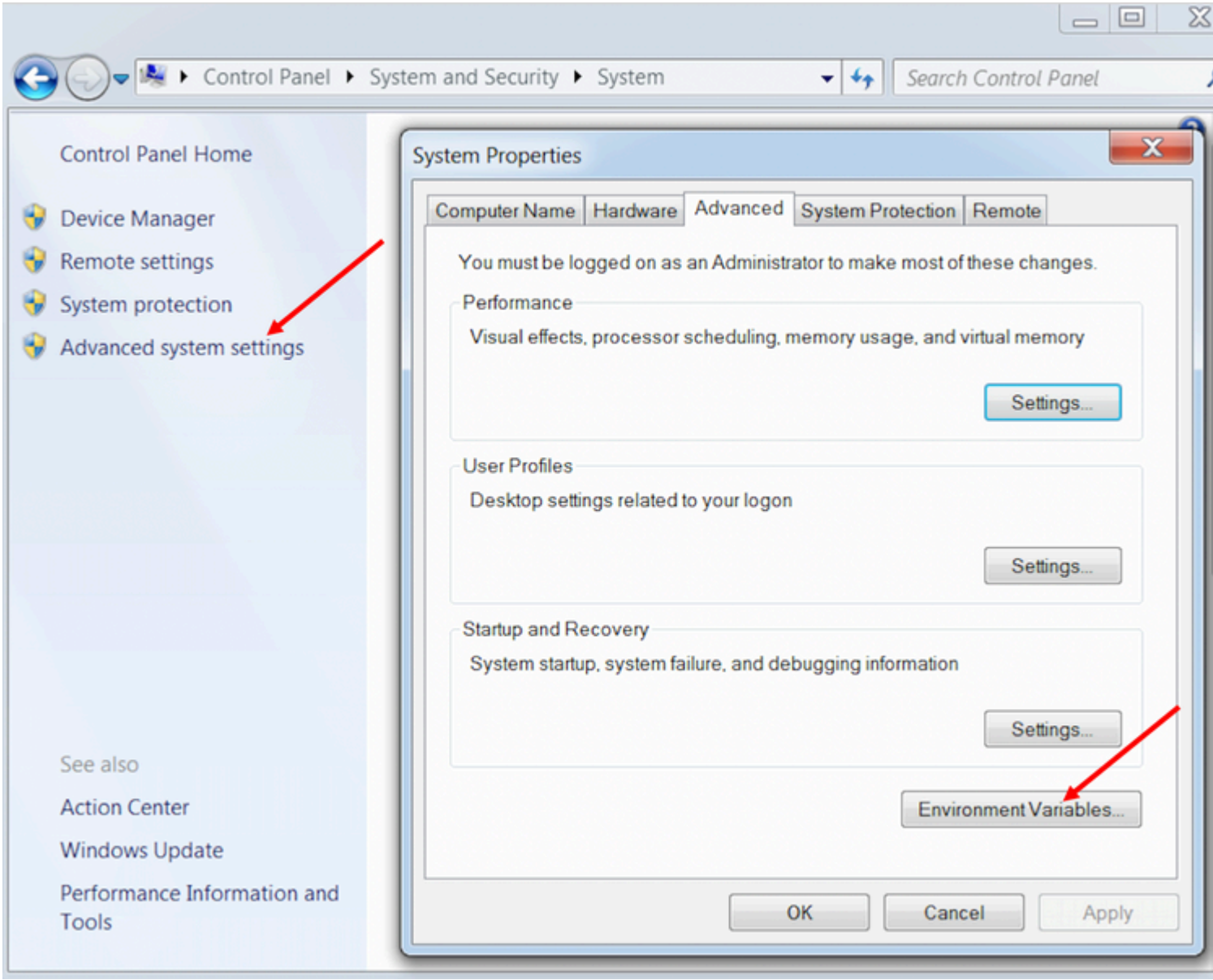
Wireshark is een algemeen gebruikte tool voor sniffing van pakketten dat kan worden gebruikt om HTTPS-verkeer te sniffen en decoderen. HTTPS-verkeer is HTTP-verkeer via Transport Layer Security (TLS) beveiligd. TLS biedt integriteit, authenticatie en vertrouwelijkheid tussen twee hosts. Het wordt veel

gebruikt in webapps, maar kan worden gebruikt met elk protocol dat TCP gebruikt als het transportlaagprotocol. Secure Sockets Layer (SSL) is de verouderde versie van het TLS-protocol en wordt wegens onveiligheid niet meer gebruikt. Deze namen worden vaak verwisseld, en het Wireshark-filter voor SSL- of TLS-verkeer is ssl.

