Définition des suivis et collecte des journaux dans CCE

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Définition des suivis et collecte des journaux Finesse
  - Client Finesse
    - Option 1 : Collecter les journaux client via le rapport d'erreurs d'envoi
    - Option 2 : Définir la journalisation permanente
    - Option 3 : Console du navigateur Web
  - Serveur Finesse
    - Option 1 : Via l'interface utilisateur (UI) - Services Web (obligatoire) et journaux supplémentaires
    - Option 2 : Via SSH et SFTP (Secure File Transfer Protocol) - Option recommandée
- Définition des suivis et collecte des journaux CVP et CVVB
  - Serveur d'appels CVP
  - Application CVP Voice XML (VXML)
  - CVP Operations and Administration Management Portal (OAMP)
  - Navigateur vocal virtualisé Cisco (CVVB)
    - Option 1 : Via un compte d'administration
    - Option 2 : Via SSH et SFTP - Option recommandée
- Définition des journaux de suivi et de collecte pour CUBE et CUSP
  - CUBE (SIP)
  - CUSPIDE
    - Collecter les journaux
- Définition des journaux de suivi et de collecte UCCE
    - Définir le niveau de trace
    - Collecte des journaux
- Définition des journaux PCCE de suivi et de collecte
- Définition des journaux CUIC/Live Data/IDS de suivi et de collecte
  - Télécharger les journaux avec SSH
  - Télécharger les journaux avec RTMT
- Capture de paquets sur VoS (Finesse, CUIC, VVB)

Introduction

Ce document décrit comment définir et collecter des suivis dans Cisco Unified Contact Center Enterprise (CCE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Enterprise (UCCE)
- Package Contact Center Enterprise (PCCE)
- Cisco Finesse
- Portail vocal client Cisco (CVP)
- Navigateur vocal virtualisé Cisco (VVB)
- Cisco Unified Border Element (CUBE)
- Cisco Unified Intelligence Center (CUIC)
- Proxy Cisco Unified Session Initiation Protocol (SIP) (CUSP)

Composants utilisés

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

- Cisco Finesse version 12.5
- Serveur CVP version 12.5
- UCCE/PCCE version 12.5
- Cisco VVB version 12.5
- CUIC version 12.5

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 l’incidence possible des commandes.

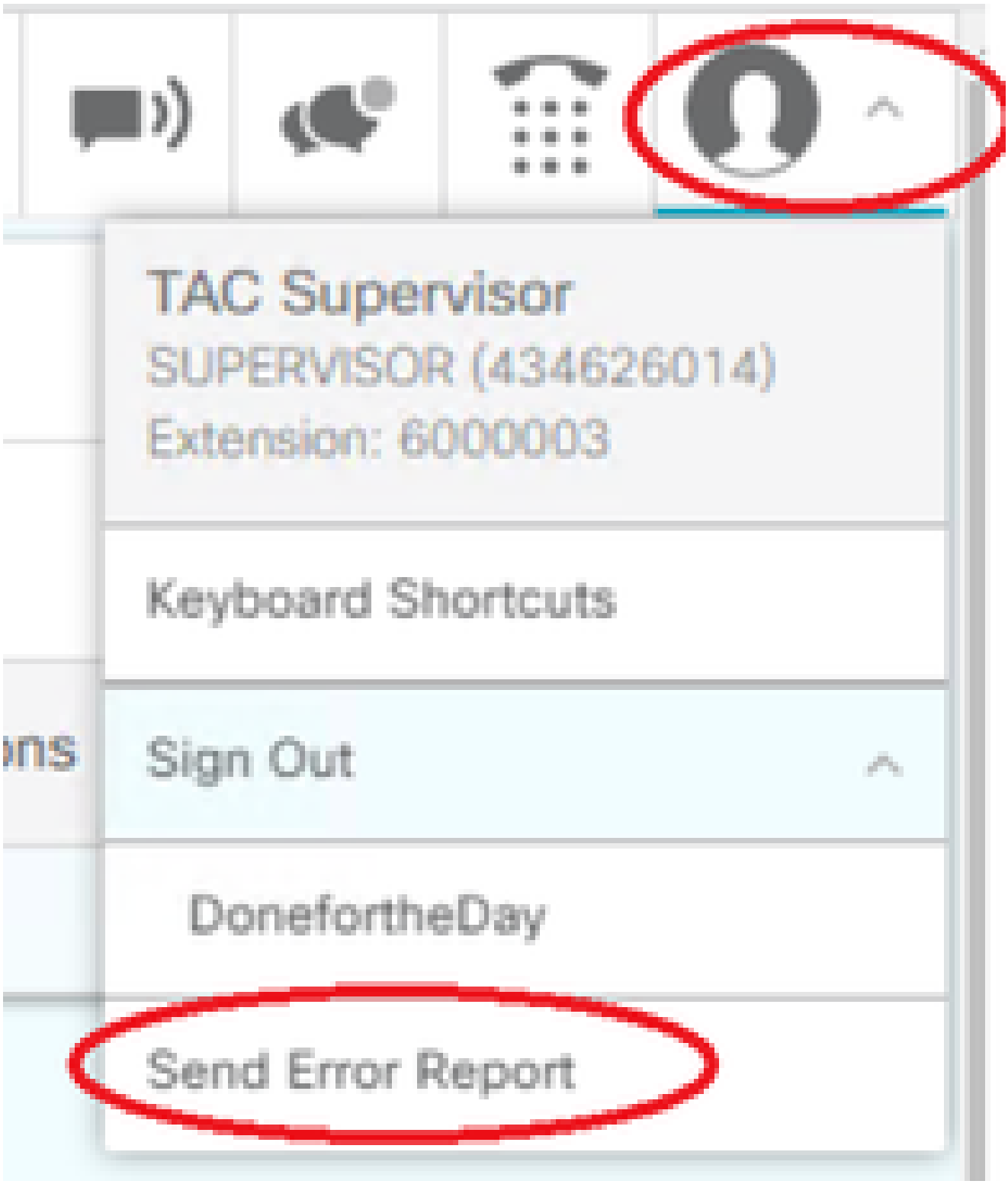
Définition des suivis et collecte des journaux Finesse

Client Finesse

Il existe plusieurs options pour collecter les journaux des clients Finesse.

Option 1 : Collecter les journaux client via le rapport d'erreurs d'envoi

1. Connectez un agent.
2. Si un agent rencontre un problème lors d'un appel ou d'un événement multimédia, demandez à l'agent de cliquer sur le lien Send Error Report dans le coin supérieur droit du bureau Finesse.

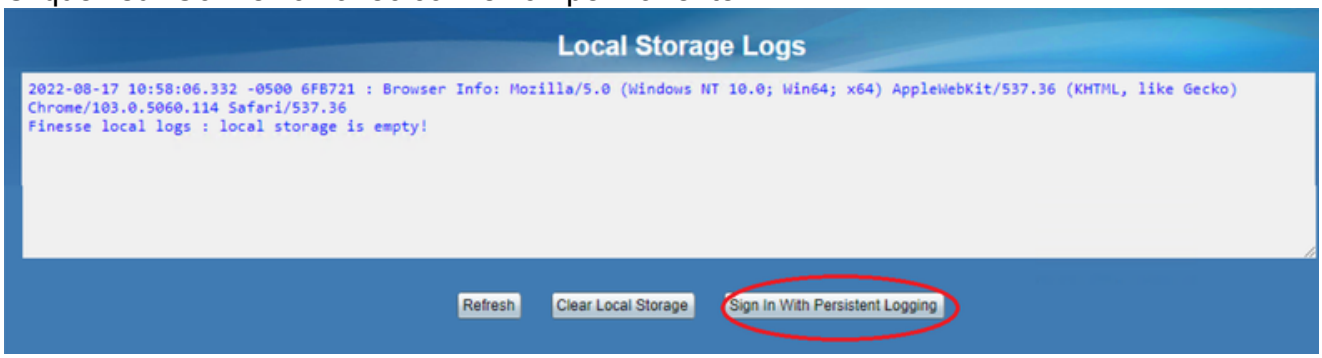


3. L'agent voit les journaux envoyés avec succès ! message.
4. Les journaux du client sont envoyés au serveur Finesse. Accédez à Journaux Finesse et connectez-vous avec un compte d'administration.
5. Collectez les journaux dans le répertoire clientlogs/ .

