# **Comprendre et dépanner la mise en oeuvre de Finesse BOSH**

# Table des matières

Introduction Conditions préalables Exigences Composants utilisés Informations générales Comprendre la mise en oeuvre de Finesse BOSH Comprendre XMPP Exemple de message XMP Mise en oeuvre XMPP avec finesse Exemple de requête/réponse XMPP Finesse Comprendre les messages et les noeuds XMPP de Finesse Exemple 1 : Utiliser Pidgin pour afficher les noeuds XMPP Finesse Exemple 2 : Utiliser l'onglet Réseau des outils de développement de navigateur pour afficher les messages HTTP Dépannage du message d'erreur de déconnexion BOSH Analyse des journaux Journaux du service de notification de débogage Journaux du service de notification Info Journaux des services Web Raisons courantes de la déconnexion BOSH Problème - Déconnexion des agents à différents moments (problème côté client) Actions recommandées Problème : tous les agents se déconnectent simultanément (problème côté serveur) Actions recommandées **Utiliser Fiddler** Émission De Violon Commun Exemple d'étapes de configuration **Utiliser Wireshark** Défauts associés Informations connexes

# Introduction

Ce document décrit l'architecture derrière les connexions Finesse qui utilisent BOSH et comment les problèmes de connexion BOSH peuvent être diagnostiqués.

# **Conditions préalables**

# Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Finesse
- Unified Contact Center Enterprise (UCCE)
- Unified Contact Center Express (UCCX)
- Outils de développement de navigateur Web
- Administration de Windows et/ou Mac

### **Composants utilisés**

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Finesse 9.0(1) 11.6(1)
- UCCX 10.0(1) 11.6(2)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€<sup>TM</sup>incidence possible des commandes.

# **Informations générales**

Les connexions qui utilisent des flux bidirectionnels sur HTTP synchrone sont appelées BOSH.

# Comprendre la mise en oeuvre de Finesse BOSH

# **Comprendre XMPP**

Le protocole XMPP (Extensible Messaging and Presence Protocol) (également connu sous le nom de Jabber) est un protocole avec état dans un modèle client-serveur. XMPP permet la livraison rapide de petits morceaux de données eXtensible Markup Language (XML) structurées d'une entité à une autre. XMPP/Jabber est largement utilisé dans les applications de messagerie instantanée et de présence.

Toutes les entités XMPP sont identifiées par leur ID Jabber (JID).



Schéma d'adressage JID : user@domain/resource

usager	nom d'utilisateur client sur le serveur XMPP ou nom de la salle de conférence
domaine	Nom de domaine complet (FQDN) du serveur XMPP
ressource	identifiant de l'entité/point d'extrémité spécifique de l'utilisateur (par exemple, ordinateur portable, smartphone, etc.), identifiant de session ou nom de noeud pubsub

**Remarque** : les trois composants JID ne sont pas utilisés dans tous les cas. Un serveur est généralement défini par le domaine, une salle de conférence par user@domain et un client par user@domain/resource.

Les messages XMPP sont appelés strophes. Il y a trois strophes principales dans XMPP :

- 1. <message> : une direction, un destinataire
- 2. <présence> : une direction, publier sur plusieurs
- 3. <iq> : info/query request/response

Toutes les strophes ont des adresses de destination et de provenance et la plupart des strophes ont également des attributs type, id et xml : langattribute.

Attribut Stanza	Objectif
par	JID de destination
expéditeur	JID source
type	objet du message
id	identifiant unique utilisé pour lier une requête à une réponse pour les <iq> stanzas</iq>
xml : lang	Définit la langue par défaut de tout code XML lisible par l'utilisateur dans la strophe

#### Exemple de message XMP

```
<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>
```

### Mise en oeuvre XMPP avec finesse

Si une application Web doit fonctionner avec XMPP, plusieurs problèmes surviennent. Les navigateurs ne prennent pas en charge XMPP sur TCP (Transmission Control Protocol) en mode natif, de sorte que tout le trafic XMPP doit être géré par un programme qui s'exécute à l'intérieur du navigateur. Les serveurs et les navigateurs Web communiquent via des messages HTTP (HyperText Transfer Protocol), de sorte que Finesse et d'autres applications Web encapsulent les messages XMPP à l'intérieur des messages HTTP.

La première difficulté de cette approche est que HTTP est un protocole sans état. Cela signifie que chaque requête HTTP n'est liée à aucune autre requête. Cependant, ce problème peut être résolu par des moyens applicatifs, par exemple par l'utilisation de cookies ou de données postales.

La deuxième difficulté est le comportement unidirectionnel du protocole HTTP. Seul le client envoie des requêtes et le serveur ne peut que répondre. L'incapacité du serveur à transmettre des données rend anormale la mise en oeuvre de XMPP sur HTTP.

Ce problème n'existe pas dans la spécification XMPP Core d'origine (RFC 6120), où XMPP est lié à TCP. Cependant, si vous voulez résoudre le problème avec XMPP lié à HTTP, par exemple, parce que Javascript peut envoyer des requêtes HTTP, il y a deux solutions possibles. Les deux nécessitent un pont entre HTTP et XMPP.

Les solutions proposées sont les suivantes :

1. Interrogation (protocole hérité) : requêtes HTTP répétées demandant de nouvelles données définies dans XEP-0025 : Interrogation HTTP Jabber

2. L'interrogation longue est également appelée BOSH : protocole de transport qui émule la sémantique d'une connexion TCP bidirectionnelle à longue durée de vie entre deux entités en utilisant efficacement plusieurs paires requête/réponse HTTP synchrones sans nécessiter l'utilisation d'une interrogation fréquente définie dans XEP-0124 : HTTP Binding et étendue par XEP-0206 : XMPP sur BOSH

Finesse implémente BOSH car il est très efficace du point de vue de la charge du serveur et du trafic. La raison d'utiliser BOSH est de dissimuler le fait que le serveur n'a pas à répondre dès qu'il y a une demande. La réponse est retardée jusqu'à une durée spécifiée jusqu'à ce que le serveur dispose de données pour le client, puis elle est envoyée en tant que réponse. Dès que le client reçoit la réponse, il fait une nouvelle demande, etc.

Le client de bureau Finesse (application Web) établit une connexion BOSH périmée sur le port TCP 7443 toutes les 30 secondes. Au bout de 30 secondes, en l'absence de mises à jour du service de notification Finesse, le service de notification envoie une réponse HTTP avec un 200 OK et un corps de réponse (presque) vide. Si le service de notification dispose d'une mise à jour sur la présence d'un agent ou d'un événement de dialogue (appel), par exemple, les données sont envoyées immédiatement au client Web Finesse.