> **Waarschuwing**: de voorbeeldconfiguratie is voor Wireshark 2.6.6 (v2.6.6-0-gdf942cd8) en Mozilla Firefox 64.0.2 (32-bit) op Windows7 x64 in een lab-omgeving. Deze procedures kunnen niet generaliseren naar alle versies van Fiddler, alle browsers of alle computer besturingssystemen. Als uw netwerk live is, zorg er dan voor dat u de mogelijke impact van elke configuratie begrijpt. Raadpleeg de officiële documentatie van Wireshark SSL voor meer informatie. Wireshark 1.6 of nieuwer is vereist.

> **Opmerking**: deze methode kan alleen werken voor Firefox en Chrome. Deze methode werkt niet voor Microsoft Edge.

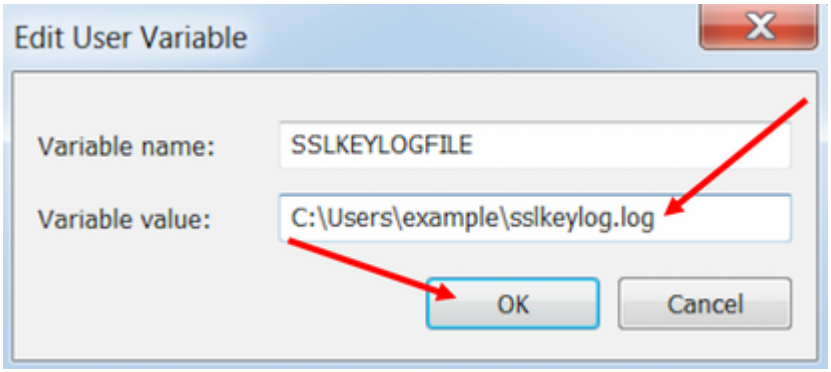
Stap 1. Op de Windows PC van de agent navigeer naar **Configuratiescherm > Systeem en beveiliging > Systeem > Geavanceerde systeeminstellingen Milieuvariabelen...**



Stap 2. Navigeren naar **gebruikersvariabelen voor gebruiker <gebruikersnaam> > Nieuw...**

Maak een variabele aan met de naam **SSLKEYLOGFILE.**

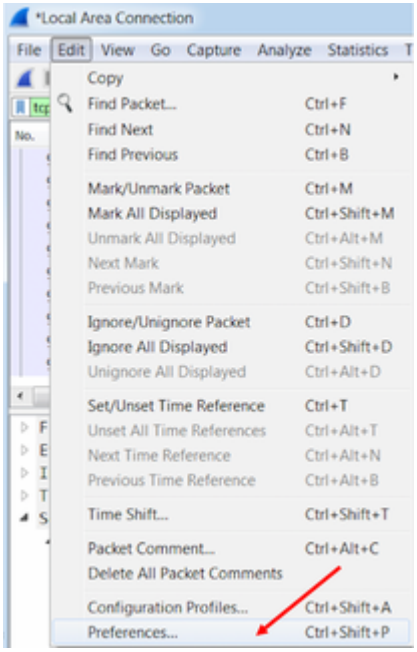
Maak een bestand om de pre-master secret van SSL op te slaan in een privé-map: SSLKEYLOGFILE=</path/to/private/directory/with/logfile>



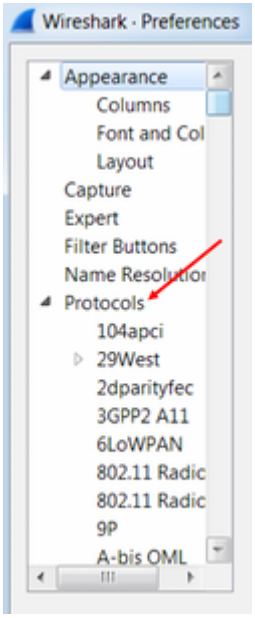
> **Opmerking**: Maak een systeemvariabele in plaats van een gebruikersvariabele en/of sla het bestand op in een niet-private directory, maar dan kunnen alle gebruikers op het systeem toegang krijgen tot het premaster geheim, dat minder veilig is.