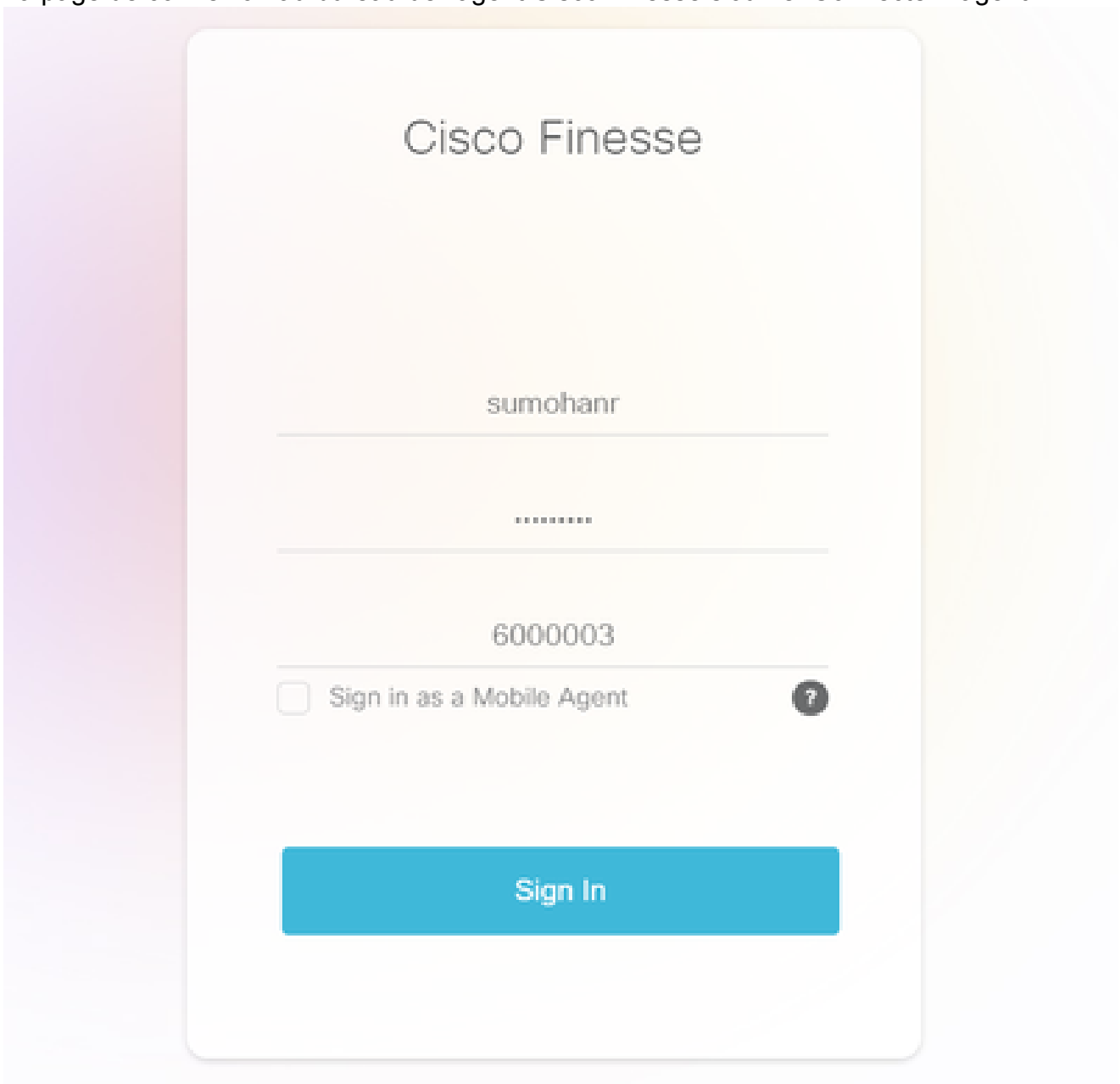


Option 2 : Définir la journalisation permanente

1. Accédez au journal local du bureau.
2. Cliquez sur Connexion avec connexion permanente.



3. La page de connexion au bureau de l'agent Cisco Finesse s'ouvre. Connectez l'agent.

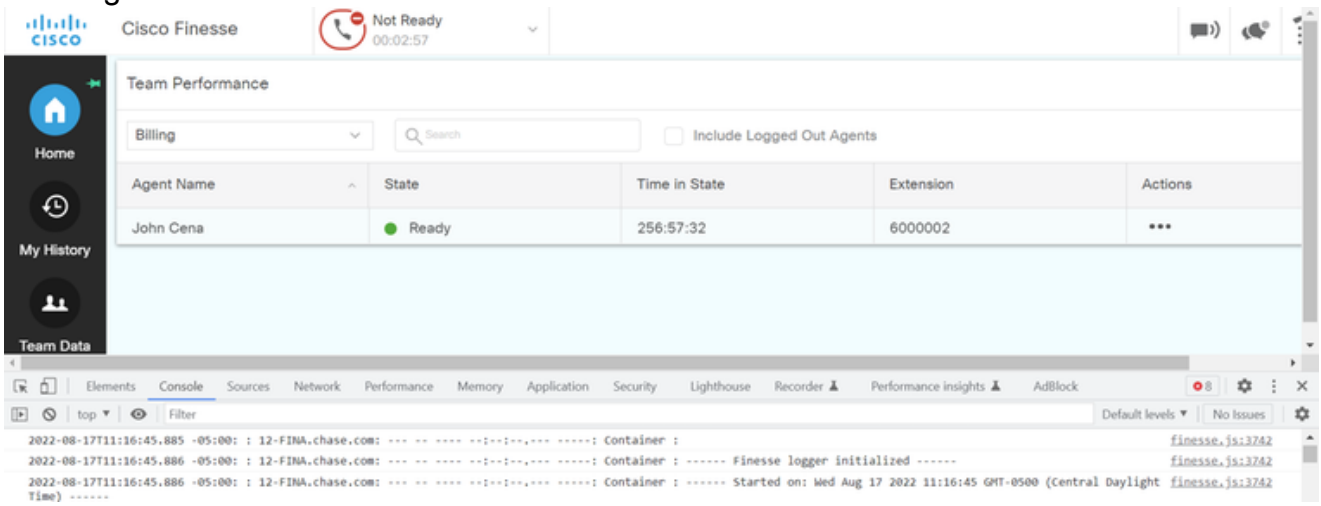


4. Toutes les interactions entre les agents et le bureau sont enregistrées et envoyées aux journaux de stockage local. Pour collecter les journaux, accédez à Desktop Local Log et copiez le contenu dans un fichier texte. Enregistrez le fichier pour une analyse plus

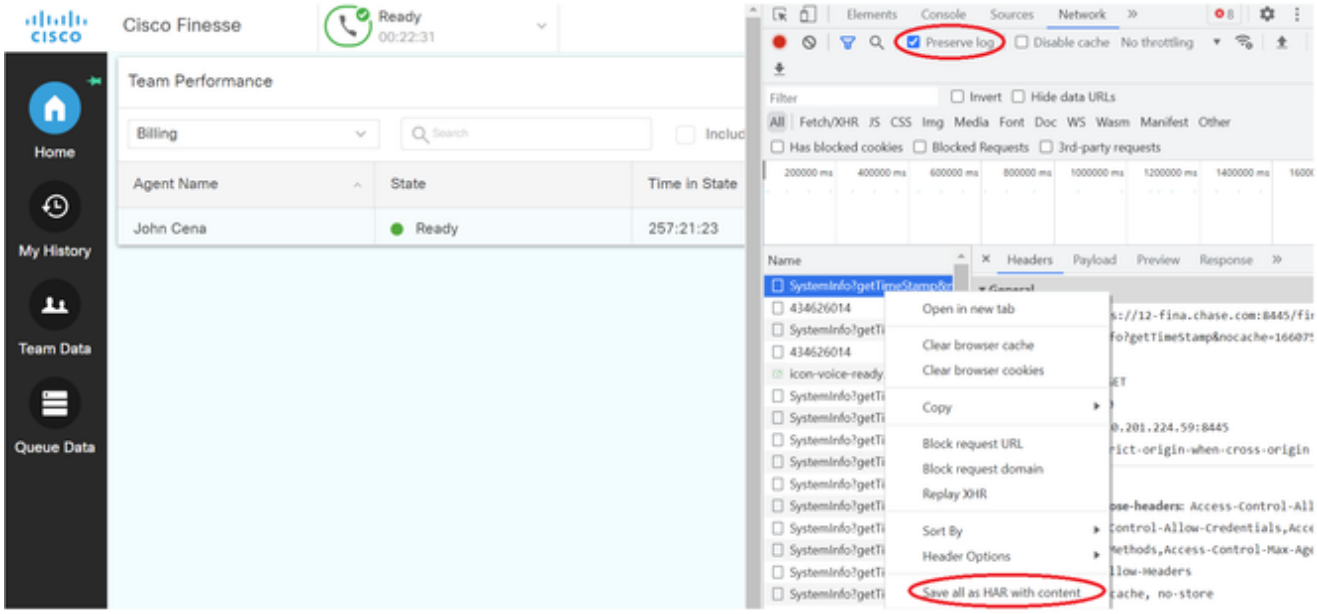
approfondie.