#### Exemple de requête/réponse XMPP Finesse

Cet exemple montre la première réponse de requête de message XMPP partagée entre le client Finesse et le serveur Finesse pour configurer la connexion BOSH.

```
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" authio</pre>

Pour récapituler :

- 1. Le client Web Finesse dispose d'une connexion HTTP périmée (http-bind) configurée sur le serveur Finesse via le port TCP 7443. C'est ce qu'on appelle un sondage long BOSH.
- 2. Le service de notification Finesse est un service de présence qui publie des mises à jour concernant l'état d'un agent, d'un appel, etc.
- 3. Si le service de notification dispose d'une mise à jour, il répond à la requête http-bind avec la mise à jour d'état sous la forme d'un message XMPP dans le corps de la réponse HTTP.
- 4. S'il n'y a aucune mise à jour d'état 30 secondes après la réception de la demande http-bind, le service de notification répond sans aucune mise à jour d'état pour permettre au client Web Finesse d'envoyer une autre demande http-bind. Cela permet au service de notification de savoir que le client Web Finesse est toujours en mesure de se connecter au service de notification et que l'agent n'a pas fermé son navigateur ou mis son ordinateur en veille, etc.

# Comprendre les messages et les noeuds XMPP de Finesse

Finesse implémente également la spécification XMPP XEP-0060 : Publish-Subscribe. L'objectif de cette spécification est de permettre au serveur XMPP (service de notification) d'obtenir des informations publiées sur les noeuds XMPP (rubriques), puis d'envoyer des événements XMPP aux entités abonnées au noeud. Dans le cas de Finesse, le serveur CTI (Computer Telephony Integration) envoie des messages CTI au service Web Finesse pour informer Finesse des mises à jour de configuration telles que, mais sans s'y limiter, la création d'agent ou de file d'attente de service de contact (CSQ) ou des informations sur un appel. Ces informations sont ensuite converties en un message XMPP que le service Web Finesse publie sur le service de notification Finesse. Le service de notification Finesse ensuite des messages XMPP sur BOSH aux agents qui sont abonnés à certains noeuds XMPP.

Certains des objets de l'API Finesse définis dans le <u>Guide du développeur des services Web Finesse</u> sont des noeuds XMPP. Les clients Web Finesse agent et superviseur peuvent s'abonner à des mises à jour d'événements pour certains de ces noeuds XMPP afin d'avoir des informations à jour sur les événements en temps réel (tels que les événements d'appel, les événements d'état, etc.). Ce tableau présente les noeuds XMPP qui sont activés pour pubsub.

Finesse API, objet	Objectif	Abonnement
/finesse/api/User/ <id connexion="" de=""></id>	Affiche l'état et le mappage d'équipe de l'agent	Agents et superviseurs
/finesse/api/User/ <id connexion="" de="">/Dialogues</id>	Affiche les appels traités par l'agent	Agents et superviseurs
/finesse/api/User/ <identifiantconnexion>/ClientLog</identifiantconnexion>	Utilisé pour capturer les journaux du client à partir du bouton <b>Envoyer le rapport d'erreur</b>	Agents et superviseurs
/finesse/api/User/ <loginid>/Queue/<queueid></queueid></loginid>	Affiche les données statistiques de la file d'attente (si activé)	Agents et superviseurs
/finesse/api/Team/ <idéquipe>/Users</idéquipe>	Affiche les agents qui appartiennent à une certaine équipe, y compris les informations d'état	Superviseurs
/finesse/api/SystemInfo	Affiche l'état du serveur Finesse. Utilisé pour déterminer si le basculement est nécessaire	Agents et superviseurs

#### Exemple 1 : Utiliser Pidgin pour afficher les noeuds XMPP Finesse

Étape 1. Téléchargez et installez le Pidgin du client XMPP.

Étape 2. Accédez à Accounts > Basic et configurez les Options de connexion :

- Protocole : XMPP
- Nom d'utilisateur : LoginID pour tout agent
- Domaine : FQDN du serveur Finesse
- Ressource : Espace réservé toute valeur peut être utilisée, par exemple, test
- Mot de passe : Agent password
- Cochez la case Mémoriser le mot de passe

Modify Account		X						
Basic Advanced Proxy								
Login Options								
Protocol:	₩ XMPP	Ŧ						
Username:	47483648							
Domain:	fin1.ucce.local							
<u>R</u> esource:	test							
Password:	•••••							
Remember pass	vord							
User Options	User Options							
Local alias:								
New <u>m</u> ail notification	ations							
Use this buddy ic	on for this account:							
<u>Remove</u>								
Create this new accour	nt on the server							
	Cancel	<u>S</u> ave						

Étape 3. Accédez à **Comptes > Modifier > Avancé** et configurez :

- Sécurité de la connexion : utilisez le chiffrement si disponible
- Cochez la case Allow plaintext auth other unencryption flows.
- Port de connexion : 522. Utilisez le port par défaut 5222. Ce port est requis pour les clients XMPP externes. Les clients de bureau Finesse utilisent 7443. N'utilisez pas le port 7443.
- Serveur de connexion : FQDN du serveur Finesse

Modify Account						
Basic Advanced Proxy						
Connection security: Use encryption if available  Allow plaintext auth over unencrypted streams						
Connect port: 5222						
Connect server: fin1.ucce.local						
File transfer proxies:						
BOSH URL:						
Show Custom Smileys						
Create this new account on the server						
<u>C</u> ancel <u>S</u> ave						

**Remarque** : le port 5222 est utilisé uniquement parce que les clients Web Finesse peuvent utiliser le port 7443 pour se connecter au service de notification.

Étape 4. Accédez à **Outils > Plugins** et activez la console XMPP.



Étape 5. Accédez à **Outils > Console XMPP > Console XMPP** pour ouvrir la console XMPP.



Étape 6. Exécutez ce message **<iq>** pour voir tous les noeuds XMPP qui existent.

Exemple :



Dans un environnement de travaux pratiques avec deux agents et deux CSQ configurés, ce résultat est contenu dans la réponse Finesse :

# **Exemple 2 : Utiliser l'onglet Réseau des outils de développement de navigateur pour afficher les messages HTTP**

Chaque navigateur dispose d'un ensemble d'outils de développement. L'onglet Réseau des outils de développement affiche les messages HTTP envoyés et reçus par le client Web Finesse (navigateur). Par exemple, cette image montre comment le client Web Finesse envoie une requête SystemInfo qui vérifie l'état de Finesse Tomcat toutes les minutes en tant que vérification de basculement. En outre, les messages httpbind de la connexion BOSH sont également affichés. Le serveur Finesse renvoie une réponse dans les 30 secondes s'il n'y a aucune mise à jour à publier sur les noeuds XMPP auxquels le client Web est abonné.

C		Inspector	Console Debugger { } Style Editor	@ Performance D Memory	📄 🗁 Network			