Stap 3. Als Firefox of Chrome zijn geopend, sluit u de toepassingen. Nadat ze zijn heropend, kunnen ze beginnen met schrijven naar het SSLKEYLOGFILE.

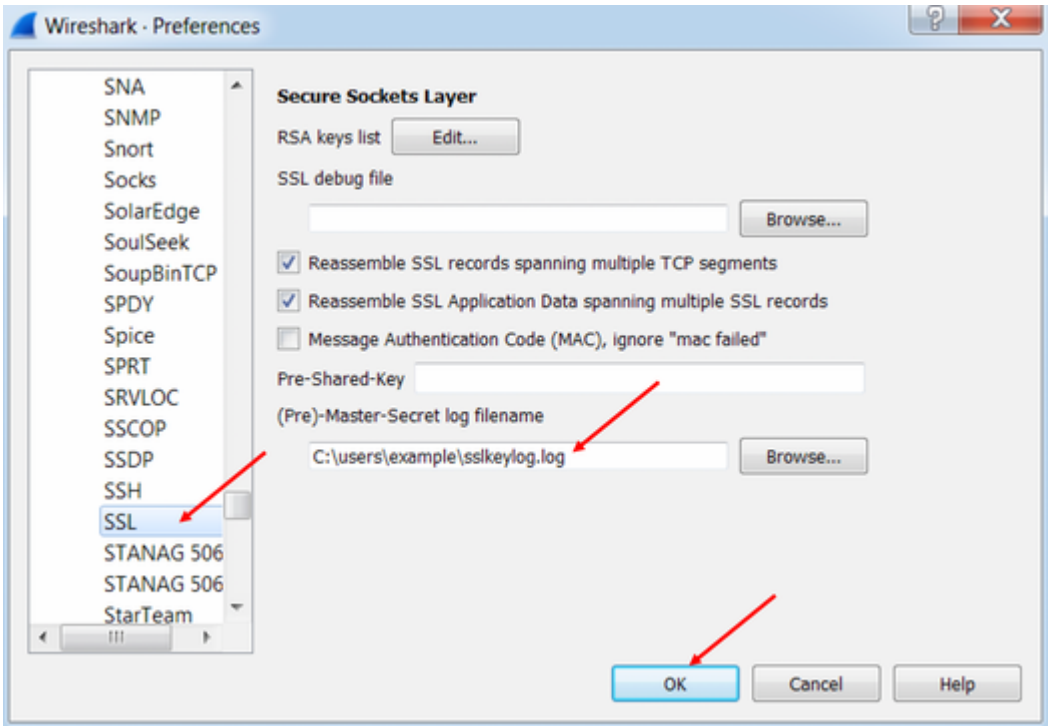
Stap 4. Ga bij Wireshark naar **Bewerken > Voorkeuren...**