Option 3 : Console du navigateur Web

1. Une fois qu'un agent se connecte, appuyez sur F12 pour ouvrir la console du navigateur.
2. Sélectionnez l'onglet Console.
3. Recherchez les erreurs sur la console du navigateur. Copiez le contenu dans un fichier texte et enregistrez-le.



4. Sélectionnez l'onglet Réseau et cochez l'option Conserver le journal.
5. Cliquez avec le bouton droit sur un événement de nom de réseau et sélectionnez Save HAR avec contenu.



Serveur Finesse

Option 1 : Via l'interface utilisateur (UI) - Services Web (obligatoire) et journaux supplémentaires

1. Accédez à Journaux Finesse et connectez-vous avec le compte d'administration.
2. Développez le répertoire webservices/.



3. Collecter les derniers journaux de service Web. Sélectionnez le dernier fichier décompressé. Par Exemple, Desktop-Webservices.201X-.log.zip. Cliquez sur le lien du fichier et vous voyez l'option pour Enregistrer le fichier.



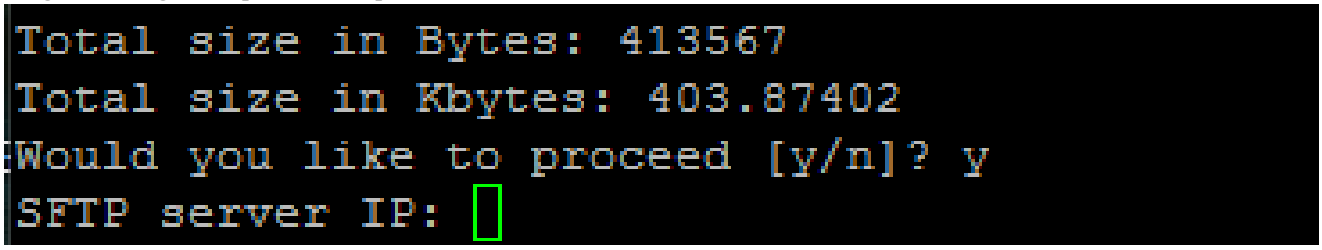
4. Collectez les autres journaux requis (selon le scénario). Par exemple, openfire pour les problèmes de service de notification, les journaux de domaine pour les problèmes d'authentification et les tomcatlogs pour les problèmes d'API.

Remarque : La méthode recommandée pour collecter les journaux du serveur Cisco Finesse est via Secure Shell (SSH) et Secure File Transfer Protocol (SFTP). Cette méthode vous permet non seulement de collecter les journaux de services Web, mais aussi tous les journaux supplémentaires comme Fippa, openfire, Realm et Clientlogs.

Option 2 : Via SSH et SFTP (Secure File Transfer Protocol) - Option recommandée

1. Connectez-vous au serveur Finesse avec le SSH.
2. Entrez cette commande afin de collecter les journaux dont vous avez besoin. La commande collecte les journaux pendant 2 heures. Vous êtes invité à identifier le serveur SFTP sur lequel les journaux sont téléchargés.

file get activelog desktop recurs compress reltime hours 2



3. Ces journaux sont stockés sur le chemin du serveur SFTP : <adresse IP>\<horodatage>\active_nnn.tgz , où nnn est l'horodatage au format long.
4. Pour collecter des journaux supplémentaires tels que tomcat, Context service, Servm et install, reportez-vous à la section Log Collection du Guide d'administration de Cisco Finesse version 12.5(1).

Définition des suivis et collecte des journaux CVP et CVVB

Serveur d'appels CVP

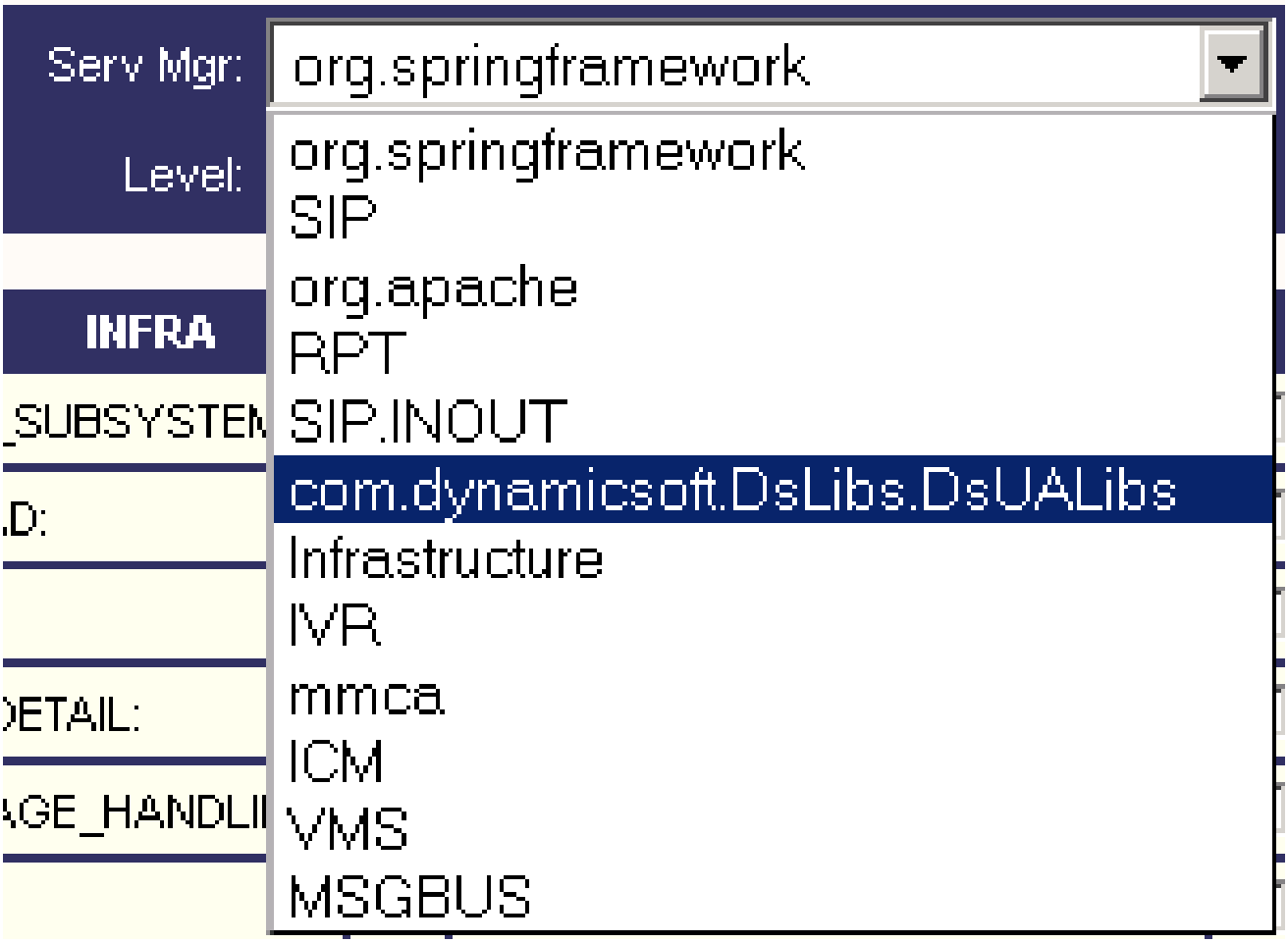
1. Le niveau de suivi par défaut de CVP CallServer est suffisant pour dépanner la plupart des cas. Cependant, lorsque vous avez besoin d'obtenir plus de détails sur les messages SIP

(Session Initiation Protocol), vous devez définir les traces de la pile SIP au niveau DEBUG.