Ĩ	All B	HTML	CSS JS XHR Fonts Images Media Flash	WS Other				@ 178
1	Status	Method	File	Domain	Cause	Type Transfe	r Size	0 ms
•	200	POST	/http-bind/	AX.XX.XX.XX :7443	🖾 xhr	xml 57 B	57 B	-
•	200	GET	SystemInfo?timestamponly&nocache=1492185680998	A xx.xx.xx 8445	🖾 xhr	xml 166 E	3 166 B	
•	200	POST	/http-bind/	AXX.XX.XX.XX :7443	🖾 xhr	xml 57 B	57 B	
•	200	POST	/http-bind/	AXXXXXXXXXX :7443	🖾 xhr	xml 57 B	57 B	
•	200	GET	SystemInfo?timestamponly&nocache=1492185741004	AXX.XX.XX.XX :8445	🖾 xhr	xml 166 E	3 166 B	
•	200	POST	/http-bind/	AXX.XX.XX.XX :7443	🖾 xhr	xml 57 B	57 B	
•	200	POST	/http-bind/	AXXXXXXXXX :7443	🖾 xhr	xml 57 B	57 B	
•	200	GET	SystemInfo?timestamponly&nocache=1492185801004	A XX.XX.XX.XX :8445	🖾 xhr	xml 166 E	3 166 B	
•	200	POST	/http-bind/	AXX.XX.XX.XX :7443	🖾 xhr	xml 57 B	57 B	
•	200	POST	/http-bind/	AX.XX.XX.XX :7443	🖾 xhr	xml 57 B	57 B	
	200	GET	SystemInfo?timestamponly&nocache=1492185861006	AXX.XX.XX.XX 8445	🗊 xhr	xml 166 E	3 166 B	
	200	POST	/http-bind/	AX.XX.XX.XX :7443	🖾 xhr	xml 57 B	57 B	
•		POST	/http-bind/	XX.XX.XX.XX :7443	🖾 xhr			

# Dépannage du message d'erreur de déconnexion BOSH

Lorsqu'une déconnexion BOSH se produit, l'erreur Connexion perdue à {Finesse Server FQDN}. Veuillez attendre qu'un serveur Finesse accessible soit trouvé... s'affiche dans une bannière rouge en haut du bureau Finesse.

			Lost connection to	XXXX.XXXX.XXXX.cisco.com. Please wait for a reachable Finess
cisco	Agent 10010	<b>001 (1001001) - E</b> 05:16	xtension 1001001	
Home	My Statistics	Manage Customer		
L Re	ady for Inco	oming Calls		
Agent C	SQ Statistics	s Report	_	
Agent C	SQ Statistic	• 11		Thresholds only

Ce message s'affiche car aucun événement d'abonnement XMPP ne peut actuellement être reçu du service de notification Cisco Finesse. Par conséquent, les informations d'état et les détails d'appel ne peuvent pas être affichés sur le bureau de l'agent.

Pour UCCX, 60 secondes après la déconnexion du navigateur, l'agent passe à l'état Déconnexion. L'agent peut être à l'état Prêt ou Non prêt pour que la déconnexion se produise.

Pour UCCE, Finesse prend jusqu'à 120 secondes pour détecter quand un agent ferme le navigateur ou que le navigateur tombe en panne et Finesse attend 60 secondes avant d'envoyer une demande de déconnexion forcée au serveur CTI, ce qui amène le serveur CTI à mettre l'agent dans un état Non prêt. Dans ces conditions, Finesse peut prendre jusqu'à 180 secondes pour déconnecter l'agent. Contrairement à UCCX, l'agent passe à l'état Non prêt au lieu de l'état Déconnexion.

**Remarque** : la déconnexion CTI n'est pas prête et Le comportement de l'état de déconnexion dans UCCE est contrôlé par le paramètre PG /LOAD. Selon les Notes de version de Unified Contact Center Enterprise et Hosted version 10.0(1), le paramètre /LOAD est déconseillé à partir de UCCE 10.0.

Pour plus d'informations sur le comportement d'UCCE Finesse Desktop, reportez-vous à la section Desktop Behavior du chapitre Cisco Finesse Failover Mechanisms du <u>Guide d'administration de Cisco Finesse</u>.

Remarque : les valeurs du minuteur peuvent changer à l'avenir selon les exigences du produit.

#### Analyse des journaux

Les journaux de service de notification Finesse et UCCX peuvent être collectés via RTMT ou via l'interface de ligne de commande :

fichier get activelog /desktop recurs compress

#### Journaux du service de notification de débogage

**Remarque** : définissez les journaux de niveau de débogage uniquement lorsque vous reproduisez un problème. Désactivez les débogages une fois le problème reproduit.

**Remarque** : Finesse 9.0(1) n'a pas de journalisation de niveau de débogage. La journalisation au niveau du débogage a été introduite dans Finesse 9.1(1). Le processus d'activation de la journalisation est différent dans 9.1(1) par rapport à Finesse 10.0(1) - 11.6(1). Pour ce processus, consultez le guide Finesse Administration and Serviceability.

Activez les journaux de débogage du service de notification de Unified Contact Center Express (UCCX), comme indiqué :

<#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.

Activez les journaux de débogage du service de notification de Unified Contact Center Enterprise (UCCE) (autonome Finesse), comme indiqué :

<#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

Ces journaux se trouvent dans le dossier /desktop/logs/openfire et sont nommés debug.log.

Comme l'illustre l'image, le fichier debug.log du service de notification (Openfire) affiche la liaison http avec le bureau, ainsi que l'adresse IP et le port du PC agent.

XXX.XXX.XXX.XX!1:34:21 [Session-1, SSL\_NULL\_WITH\_NULL\_NULL] received 0 sent 0 2017.04.14 21:34:21 REQUEST /http-bind/ on org.eclipse.jetty.server.nio.SelectChannelConnector\$SelectChannelHttpConnection@2dta26@XXX.XXX 2017.04.14 21:34:21 scope null|//http-bind/ @ o.e.j.s.ServletContextHandler{/http-bind,null} 2017.04.14 21:34:21 context=/http-bind||/ @ o.e.j.s.ServletContextHandler{/http-bind,null} 2017.04.14 21:34:21 sessionManager=org.eclipse.jetty.server.session.HashSessionManager@176fe4#STARTED 2017.04.14 21:34:21 session=null 2017.04.14 21:34:21 session=null 2017.04.14 21:34:21 servlet /http-bind|// -> org.jivesoftware.openfire.http.HttpBindServlet-1643193 2017.04.14 21:34:21 chain=null 2017.04.14 21:34:21 HTTPBindLog: HTTP RECV(3445afbe): <> body sid="3445afbe" rid="164053266"/> ttp HttpSession@dd7653\_status: 3 address: 1001003@xxx.xxxx.xxx.xxx.xxx.xx.cisco 2017.04.14 21:34:21 consumeResponse: org. jivesoftware.open <c xmlns="http://jabber.org/protocol/caps" hash="sha-1" node="http://jabber.cisco.com/caxl" ver="VNC6fNwvCxe6FJfDJIpLryVJRwM="/> </presence> rid: 164053266 2017.04.14 21:34:21 suspended org.eclipse.jetty.server.nio.SelectChannelConnector\$SelectChannelHttpConnection@2d5azb@ xxx.xxx.xxx:7443<-> 2017.04.14 21:34:24 Launching thread for /127.0.0.1:44667 2017.04.14 21:34:24 Launching thread for /127.0.0.1:44656

Comme lâ€<sup>™</sup>illustre lâ€<sup>™</sup>image, la dernière durée active de 0 ms indique que la session est toujours active.

Openfire fermant la session inactive indique que la déconnexion de l'agent peut se déclencher en 60 secondes, où Finesse peut envoyer une déconnexion forcée avec un code de raison de 255 au serveur CTI. Le comportement réel du bureau dans ces conditions dépend du paramètre de déconnexion lors de la déconnexion de l'agent (LOAD) dans UCCE. Dans UCCX, c'est toujours le comportement.

Si le client Finesse n'envoie pas de messages http-bind au serveur Finesse, les journaux peuvent afficher le temps de fonctionnement de la session et indiquer la fermeture de la session.