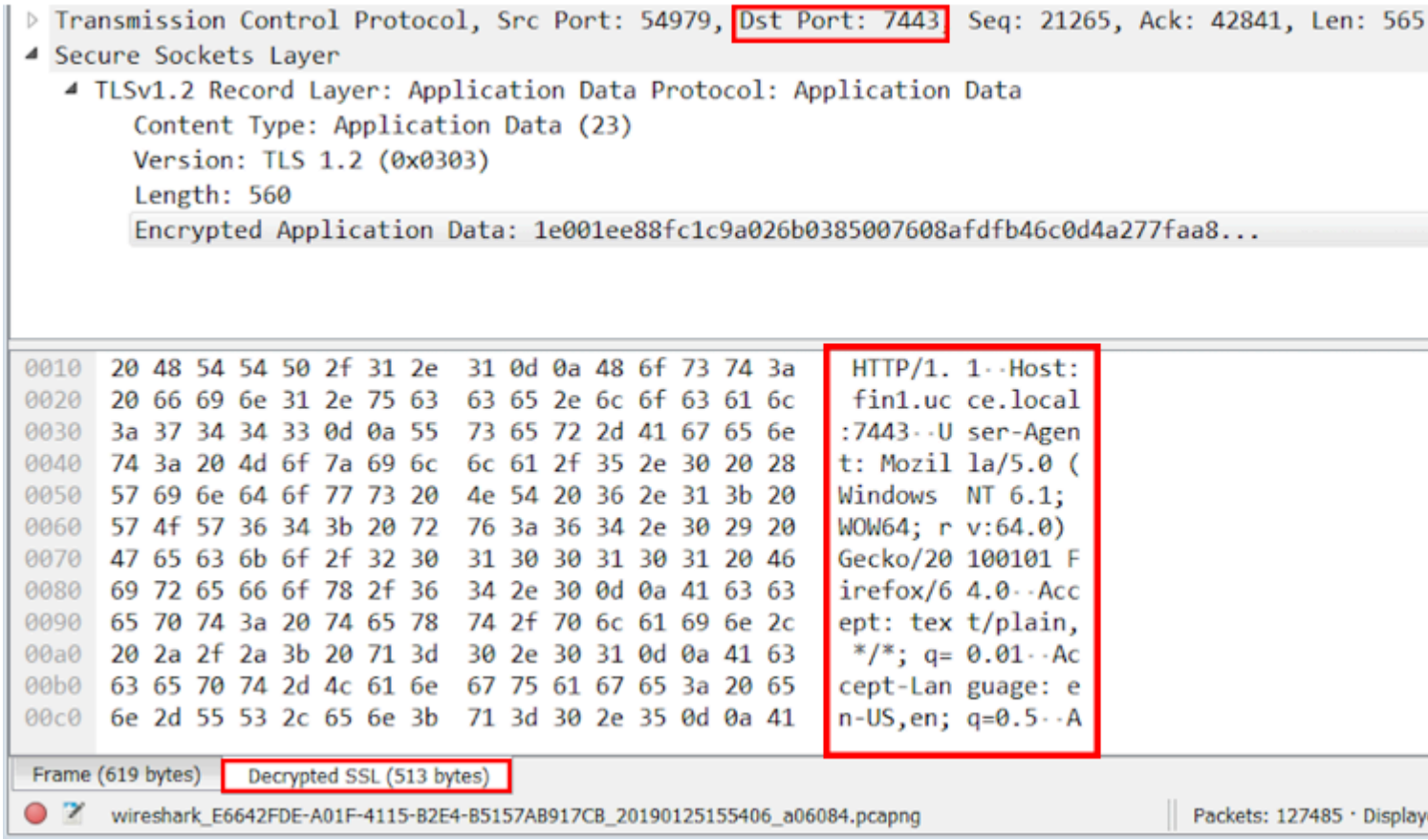
Ga naar **Protocols > SSL**.



Stap 5. Voer de locatie in van de vooraf ingestelde bestandsnaam van het geheime logboek die in Stap 2 is ingesteld.



Stap 6. Gebruik Wireshark filter **tcp.port==7443 & ssl**, de beveiligde HTTP communicatie tussen de Finesse-client en Finesse-server (Notification Service) wordt gezien als ontsleuteld.



Gerelateerde gebreken

- Cisco bug-id CSCva72280 - Finesse Tomcat en OpenFire Crash voor ongeldige XML-tekens
- Cisco bug-id CSCva72325 - UCCX: Finesse Tomcat en Open Fire Crash voor ongeldige XML-tekens

Gerelateerde informatie

- XMPP-specificaties
- XEP-0124: BOSH
- XEP-0060: publiceren-abonneren
- Webconsole van Firefox
- Microsoft Edge-webconsole
- Webconsole van Chrome
- Windows PowerShell
- Windows Prestatiemeter
- Afwijzingen in invoerwachtrijen en afwijzingen in uitvoerwachtrijen troubleshooten
- Windows Taakbeheer
- Mac Terminal
- Mac Activiteitenweergave
- Fiddler downloaden
- Fiddler configureren
- Wireshark downloaden
- Wireshark SSL-decryptie
- Technische ondersteuning en documentatie â€“ Cisco Systems

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.