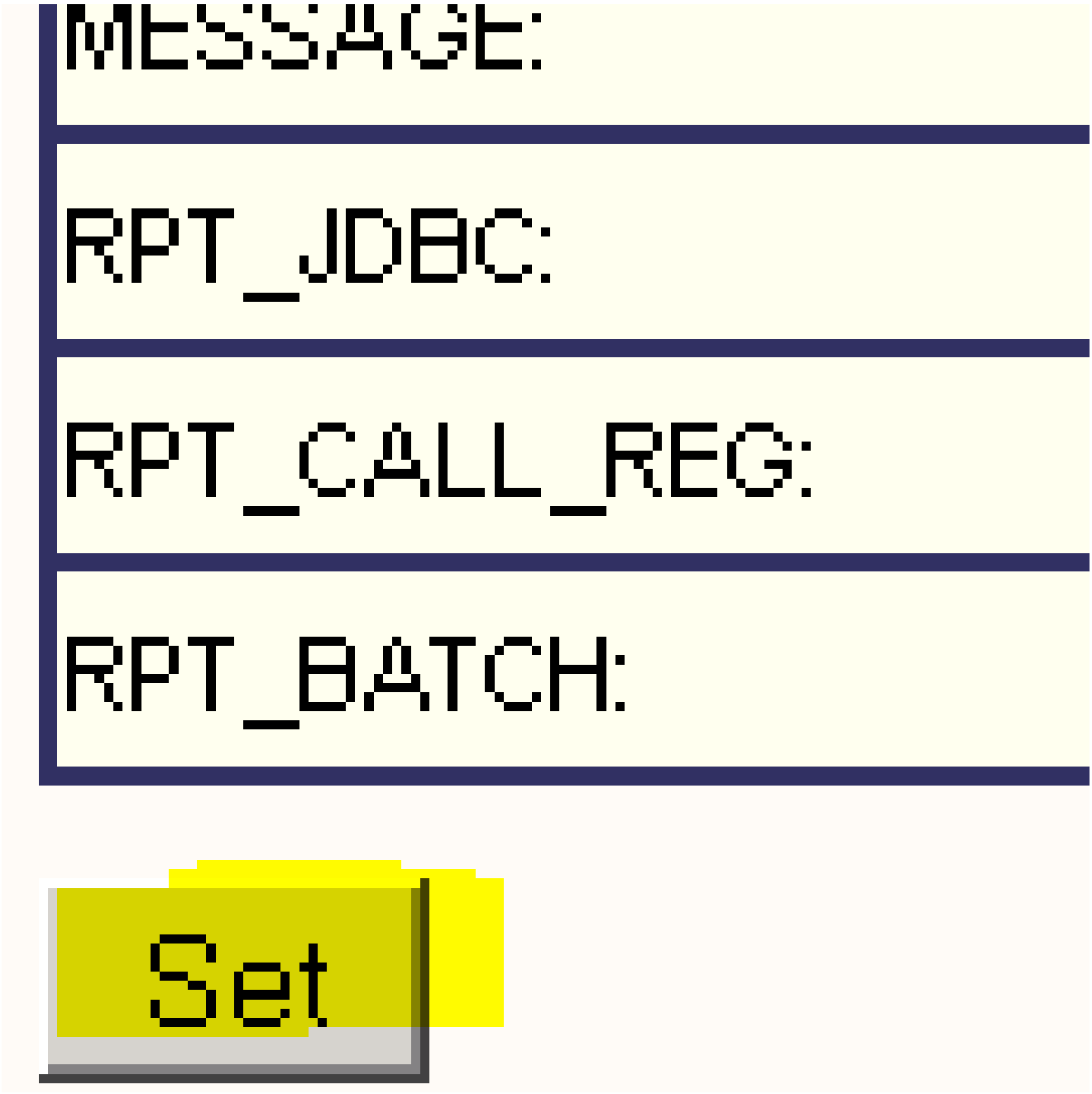
2. Accédez à l'URL de la page Web CVP CallServer Diag Local Host 8000.

> Remarque : Cette page fournit de bonnes informations sur le serveur d'appels CVP et il est très utile de dépanner certains scénarios.

3. Sélectionnez com.dynamicsoft.DsLibs.DsUALibs dans le Serv. Menu déroulant Mgr dans l'angle supérieur gauche.



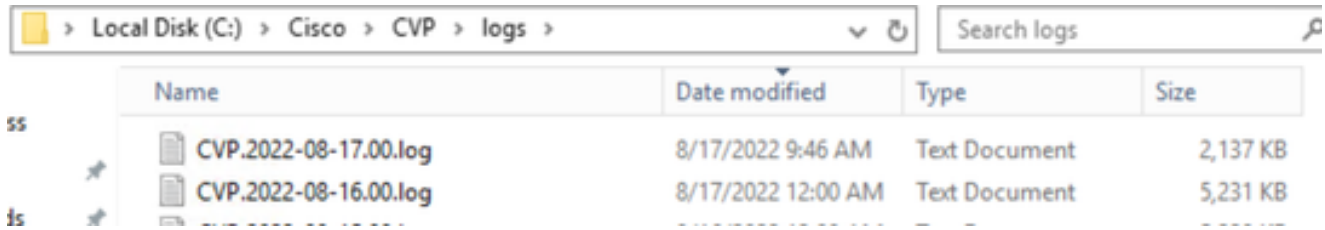
4. Cliquez sur le bouton Set.



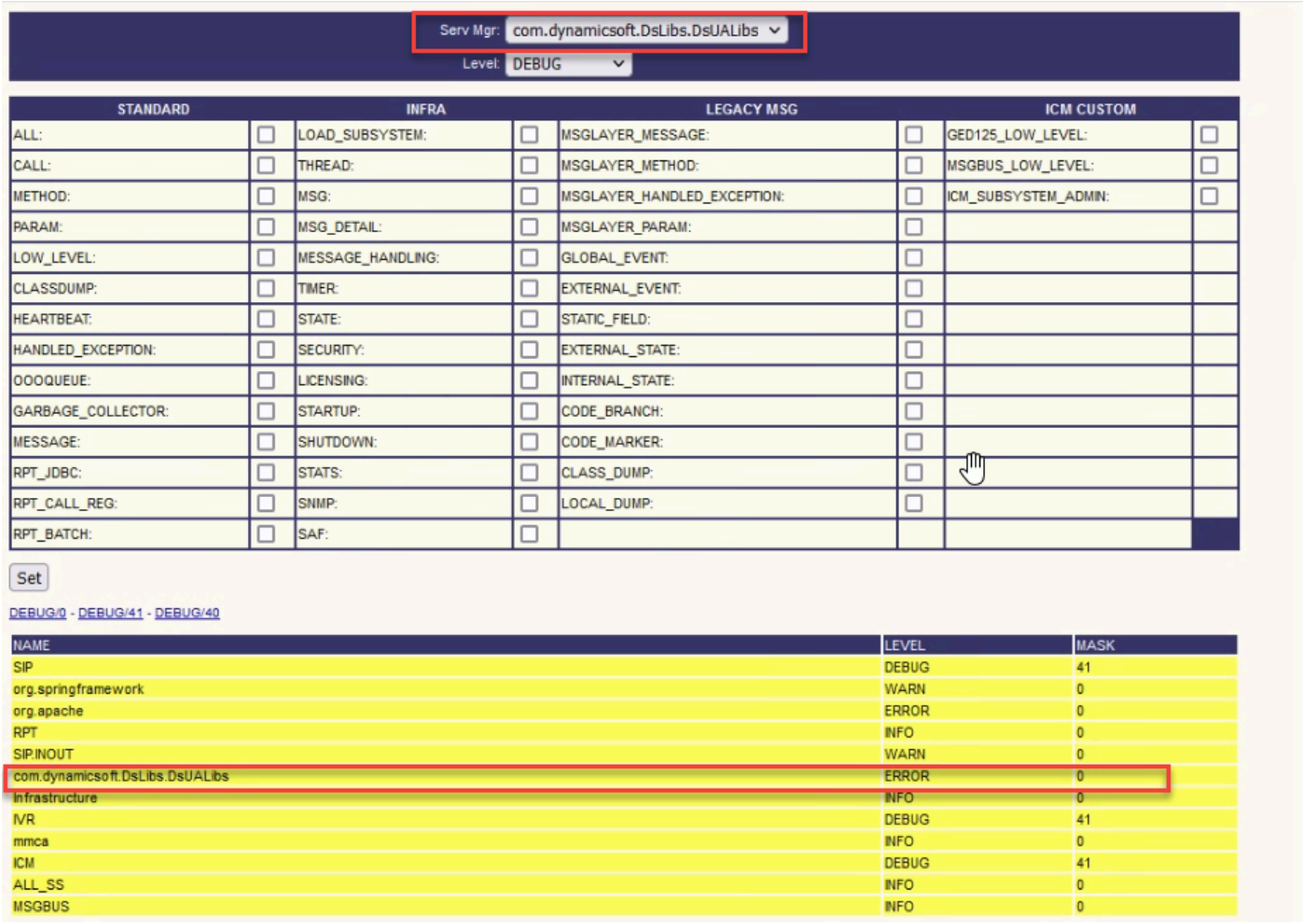
5. Faites défiler la fenêtre de trace vers le bas afin de vous assurer que le niveau de trace a été défini correctement. Voici vos paramètres de débogage.