2017.06.17 00:14:34 Session (id=f382a015) was last active 0 ms ago: 1001003@xxxxx.xxxx.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.cisco.com

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

Journaux du service de notification Info

Ces journaux se trouvent dans le dossier /desktop/logs/openfire et sont nommés info.log. Si le client Finesse n'envoie pas de messages http-bind au serveur Finesse, les journaux peuvent indiquer que la session est devenue inactive.

2017.06.17 00:16:04 Closing idle session (id=f382a015): 1001003@xxxxx.xxxx.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.cisco.com/desktop

#### Journaux des services Web

Ces journaux se trouvent dans le dossier /desktop/logs/webservices et sont nommés Desktopwebservices.YYY-MM-DDTHH-MM-SS.sss.log. Si le client Finesse n'envoie pas de messages http-bind au serveur Finesse dans le délai spécifié, les journaux peuvent afficher l'état d'indisponibilité de la présence de l'agent et, 60 secondes plus tard, une déconnexion pilotée par la présence peut se produire.

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-UNSUBSCR 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\_MONIT( 0000001060: XX.XX.XX.XXX:: Jun 17 2017 00:17:04.632 +0530: %CCBU\_CoreImpl-worker12-6-PRESENCE DRIVEN LOC 0000001061: XX.XX.XX.XXX:: Jun 17 2017 00:17:04.633 +0530: %CCBU\_CoreImpl-worker12-6-MESSAGE\_TO\_CTI\_SERN 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\_MI skillGroupNumber=-1, skillGroupPriority=0, agentState=1 (LOGOUT), eventReasonCode=255, numFltSkillGroupPr duration=null, nextAgentState=null, fltSkillGroupNumberList=[], fltSkillGroupIDList=[], fltSkillGroupPr msgID=30, timeTracker={"id":"AgentStateEvent","CTI\_MSG\_RECEIVED":1497638824642,"CTI\_MSG\_DISPATCH":149763 Decoded Message to Finesse from backend cti server

### Raisons courantes de la déconnexion BOSH

Les connexions BOSH sont configurées par le client Web et le serveur Finesse détermine si la présence de l'agent n'est pas disponible. Ces problèmes sont presque toujours des problèmes côté client liés au navigateur, à l'ordinateur de l'agent ou au réseau, car la responsabilité du démarrage de la connexion incombe au client.

### Problème - Déconnexion des agents à différents moments (problème côté client)

#### Actions recommandées

Recherchez les problèmes suivants :

- 1. Problème réseau :
  - Examiner les règles et les journaux du pare-feu : le port TCP 7443 ne doit pas être bloqué ou limité
  - Utilisez un analyseur de trafic Web HTTP tel que <u>Fiddler<sup>®</sup></u> ou <u>Wireshark<sup>®</sup></u> pour confirmer que le navigateur envoie des requêtes http-bind sur le port TCP 7443 et reçoit des réponses
  - Vérifier tous les périphériques/interfaces réseau entre l'ordinateur de l'agent et le serveur Finesse pour

détecter tout retard excessif ou toute perte de paquets

- La commande traceroute peut être utile pour déterminer le chemin et les délais
  - Sur un PC Microsoft<sup>®</sup> Windows<sup>®</sup> : tracert {Finesse Server IP | Nom de domaine complet du serveur Finesse}
  - Sur un Mac<sup>®</sup> : traceroute {Finesse Server IP | Nom de domaine complet du serveur Finesse}
  - Sur le logiciel Cisco IOS<sup>®</sup>, les statistiques d'interface peuvent être vérifiées : show interfaces
    - Référez-vous Dépannage des pertes de file d'attente en entrée et de sortie
- Collecter les journaux du client Finesse pour un agent de test. Les journaux clients peuvent être collectés de trois manières :
  - 1. Journaux de console Web du navigateur
    - Console Web Firefox
    - <u>Console Web Microsoft Edge</u>
    - Console Web Chrome
  - 2. Appuyez sur le bouton <u>Send Error Report</u> sur la page Finesse et collectez les journaux du serveur Finesse. Les journaux se trouvent dans /desktop/logs/clientlogs.
  - 3. Connectez-vous via https://<Finesse-FQDN>/desktop/locallog et collectez les journaux après le problème.

Chaque minute, le client se connecte au serveur Finesse pour calculer la dérive et la latence du réseau :

<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

En cas de problèmes de collecte de journaux, référez-vous à <u>Dépannage du problème de journalisation</u> persistante de <u>Cisco Finesse Desktop</u>

2. Navigateur et/ou version non pris en charge :

Utiliser le navigateur/la version et les paramètres pris en charge conformément aux matrices de compatibilité :

Matrice de compatibilité UCCE

Matrice de compatibilité UCCX

3. État de blocage du navigateur en raison du contenu/traitement d'un autre onglet/fenêtre :

Vérifiez le workflow de l'agent pour voir s'il :

- Ont généralement d'autres onglets ou fenêtres en cours d'exécution qui exécutent constamment d'autres applications en temps réel telles que la musique/vidéo en continu, les connexions WebSocket, les clients Web personnalisés de gestion de la relation client (CRM), etc
- Ouvrir un très grand nombre d'onglets ou de fenêtres
- Ont désactivé la mise en cache du navigateur
- ont maintenu leur navigateur en fonctionnement pendant une longue période et ne ferment pas le navigateur à la fin de la journée de travail

4. Ordinateur mis en veille :

Vérifiez si l'agent met son ordinateur en veille avant de se déconnecter de Finesse ou si le minuteur de mise en veille de son ordinateur est très bas.

5. Problème de CPU élevé ou de mémoire élevée sur l'ordinateur client :

- Si le navigateur de l'agent s'exécute dans un environnement partagé tel que Microsoft Windows Remote Desktop Services, Citrix<sup>®</sup> XenApp<sup>®</sup>, Citrix XenDesktop<sup>®</sup>, déterminez si les performances du navigateur dépendent du nombre d'utilisateurs exécutant le navigateur en même temps
  - Assurez-vous que la mémoire et les ressources processeur appropriées sont configurées en fonction du nombre d'utilisateurs
- Vérifier les problèmes d'utilisation des ressources informatiques :
  - Fenêtres:
    - Commande Windows <u>PowerShell Get-Counter</u> qui vérifie le % de temps processeur, le mégaoctet de mémoire disponible et le % de mémoire utilisée toutes les 2 secondes : Get-Counter -Counter "\Processor(\_Total)\% Processor Time","\Memory\Available MBytes","\Memory\% Committed Bytes In Use" -SampleInterval 2 -Continuous
    - Au lieu d'utiliser PowerShell pour afficher les compteurs de performance de Windows, <u>Windows Performance Monitor</u> peut être utilisé
    - <u>Le Gestionnaire des tâches</u> peut être utilisé pour afficher les statistiques de CPU et de mémoire en direct globalement et processus par processus
  - Mac :
    - Commande Terminal Top qui vérifie le CPU total et la mémoire en direct : top
      - Vérifier les processus et trier par utilisation du CPU : top -o CPU