NAME	LEVEL	MASK
org.springframework	WARN	0
SIP	DEBUG	41
org.apache	ERROR	0
RPT	DEBUG	1
SIP.INOUT	WARN	0
com.dynamicsoft.DsLibs.DsUALibs	DEBUG	0
Infrastructure	INFO	0
IVR	DEBUG	41
mmca	INFO	0
ICM	DEBUG	41
MSGBUS	INFO	0

6. Lorsque vous reproduisez le problème, collectez les journaux à partir de C:\Cisco\CVP\logs et sélectionnez le fichier journal CVP en fonction de l'heure à laquelle le problème s'est produit.



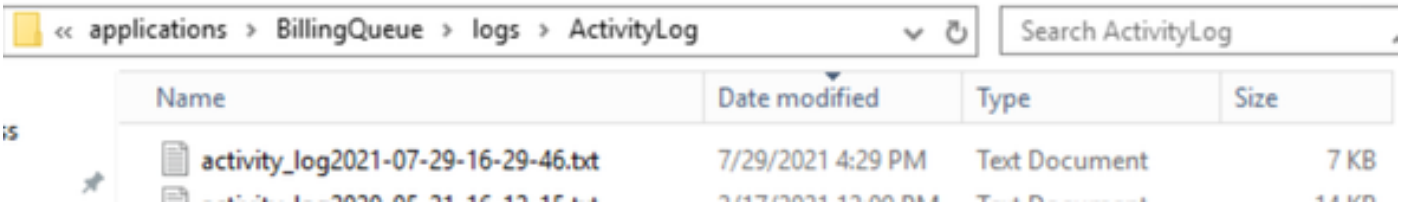
7. Après avoir reproduit le problème, assurez-vous de restaurer les traces au niveau par défaut. Sélectionnez com.dynamicsoft.DsLibs.DsUALibs dans le Serv. Menu déroulant Mgr dans le coin supérieur gauche et définissez-le sur Erreur.



Application CVP Voice XML (VXML)

Dans de très rares cas, vous devez augmenter le niveau de traces des applications serveur VXML. D'un autre côté, il n'est pas recommandé de l'augmenter à moins qu'un ingénieur Cisco ne le demande.

Pour collecter les journaux d'application du serveur VXML, accédez au répertoire d'application spécifique sous le serveur VXML, par exemple : C:\Cisco\CVP\VXMLServer\applications\{nom de l'application}\logs\ActivityLog\ et collectez les journaux d'activité.



CVP Operations and Administration Management Portal (OAMP)

Dans la plupart des cas, le niveau de traces par défaut d'OAMP et d'ORM est suffisant pour déterminer la cause première du problème. Cependant, si le niveau de traces doit être augmenté, voici les étapes pour exécuter cette action :

1. Sauvegarder %CVP_HOME%\conf\oamp.properties.

2. Modifiez %CVP_HOME%\conf\oamp.properties.

```
omgr.traceMask=-1
omgr.logLevel=DEBUG
org.hibernate.logLevel=DEBUG
org.apache.logLevel=ERROR
net.sf.ehcache.logLevel=ERROR
```

3. Redémarrez OPSConsoleServer après la modification comme indiqué.

Informations sur le niveau de suivi

Niveau de suivi	Description	Niveau de consignation	Masque de suivi
0	Installation du produit par défaut. Impact sur les performances nul ou minimal attendu.	INFOS	Aucune
1	Messages de suivi moins détaillés avec un impact limité sur les performances.	DÉBOGUER	CONFIGURATION_PÉRIPHÉRIQUE + MODIFIER_BASE_DE_DONNÉES + GESTION=0x01011000
2	Messages de suivi détaillés avec un impact moyen sur les performances.	DÉBOGUER	CONFIGURATION_PÉRIPHÉRIQUE + SYSLVL_CONFIGURATION + MODIFIER_BASE_DE_DONNÉES +

Niveau de suivi	Description	Niveau de consignation	Masque de suivi
			GESTION=0x05011000
3	Message de suivi détaillé avec un impact élevé sur les performances.	DÉBOGUER	CONFIGURATION_PÉRIPHÉRIQUE + SYSLVL_CONFIGURATION + OPÉRATIONS_MASSE + MODIFIER_BASE_DE_DONNÉES + GESTION=0x05111000
4	Message de suivi détaillé avec un impact très important sur les performances.	DÉBOGUER	MISC + CONFIGURATION_PÉRIPHÉRIQUE + ST_CONFIGURATION + SYSLVL_CONFIGURATION + OPÉRATIONS_MASSE + BULK_EXCEPTION_STACKTRACE + MODIFIER_BASE_DE_DONNÉES + SÉLECTION_BASE_DE_DONNÉES + INFO_PO_BASE_DE_DONNÉES + GESTION + TRACE_METHOD + TRACE_PARAM=0x17371000
5	Message de suivi détaillé le plus élevé.	DÉBOGUER	MISC + CONFIGURATION_PÉRIPHÉRIQUE + ST_CONFIGURATION + SYSLVL_CONFIGURATION + OPÉRATIONS_MASSE + BULK_EXCEPTION_STACKTRACE + MODIFIER_BASE_DE_DONNÉES + SÉLECTION_BASE_DE_DONNÉES +

Niveau de suivi	Description	Niveau de consignation	Masque de suivi
			INFO_PO_BASE_DE_DONNÉES + GESTION + TRACE_METHOD + TRACE_PARAM=0x17371006

Navigateur vocal virtualisé Cisco (CVVB)

Dans CVVB, un fichier de trace est un fichier journal qui enregistre l'activité des sous-systèmes et des étapes des composants Cisco VVB.

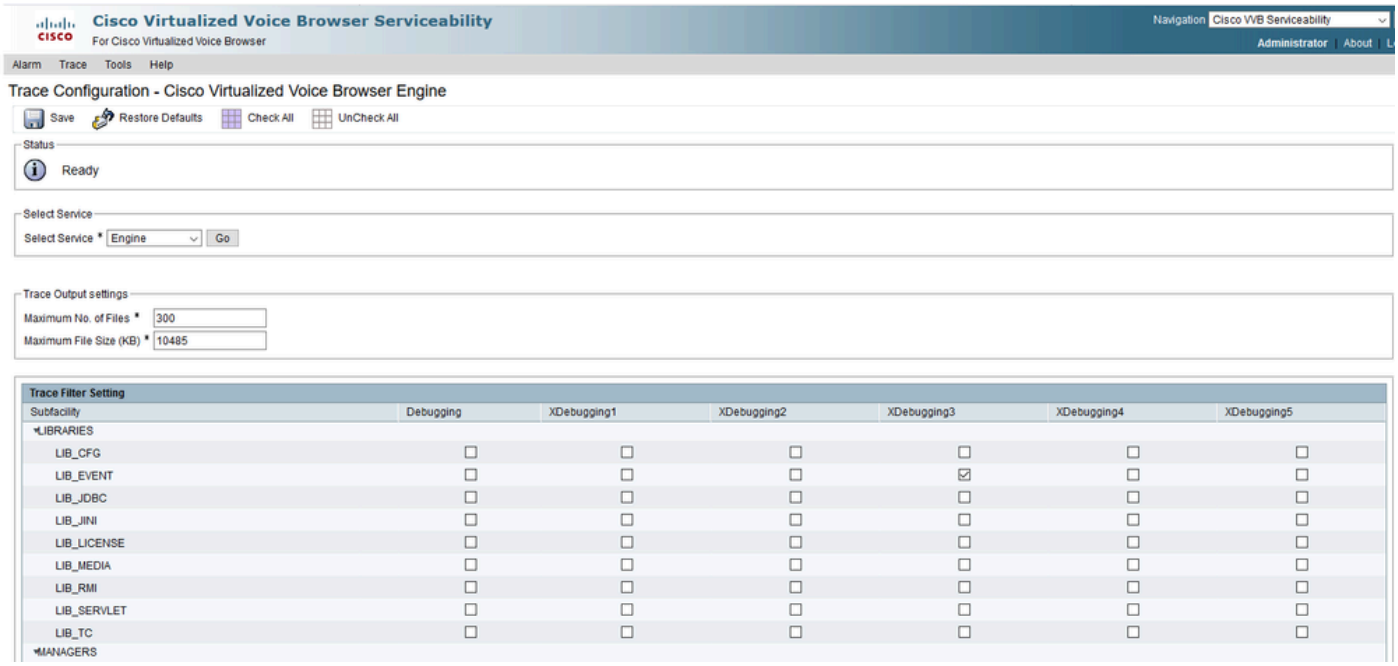
Cisco VVB comporte deux composants principaux :

1. Suivis d'administration Cisco VVB appelés journaux MADM
2. Suivis du moteur Cisco VVB appelés journaux MIVR

Vous pouvez spécifier les composants pour lesquels vous souhaitez collecter des informations et le niveau d'informations que vous souhaitez collecter.