      - Vérifier les processus et trier par utilisation de la mémoire : top -o MEM
    - <u>Activity Monitor</u> peut être utilisé pour afficher les statistiques de CPU et de mémoire en direct globalement et processus par processus
- 6. Gadgets tiers effectuant une activité inattendue et problématique en arrière-plan :

Testez le comportement du bureau Finesse en supprimant tous les gadgets tiers.

- 7. Problème NTP sur le serveur ou le client :
  - Vérifiez l'**état ntp utils** sur le serveur de publication Finesse pour vous assurer que la strate de serveur NTP est 4 ou inférieure
  - Dans les journaux du client, vérifiez la dérive et la latence du réseau

## Problème : tous les agents se déconnectent simultanément (problème côté serveur)

#### Actions recommandées

Recherchez les problèmes suivants :

1. Déconnexion du service Cisco Unified Communications Manager CTIManager. Si tous les fournisseurs CTIManager pour UCCX sont arrêtés ou se bloquent, les agents UCCX voient l'erreur de bannière rouge. Les agents UCCE ne voient pas la bannière rouge si cela se produit, mais les appels ne parviennent pas à être acheminés correctement vers les agents.

- Vérifiez si le service Cisco TIManager est démarré sur les serveurs CUCM utilisés comme fournisseurs CTI
- Vérifiez si le service Cisco CTIManager s'est bloqué via l'Observateur d'événements L'application se

connecte à RTMT pour voir si le service Cisco CTIManager s'est bloqué

Pour collecter les journaux de l'Observateur d'événements sur RTMT, accédez à Système > Outils > Trace et Log Central > Collecter les fichiers > Sélectionner les services/applications du système > Journal des applications de l'Observateur d'événements.

System	Trace & Log Central				
stem Summary	Trace & Log Central Remote Browse	Collect Files			<b>x</b>
erver	Collect Files Ouery Wilcard Othership Collector	Select System Services/Applications	all Services on all Serve	19.	
Process	- Local Browse	in the second		C dat uses have	
	C Real Time Trace	PARTIE AND A DESCRIPTION AND	All pervers	L BRITISCOR FOCAR	U
Disk Usage	D cuted Crash Dura	Class Listed Basedies Wat Salara	- H	H	-
Collinal Services	Renearchanter	Ciana Lines Calls Resident	- H	H	
	Coned water Logs	Cisco Coler Data periodes	<u> </u>	8	-
- Contractor	Audit Logs	Class Bud Call State and State and State	- H	<u> </u>	
Performance		Case Later	H	<u> </u>	-
Participance I on Viewer		Cron Loga			-
Land and the state		Event viewer-Application Log			
		Event viewer-oldsern Fog		<u> </u>	-
Alet Central		PPG Logs	X	<u> </u>	
Trace & Lon Certral		Prost Resources Agent			-
		PT Platorm CLI Created Reports			
Job Status		IPT Platorin CLI Loga		<u> </u>	-
Rost on Viewer		IPT Platorm Cerl Monitor Logs			-
a since a second		IPT Platorm Certiligr Logs			
- VLT		IPT Platorin Cluster Manager Logs			-
Audit on Viewer		IPT Platorm GUI Logs			
Concess interest		IPT Platform IPSecMgmt Logs			
		IPT Platform RemoteDupportLogs			
		Install File Signing			
		Install and Upgrade Logs	0		
		Kamaldump Logs			
		M02 Agent			
		Mail Logs			
		Mgetty Logs			
		NTP Logs	0	0	
		Packet Capture Logs			
		Buss Land			

- Pour collecter les journaux d'application de l'Observateur d'événements sur l'interface de ligne de commande : fichier get activelog /syslog/CiscoSyslog\* abstime hh:mm:MM/DD/YY hh:mm:MM/DD/YY
- Pour afficher les vidages principaux sur l'interface de ligne de commande : utilise la liste active principale

**Remarque** : les noms de fichier des vidages principaux utilisent le format : core.<ProcessID>.<SignalNumber>.<ProcessName>.<EpochTime>. Exemple : core.24587.6.CTIManager.1533441238 Par conséquent, l'heure de l'accident peut être déterminée à partir de l'heure de l'époque.

- 2. Arrêt ou blocage du service de notification Finesse/UCCX :
  - Recherchez les erreurs du service de notification dans les journaux d'application de l'Observateur d'événements ou vérifiez si le service a été arrêté
  - Vérifiez si le service de notification est activé : utils service list
  - Vérifiez les heures d'arrêt du service de notification : file search activelog /desktop/logs/openfire "Openfire arrêté"
  - Vérifiez les heures de démarrage du service de notification : file search activelog /desktop/logs/openfire "HTTP bind service started"
  - Recherchez les vidages de mémoire du service de notification résultant d'une panne : file list activelog /desktop/logs/openfire/\*.hprof
  - Vérifiez si le service de notification écoute le trafic sur le port TCP 7443 : show open ports regexp 7443.\*LISTEN
  - Vérifiez si ces défauts sont applicables (ces défauts provoqueraient un échec de connexion pour les agents qui se connectent et pour les agents déjà connectés, ces agents verraient le message de déconnexion Finesse de la bannière rouge) :
    - ID de bogue Cisco <u>CSCva7280</u> Tomcat Finesse et crash d'Openfire pour caractères XML non valides
    - ID de bogue Cisco <u>CSCva72325</u> UCCX : Finesse Tomcat et Openfire Crash pour caractères XML non valides

Redémarrez Cisco Finesse Tomcat et le service de notification si vous suspectez une panne. Ceci n'est recommandé que dans une situation de réseau en panne, sinon, ces redémarres déconnectent les agents du serveur Finesse.

Étapes pour UCCE :

- utils service stop Cisco Finesse Tomcat
- utils service stop Service de notification Cisco Finesse
- utils service start Cisco Finesse Tomcat
- utils service start Service de notification Cisco Finesse

Étapes pour UCCX :

- utils service stop Cisco Finesse Tomcat
- utils service stop Service de notification Cisco Unified CCX
- utils service start Cisco Finesse Tomcat
- utils service start Service de notification Cisco Unified CCX

# **Utiliser Fiddler**

La configuration de Fiddler peut être une tâche assez difficile sans comprendre les étapes nécessaires et le fonctionnement de Fiddler. Fiddler est un proxy web man-in-the-middle qui se trouve entre le client Finesse (navigateur web) et le serveur Finesse. En raison des connexions sécurisées entre le client Finesse et le serveur Finesse, cela ajoute une couche de complexité à la configuration de Fiddler afin de visualiser les messages sécurisés.

### Émission De Violon Commun

Fiddler se trouvant entre le client Finesse et le serveur Finesse, l'application Fiddler doit créer des certificats signés pour tous les ports TCP Finesse qui nécessitent des certificats :

Certificats de service Cisco Finesse Tomcat

- 1. Serveur d'édition Finesse TCP 8445 (et/ou 443 pour UCCE)
- 2. Serveur d'abonnés Finesse TCP 8445 (et/ou 443 pour UCCE)

Certificats du service de notification Cisco Finesse (Unified CCX)

- 1. Serveur d'édition Finesse TCP 7443
- 2. Serveur d'abonnés Finesse TCP 7443

Le déchiffrement HTTPS doit être activé pour que Fiddler puisse générer dynamiquement des certificats pour le compte du serveur Finesse. Cette option n'est pas activée par défaut.

Si le déchiffrement HTTPS n'est pas configuré, la connexion initiale du tunnel au service de notification est visible, mais le trafic http-bind ne l'est pas. Fiddler ne montre que :

Tunnel to <Finesse server FQDN>:7443

File	Edit R	ules Tools	View Help	GET /book	C GeoEd	ige				
<b>Q</b> fy	Replay	X · > Go	🔹 💺 Stream	🐞 Decode	Keep: All	sessio	ns • 🕀	Any Process	🐴 Find	😹 Save
*	Result	Prot	Host	URL		Body	Cachi	Content	Process	Comments
<u>61</u>	200	HTTP	Tunnel to	fin1.ucce.local:8	3445	0			firefo	
<u>m</u> 2	200	HTTP	Tunnel to	fin1.ucce.local:8	3445	0			firefo	
<u>m</u> 3	200	HTTP	Tunnel to	fin1.ucce.local:8	3445	0			firefo	
<u>64</u>	200	HTTP	Tunnel to	fin1.ucce.local:8	3445	0			firefo	
ô 5	200	HTTP	Tunnel to	fin1.ucce.local:8	3445	0			firefo	
m 6	200	HTTP	Tunnel to	fin1.ucce.local:8	3445	0			firefo	
07	200	HTTP	Tunnel to	fin1.ucce.local;7	443	0			frefo	

Ensuite, les certificats Finesse signés par Fiddler doivent être approuvés par le client. Si ces certificats ne sont pas approuvés, il est impossible de passer l'étape Établissement d'une connexion chiffrée... de la connexion Finesse.

Establishing encrypted connection

Dans certains cas, l'acceptation des exceptions de certificat à partir de la connexion ne fonctionne pas, et les certificats doivent être approuvés manuellement par le navigateur.

#### Exemple d'étapes de configuration

Attention : l'exemple de configuration fourni concerne Fiddler v5.0.20182.28034 pour .NET 4.5 et Mozilla Firefox 64.0.2 (32 bits) sous Windows 7 x64 dans un environnement de travaux pratiques. Ces procédures ne peuvent pas être généralisées à toutes les versions de Fiddler, à tous les navigateurs ou à tous les systèmes d'exploitation des ordinateurs. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute configuration. Consultez la <u>documentation officielle de Fiddler</u> pour plus d'informations.

Étape 1. Télécharger Fiddler

Étape 2. Activez le déchiffrement HTTPS. Accédez à **Tools > Options > HTTPS** et cochez la case **Decrypt HTTPS traffic**.

Options	
General HTTPS Connections Gateway Appearance Scripting Extensions Performance Tools	
Fiddler can decrypt HTTPS sessions by re-signing traffic using self-generated certificates.	
Capture HTTPS CONNECTS	Actions
✓ Decrypt HTTPS traffic	
from all processes   Certificates generated by CertEnroll engine	
Ignore server certificate errors (unsafe)	
Check for certificate revocation	
Protocols: <client>; ssl3;tls1.0</client>	
Skip decryption for the following hosts:	
Help         Note: Changes may not take effect until Fiddler is restarted.         OK	Cancel

Étape 3. Un message d'avertissement s'affiche pour demander l'approbation du certificat racine Fiddler. Sélectionnez **Oui**.

Étape 4. Un message d'avertissement s'affiche avec le message « Vous êtes sur le point d'installer un certificat d'une autorité de certification (AC) prétendant représenter : DO\_NOT\_TRUST\_FiddlerRoot... Voulez-vous installer ce certificat ?". Sélectionnez **Oui**.

Étape 5. Ajoutez manuellement les certificats d'éditeur et d'abonné Finesse au magasin de certificats de confiance de l'ordinateur ou du navigateur. Assurez-vous que les ports 8445, 7443 et (uniquement pour UCCE) 443. Par exemple, sur Firefox, cela peut être fait simplement sans télécharger de certificats à partir de la page Finesse Operating System Administration :

**Options > Find in Options** (search) **> Certificates > Servers > Add Exception > Location >** Enter https://<Finesse server>:port for the relevant ports for both Finesse servers.



Étape 6. Connectez-vous à Finesse et voyez les messages http-bind qui laissent le client Finesse au serveur Finesse via Fiddler.

Dans l'exemple fourni, les 5 premiers messages affichent des messages http-bind auxquels le serveur Finesse a répondu. Le premier message contient 1 571 octets de données renvoyées dans le corps du message. Le corps contient une mise à jour XMPP concernant un événement d'agent. Le dernier message http-bind a été envoyé par le client Finesse, mais n'a pas reçu de réponse du serveur Finesse. Cela peut être déterminé lorsque vous voyez que le résultat HTTP est nul (-) et que le nombre d'octets dans le corps de la réponse est nul (-1).

15.	0	V 1	C	III Donald Lat		0	4	44.00	El c	68 \land 🕫	Active the manual transmission
?* <del>*</del>	Replay	X . )	Go 👎 Stream	Decode Keep: A	All sessio	ons • 🕀	Any Process	Find Find	Save	lio (2) 🌮	Browse · 🛠 Clear Cache 🔏 TextWizard 🛃 Tearoff
	Result	Prot	Host	URL	Body	Cachi	Content	Process	Comments	Custo *	⑦ Statistics SK Inspectors
g6	200	HTTPS	fin1.ucce.local:	/desktop/thirdparty/	1,135		text/java	firefo			Headers TextView SyntaxView WebForms HexV
g6	200	HTTPS	fin1.ucce.local:	/desktop/thirdparty/	1,655		text/java	firefo			POST <u>https://fin1.ucce.local:7443/http-bind/</u> Host: fin1.ucce.local:7443
g6	200	HTTPS	fin1.ucce.local:	/desktop/thirdparty/	3,579		text/java	firefo			User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64
§6	200	HTTPS	fin1.ucce.local:	/desktop/thirdparty/	4,744		text/java	firefo			Accept: text/plain, */*; q=0.01 Accept-Language: en-US.en:g=0.5
§6	200	HITPS	fin1.ucce.locat	/desktop/thirdparty/	1,630		text/java	firefo			Accept-Encoding: gzip, deflate, br
6	200	HITPS	fin1.ucce.local:	/desktop/thirdparty/	812		text/ntmi	firefo			Content-Type: text/xml
6	200	HITPS	fin1.ucce.local:	/desktop/thirdparty/	729		text/ntmi	firefo			X-Requested-With: XMLHttpRequest
6	200	HITPS	Influcce.ocac	/desktop/thirdparty/	352		text/ntmi	firefo			Content-Length: 83 Cookie: finesse_ag_extension=10005: JSESSIONIO
6	200	HITP	detectportal.fre	/success.txt	8	no-ca	text/pian	firefo			Connection: keep-alive
· 0	200	HITPS	fin1.ucce.iocat	/desktop/thirdparty/	244		text/ntmi	firefo			Cache-Control: no-cache
· 0	200	HITPS	fin1.ucce.iocat	/desktop/thirdparty/	/31		text/ntmi	firefo			