Les niveaux de consignation s'étendent de :

- Débogage - Détails de flux de base vers
- XDebugging 5 - Niveau détaillé avec Stack Trace



Avertissement : Xdebugging5 ne doit pas être activé sur le système chargé en production.

Les journaux les plus courants que vous devez collecter sont le moteur. Le niveau de suivi par

défaut du moteur CVB est suffisant pour résoudre la plupart des problèmes. Toutefois, si vous devez modifier le niveau de suivi d'un scénario spécifique, Cisco vous recommande d'utiliser les profils de journal système prédéfinis.

Profils du journal système

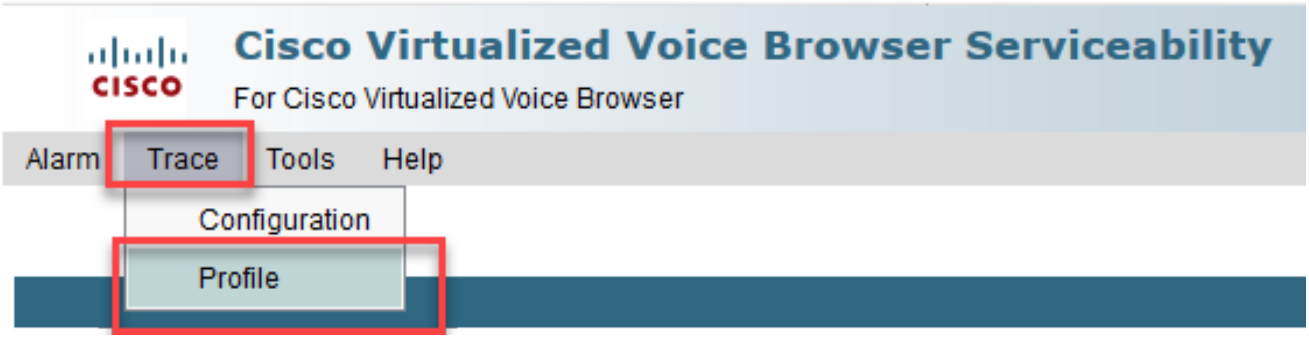
Nom	Scénario dans lequel ce profil doit être activé
VB par défaut	Les journaux génériques sont activés.
AppAdminVVB	Pour les problèmes d'administration Web via AppAdmin, Cisco VVB Serviceability et d'autres pages Web.
MediaVB	Pour les problèmes de configuration ou de transmission multimédia.
VoiceBrowserVVB	Pour les problèmes de gestion des appels.
MRCPVB	Pour les problèmes d'interaction ASR/TTS avec Cisco VVB.
ContrôleAppelVB	Pour les problèmes liés au signal SIP sont publiés dans le journal.

Option 1 : Via un compte d'administration

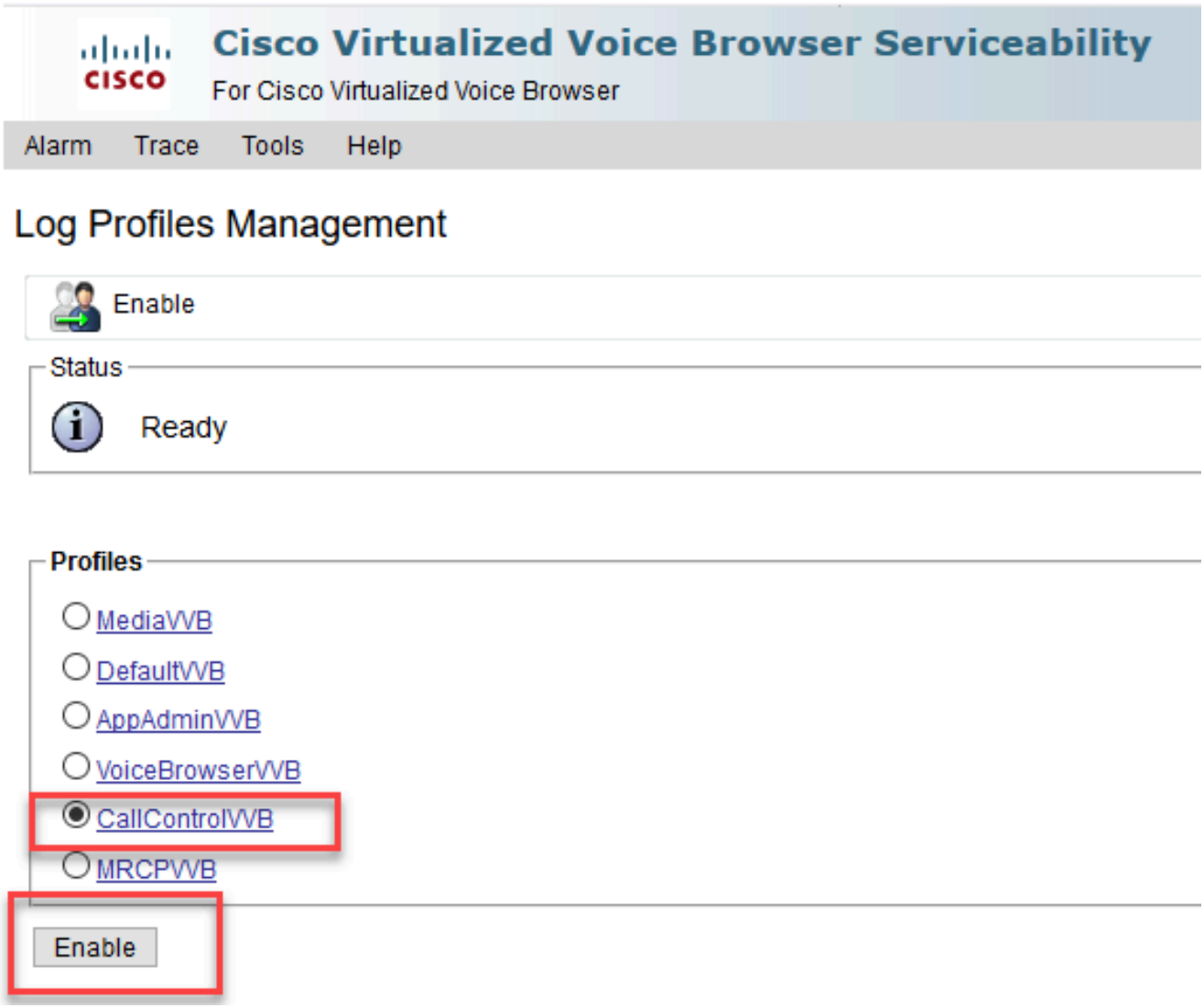
1. Ouvrez la page principale de CVVB, UCCX Service Main, et accédez à la page Cisco VVB Serviceability. Connectez-vous avec le compte d'administration.



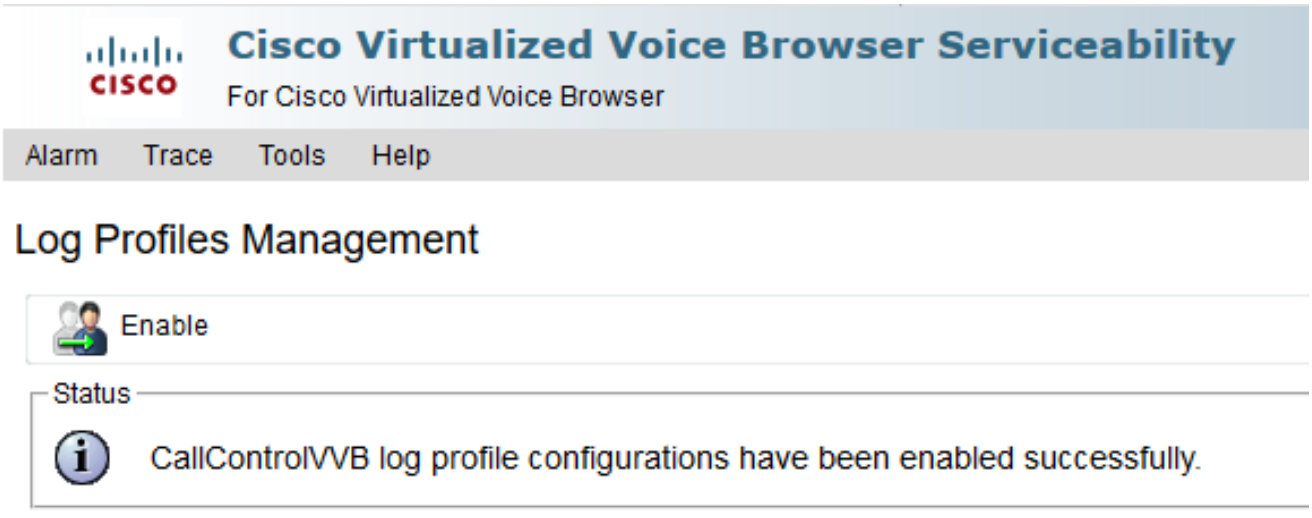
2. Sélectionnez Trace > Profile.