6	200	HITPS	fin1.ucce.local:	/desktop/thirdparty/	901		text/ntmi	firefo			<body 47483648@fin1.ucce.local"="" http:="" id="/finesse/api/User/4748&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;· 0&lt;/td&gt;&lt;td&gt;200&lt;/td&gt;&lt;td&gt;HITPS&lt;/td&gt;&lt;td&gt;In1.ucce.local:&lt;/td&gt;&lt;td&gt;/desktop/cscowidge&lt;/td&gt;&lt;td&gt;1,176&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;text/ntmi&lt;/td&gt;&lt;td&gt;firefo&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;pmIns=" jabber.org="" protocol="" pubsub#event"="" xmlns="http://jabber.org/protocol/httpb&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;6&lt;/td&gt;&lt;td&gt;200&lt;/td&gt;&lt;td&gt;HITPS&lt;/td&gt;&lt;td&gt;fin1.ucce.local&lt;/td&gt;&lt;td&gt;/desktop/thirdparty/&lt;/td&gt;&lt;td&gt;1,302&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;text/ntmi&lt;/td&gt;&lt;td&gt;firefo&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;· 6&lt;/td&gt;&lt;td&gt;200&lt;/td&gt;&lt;td&gt;HTTPS&lt;/td&gt;&lt;td&gt;fin1.ucce.iocai:&lt;/td&gt;&lt;td&gt;/desktop/thirdparty/&lt;/td&gt;&lt;td&gt;307&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;text/ntmi&lt;/td&gt;&lt;td&gt;firefo&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;End /mars Chris Enter to hisblaht all&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;· 6&lt;/td&gt;&lt;td&gt;200&lt;/td&gt;&lt;td&gt;HTTPS&lt;/td&gt;&lt;td&gt;fin1.ucce.iocat&lt;/td&gt;&lt;td&gt;/desktop/thirdparty/&lt;/td&gt;&lt;td&gt;287&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;text/ntmi&lt;/td&gt;&lt;td&gt;firefo&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;Find (press currenter to highlight al)&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;· 0&lt;/td&gt;&lt;td&gt;200&lt;/td&gt;&lt;td&gt;HITPS&lt;/td&gt;&lt;td&gt;fin1.ucce.iocat&lt;/td&gt;&lt;td&gt;/desktop/thirdparty/&lt;/td&gt;&lt;td&gt;569&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;text/ntmi&lt;/td&gt;&lt;td&gt;firefo&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;Transformer Headers TextView SyntaxView Imag&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;6&lt;/td&gt;&lt;td&gt;200&lt;/td&gt;&lt;td&gt;HTTPS&lt;/td&gt;&lt;td&gt;fin1.ucce.local:&lt;/td&gt;&lt;td&gt;/desktop/thirdparty/&lt;/td&gt;&lt;td&gt;910&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;text/html&lt;/td&gt;&lt;td&gt;firefo&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;Raw JSON XML&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;6&lt;/td&gt;&lt;td&gt;200&lt;/td&gt;&lt;td&gt;HTTP&lt;/td&gt;&lt;td&gt;detectportal.fre&lt;/td&gt;&lt;td&gt;/success.txt&lt;/td&gt;&lt;td&gt;8&lt;/td&gt;&lt;td&gt;no-ca&lt;/td&gt;&lt;td&gt;text/plan&lt;/td&gt;&lt;td&gt;firefo&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;Sody xmlns='http://jabber.org/protocol/httpbind'&gt;&lt;message&lt;/p&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;6&lt;/td&gt;&lt;td&gt;200&lt;/td&gt;&lt;td&gt;HTTPS&lt;/td&gt;&lt;td&gt;fin1.ucce.local&lt;/td&gt;&lt;td&gt;/desktop/thirdparty/&lt;/td&gt;&lt;td&gt;43&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;mage/gr&lt;/td&gt;&lt;td&gt;firefo&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;to="><items n<br="">4752-9a1d-5adbdac74a7717"&gt;</items></body>
6	200	HTTPS	fin1.ucce.local:	/desktop/theme/fine	673		image/gr	tirefo			Sit data&ot:
· 6	200	HITPS	fin1.ucce.iocat	/desktop/cscowidge	/20		text/ntmi	firefo			<user></user>
6	200	HITPS	fin1.ucce.iocat	/finesse/api/User/4/	631	no-ca	appicatio	firefo			<dialogs>/finesse/api/User/47483648/Dialogs<!--</td--></dialogs>
b	200	HITPS	fin1.ucce.iocat	/desktop/thirdparty/	12,/		mage/png	firefo			⁢extension>10005⁢/extension>
0	200	HITPS	fin1.ucce.iocat	/desktop/theme/me	2,205		mage/png	nrero		$\int$	Sit lastName&at:Newton⁢/lastName&at:
6	200	HITPS	fin1.ucce.iocac	/finesse/ap/User/4/	340	no-ca	appicatio	firefo			<loginid>47483648</loginid>
6	200	HITPS	fin1.ucce.iocac	/inesse/ap/User/4/	1,851	no-ca	appicatio	frefo		/	<loginname>isaac</loginname>
0	200	HITPS	fin1.ucce.local	/messe/ap/User/4/	20	no-ca	appicatio	firefo			<mediatype>1</mediatype>
0	200	HITTO	Turnel to	/gaugets/makekequ	340	no-ca	appicauo	firefo	/		äit,pendingstateagt,ait,/pendingstateagt, ält:rolesäat:
0	200	NTTRE	fort uses local	(and ants/makeDeau	240	00.03	appleatio	frefo			<role>Agent</role>
6	200	HTTP	detectnortal fra	/gaugets/maxekequ	340	10°Cd	dppicduo	frefo			
0	200	HITP	detectportal.ire	/success.txt	8	no-ca	text/pan	frefo			⁢settings>
6	200	HTTP	detectmontal fire	Culc1.0cce.0cd.o+++		00.03	toxt/obio	firefo	1		alt,wapoponincomingagt,or nonecalt,wapoponi alt/settingsagt
6	200	HTTPS	felt ucce local:	/success.ck	1 5 7 1	110°Cd	text/pair	firefo	r		<state>READY</state>
6	200	HTTPS	fin1.ucce.local:	/http://itu/	1,5/1	00-03	anoleatio	firefo			<statechangetime>2019-01-11T23:56:54.783Z8</statechangetime>
6	202	HTTPS	fin1.ucce.local	/deckton/theme/fine	673	110°0	image/of	firefo			⁢teamid>5000⁢/teamid>
6	200	HTTPS	fin1.ucce.local:	/bttp.bipd/	57		tovt/vml	firefo	<b>1</b> 1		alturiåat/finesse/api/User/47483648</uri&at
6	200	HTTPS	fin1 ucce local:	/finesse/ani/SystemI	232	no-ca	annicatio	firefo			
6	200	HTTPS	fin1 ucce local:	/http-hind/	57	no com	text/xml	firefo	1		
6	200	HTTPS	fin1.ucce.local:	/http-bind/	57		text/xml	firefo	1		⁢event>PUT⁢/event> ⁢requestid&at:07/14a42-6b3c-4855-a4c9-af50ab5c7c
16	200	HTTPS	fin1.ucce.local:	/finesse/ani/SystemI	232	no-ca	applicatio	firefo			air, requestidagi, 071144/2-005C-4655-84C8-8150805670 <:source&at:/finesse/api/User/47483648<:/source&at:
6	200	HTTPS	fin1.ucce.local	/http-bind/	57	Star Contra	text/xml	firefo	1		</Update>
6.	-	HTTPS	fin1.ucce.local	/http-bind/	-1		teny arrest	firefo	<b>i</b>	=	
6	200	HTTPS	fin1.ucce.local:	/finesse/api/SystemI	232	no-ca	applicatio	firefo			
										Ψ.	
				111						- F	h

Vue rapprochée des données :

-								
36	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
<b>2</b> 6	200	HTTPS	fin1.ucce.local:	/desktop/theme/fine	673		image/gif	firefo
36	200	HTTPS	fin1.ucce.local:	/http-bind/	57		text/xml	firefo
🔹 <b>6</b>	200	HTTPS	fin1.ucce.local:	/finesse/api/SystemI	232	no-ca	applicatio	firefo
36	200	HTTPS	fin1.ucce.local:	/http-bind/	57		text/xml	firefo
36	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
36	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

Corps de réponse pour le message XMPP :

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

## **Utiliser Wireshark**

Wireshark est un outil d'analyse de paquets couramment utilisé pour analyser et décoder le trafic HTTPS. Le trafic HTTPS est le trafic HTTP sécurisé sur TLS (Transport Layer Security). TLS assure l'intégrité, l'authentification et la confidentialité entre deux hôtes. Il est couramment utilisé dans les

applications Web, mais il peut être utilisé avec n'importe quel protocole qui utilise TCP comme protocole de couche transport. SSL (Secure Sockets Layer) est l'ancienne version du protocole TLS, qui n'est plus utilisé car il n'est pas sécurisé. Ces noms sont souvent utilisés de manière interchangeable, et le filtre Wireshark utilisé pour le trafic SSL ou TLS est ssl.