3. Cochez le profil que vous souhaitez activer pour le scénario spécifique et cliquez sur le bouton Enable. Par exemple, activez le profil CallControlVVB pour les problèmes liés au SIP ou MRCPVVB pour les problèmes liés à la reconnaissance vocale automatique et à l'interaction texte-parole (ASR/TTS).

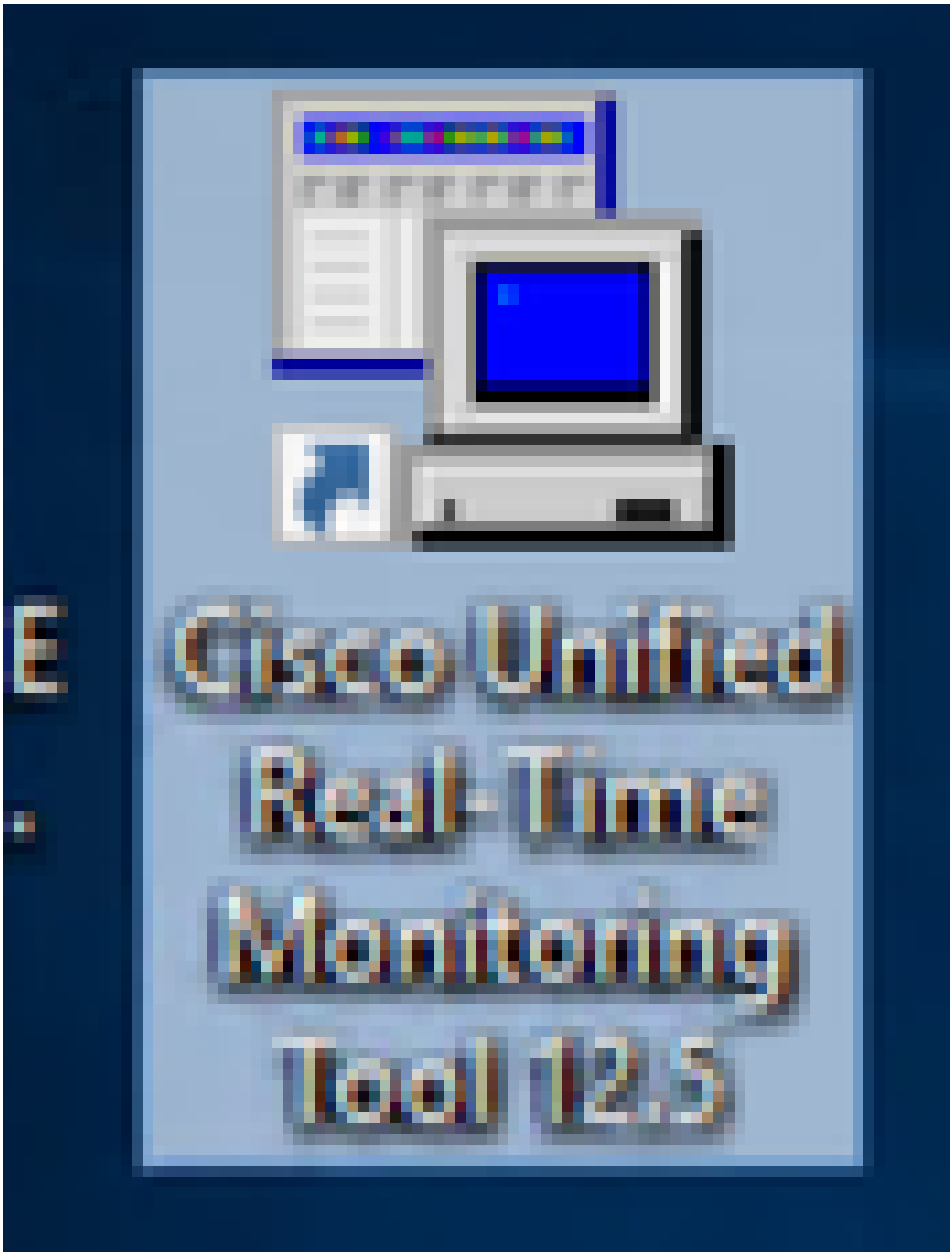


4. Le message de réussite s'affiche lorsque vous cliquez sur le bouton enable.

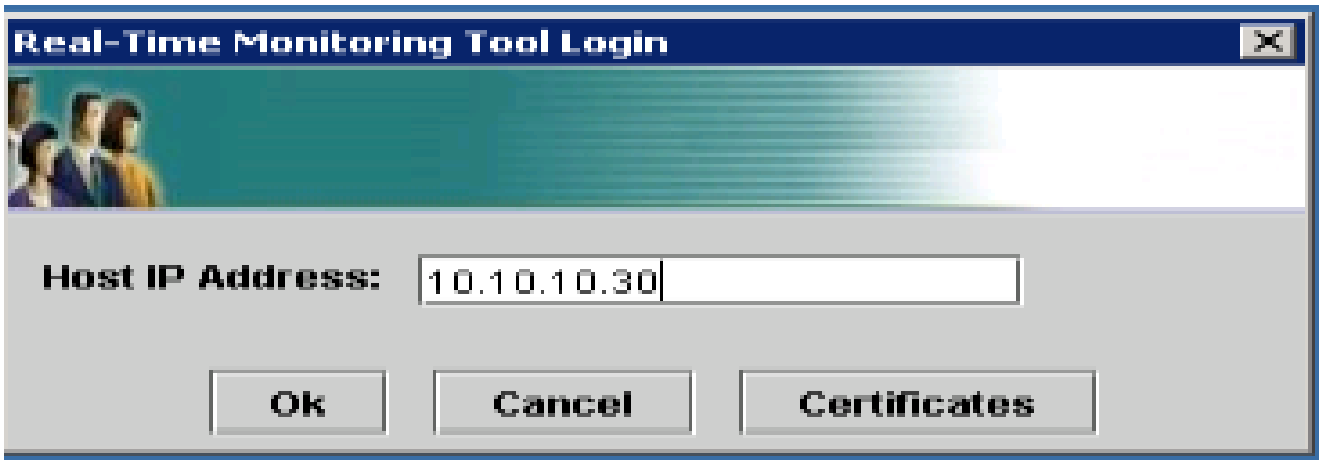


5. Une fois le problème reproduit, collectez les journaux. Utilisez l'outil de surveillance en temps réel (RTMT) fourni avec le CVVB pour collecter les journaux.

6. Cliquez sur l'icône Cisco Unified Real-Time Monitoring Tool sur votre bureau (si nécessaire, téléchargez cet outil à partir du CVVB).



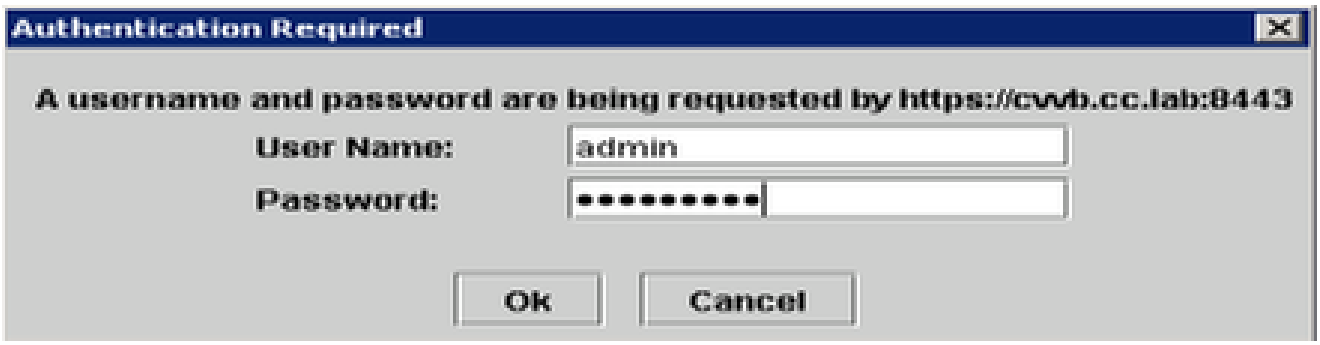
7. Fournissez l'adresse IP du VVB et cliquez sur OK.