**Attention** : l'exemple de configuration fourni concerne Wireshark 2.6.6 (v2.6.6-0-gdf942cd8) et Mozilla Firefox 64.0.2 (32 bits) sous Windows7 x64 dans un environnement de travaux pratiques. Ces procédures ne peuvent pas être généralisées à toutes les versions de Fiddler, à tous les navigateurs ou à tous les systèmes d'exploitation des ordinateurs. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute configuration. Pour plus d'informations, consultez la documentation SSL officielle de Wireshark. Wireshark 1.6 ou version ultérieure est requis.

**Remarque** : cette méthode ne fonctionne que pour Firefox et Chrome. Cette méthode ne fonctionne pas pour Microsoft Edge.

Étape 1. Sur le PC Windows de l'agent, accédez à **Panneau de configuration > Système et sécurité > Système > Paramètres système avancés Variables environnementales...** 

🚱 🕞 💌 🦂 🕨 Control Panel 🕨 Sys	tem and Security   System
Control Panel Home	System Properties
😚 Device Manager	Computer Name Hardware Advanced System Protection Remote
😚 Remote settings	You must be logged on as an Administrator to make most of these changes.
System protection	Performance
Advanced system settings	Visual effects, processor scheduling, memory usage, and virtual memory
	Settings
	User Profiles
	Desktop settings related to your logon
	Settings
	Startup and Recovery
	System startup, system failure, and debugging information
	Settings
See also	
Action Center	Environment Variables
windows Update	
Tools	OK Cancel Apply

#### Étape 2. Accédez aux variables utilisateur pour l'utilisateur <username> > Nouveau...

Créez une variable nommée SSLKEYLOGFILE.

Créez un fichier pour stocker le secret de prémaître SSL dans un répertoire privé : SSLKEYLOGFILE=</path/to/private/directory/with/logfile>

Edit User Variable	×
Variable name:	SSLKEYLOGFILE
Variable value:	C:\Users\example\sslkeylog.log
	OK Cancel

**Remarque** : créez une variable système au lieu d'une variable utilisateur et/ou stockez le fichier dans un répertoire non privé, mais tous les utilisateurs du système peuvent accéder au secret prémaître, qui est moins sécurisé.

Étape 3. Si Firefox ou Chrome sont ouverts, fermez les applications. Une fois rouverts, ils peuvent commencer à écrire dans le fichier SSLKEYLOGFILE.

Étape 4. Sur Wireshark, accédez à Edit > Preferences...

📕 *Local	Area Connection					
File Edi	t View Go Capture Analy	ze Statistics T				
No.	Copy Find Packet Find Next Find Previous	, Ctrl+F Ctrl+N Ctrl+B				
	Mark/Unmark Packet Mark All Displayed Unmark All Displayed Next Mark Previous Mark	Ctrl+M Ctrl+Shift+M Ctrl+Alt+M Ctrl+Shift+N Ctrl+Shift+B				
	Ignore/Unignore Packet Ignore All Displayed Unignore All Displayed	Ctrl+D Ctrl+Shift+D Ctrl+Alt+D				
<ul> <li>F</li> <li>►</li> <li>►</li> <li>►</li> <li>►</li> <li>T</li> </ul>	Set/Unset Time Reference Unset All Time References Next Time Reference Previous Time Reference	Ctrl+T Ctrl+Alt+T Ctrl+Alt+N Ctrl+Alt+B				
⊳ T ⊿ S	Time Shift	Ctrl+Shift+T				
1	Packet Comment Delete All Packet Comments	Ctrl+Alt+C				
	Configuration Profiles Preferences	Ctrl+Shift+A Ctrl+Shift+P				

Accédez à **Protocoles > SSL**.

Columns Font and C	
Font and (	
i one ana s	ol
Layout	
Capture	
Expert	
Filter Buttons	1
Name Resolut	ior
Protocols	
104apci	
29West	
2dparityfe	с
3GPP2 A11	L
6LoWPAN	
802.11 Rad	dic
802.11 Rad	dic
9P	-
A-bis OML	Ψ.

Étape 5. Entrez l'emplacement du nom de fichier journal secret prémaître configuré à l'étape 2.

Wireshark · Preferences		^
SNA SNMP Snort Socks SolarEdge SoulSeek SoupBinTCP SPDY Spice SPRT SRVLOC SSCOP SSDP SSH SSL STANAG 506 STANAG 506 STANAG 506	Secure Sockets Layer RSA keys list Edit SSL debug file Reassemble SSL records spanning multiple TCP segments Reassemble SSL Application Data spanning multiple SSL records Message Authentication Code (MAC), ignore "mac failed" Pre-Shared-Key (Pre)-Master-Secret log filename C:\users\example\ssikeylog.log Browse	

Étape 6. Utilisez le filtre Wireshark **tcp.port==7443 && ssl**, la communication HTTP sécurisée entre le client Finesse et le serveur Finesse (Service de notification) est vue déchiffrée.

															_								
D Tra	Transmission Control Protocol, Src Port: 54979, Dst Port: 7443 Seq: 21265, Ack: 42841, Len: 56 Secure Sockets Laver													565									
- Sec	- Secure Suckets Layer																						
4	ILSv1.2 Record Layer: Application Data Protocol: Application Data																						
	Content Type: Application Data (23)																						
	Version: TLS 1.2 (0x0303)																						
	Length: 560																						
	Encrypted Application Data: 1e001ee88fc1c9a026b0385007608afdfb46c0d4a277faa8																						
	Encrypted Application Data: leooleessicic9a02000565007008arur040c004a277taa8																						
																			_				
0010	20	48	54	54	50	2f	31	2e	31	Ød	0a	48	6f	73	74	3a	HTTP/1.	1 - · Ho	ost:				
0020	20	66	69	6e	31	2e	75	63	63	65	2e	6c	6f	63	61	6c	fin1.uc	ce.lo	ocal				
0030	3a	37	34	34	33	0d	0a	55	73	65	72	2d	41	67	65	6e	:7443U	ser-A	Agen				
0040	74	3a	20	4d	6f	7a	69	6c	6c	61	2f	35	2e	30	20	28	t: Mozil	la/5.	.0 (				
0050	57	69	6e	64	6f	77	73	20	4e	54	20	36	2e	31	3b	20	Windows	NT 6.	.1;				
0060	57	4f	57	36	34	3b	20	72	76	3a	36	34	2e	30	29	20	WOW64; r	v:64.	.0)				
0070	47	65	63	6b	6f	2f	32	30	31	30	30	31	30	31	20	46	Gecko/20	10010	91 F				
0080	69	72	65	66	6f	78	2f	36	34	2e	30	Ød	0a	41	63	63	irefox/6	4.0-	Acc				
0090	65	70	74	3a	20	74	65	78	74	2f	70	6c	61	69	6e	2c	ept: tex	t/pla	ain.				
00a0	20	2a	2f	2a	3b	20	71	3d	30	2e	30	31	Ød	0a	41	63	*/*: a=	0.01	- Ac				
00b0	63	65	70	74	2d	4c	61	6e	67	75	61	67	65	3a	20	65	cept-Lan	guage	e: e				
00c0	6e	2d	55	53	20	65	6e	Зb	71	3d	30	2e	35	Ød	0a	41	n-US, en:	a=0.5	5 A				
0000		2.0			20			50		50	50				00		ii ooyeny	9-01.					
Frame	(619	byte	s)	De	crypt	ed S	SL (S	513 b	ytes)	1													
07	wire	ocha	rk Fr	56425	EDE-	1015	-411	5-826	4-851	5745	017	- 8 - 2	0100	1251	5540	6 3060	184 pcappo			11	Packete: 12	7485 • 0	icolau
wiresnark_coo42FDE-A01F-4115-82E4-85157A8917C8_20190125155406_a06084.pcapng											rackets, 12	/405 D	ispidy										

## Défauts associés

- ID de bogue Cisco <u>CSCva7280</u> Tomcat Finesse et crash d'Openfire pour caractères XML non valides
- ID de bogue Cisco <u>CSCva72325</u> UCCX : Finesse Tomcat et Openfire Crash pour caractères XML non valides

# **Informations connexes**

- Spécifications XMPP
- <u>XEP-0124 : BOSH</u>
- XEP-0060 : Publier-S'abonner
- <u>Console Web Firefox</u>
- <u>Console Web Microsoft Edge</u>
- <u>Console Web Chrome</u>
- <u>Windows PowerShell</u>
- <u>Analyseur de performances Windows</u>
- Dépannage des suppressions dans la file d'attente d'entrée et de sortie
- Gestionnaire des tâches Windows
- Terminal Mac
- Moniteur d'activité Mac
- <u>Téléchargement de Fiddler</u>
- <u>Configuration de violon</u>
- <u>Téléchargement Wireshark</u>
- <u>Décodage SSL Wireshark</u>
- <u>Assistance et documentation techniques Cisco Systems</u>

# À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.