8. Accepter les informations de certificat, si elles sont affichées



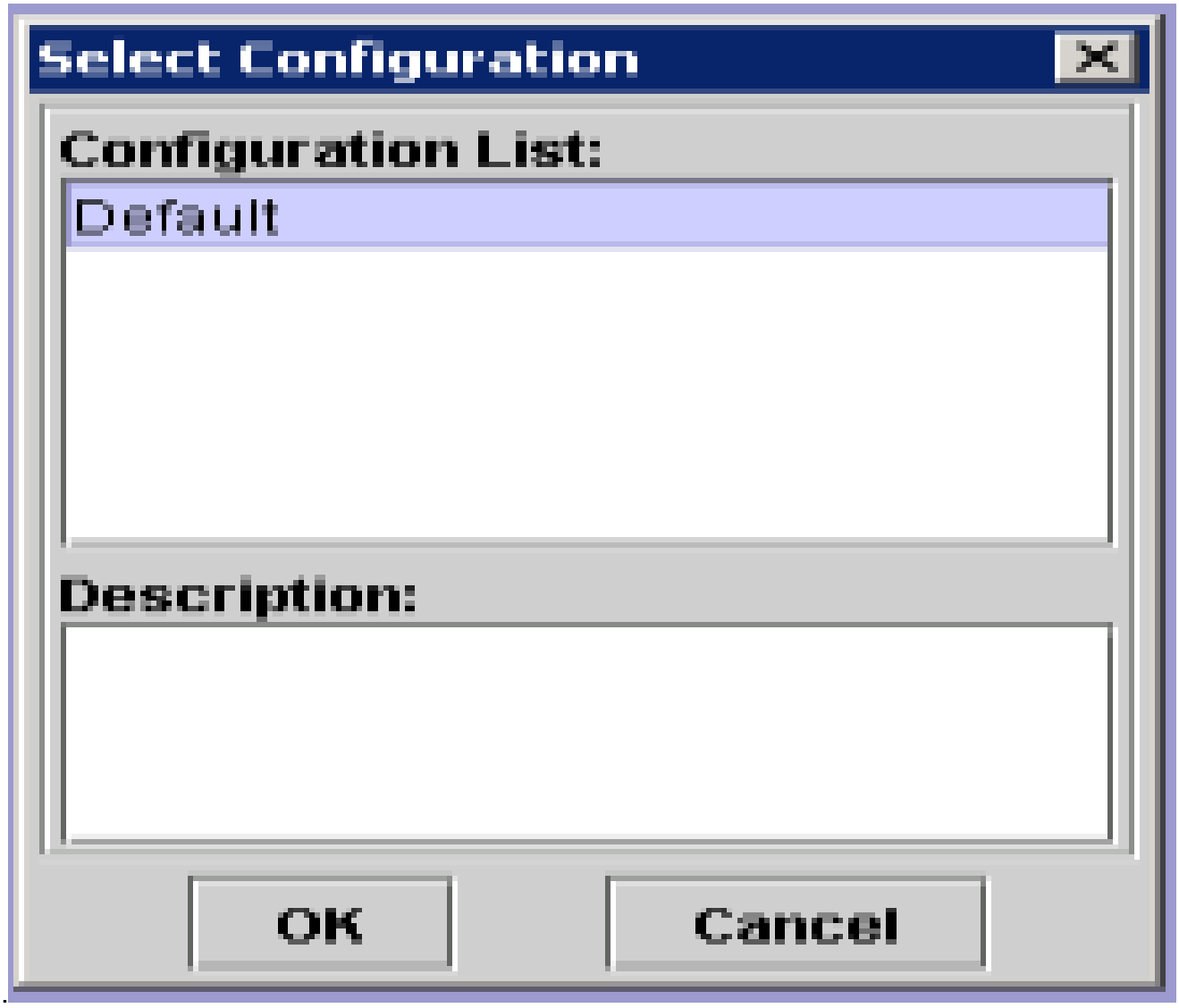
9. Fournissez les informations d'identification et cliquez sur OK.



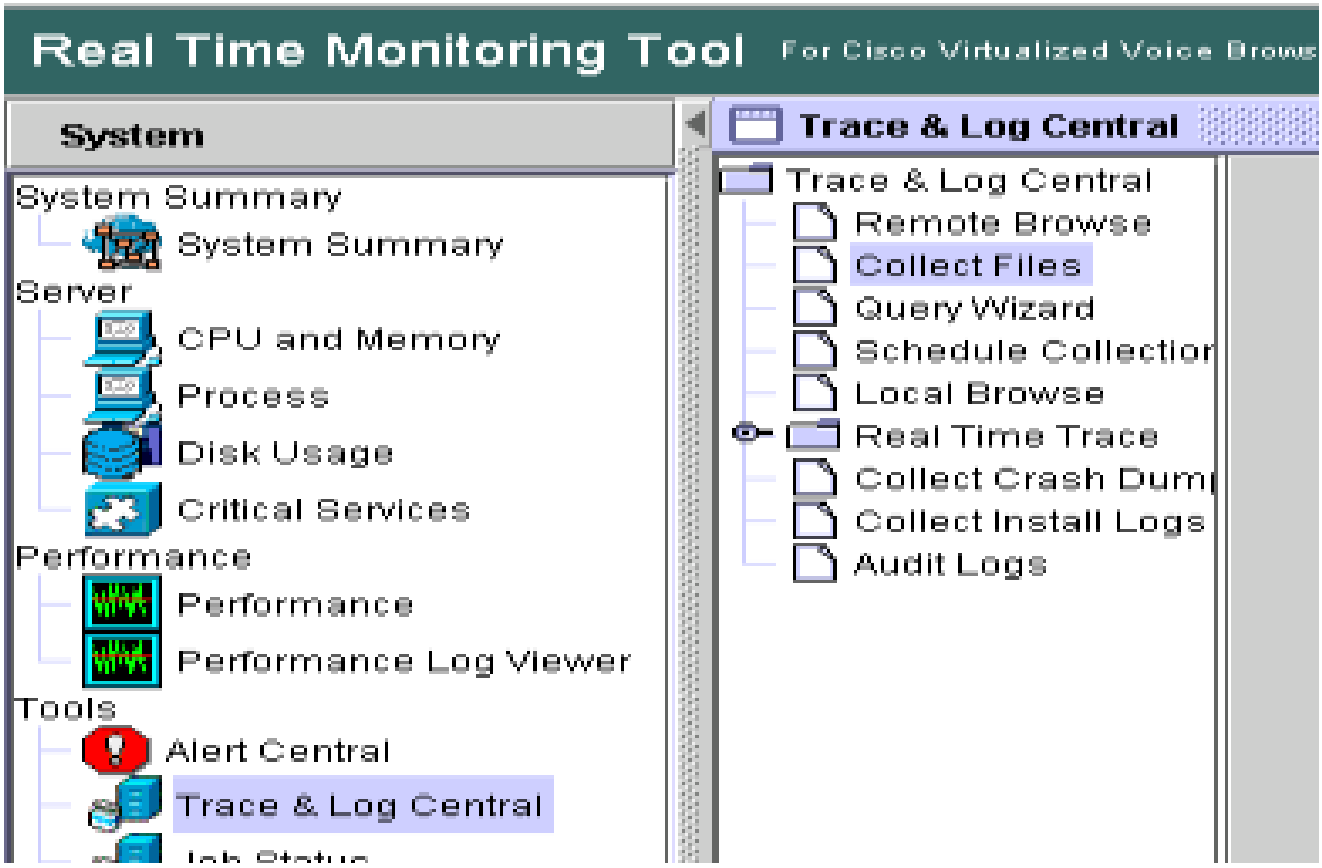
10. Si vous avez reçu l'erreur TimeZone, RTMT peut se fermer après avoir cliqué sur le bouton Yes. Relancez l'outil RTMT.



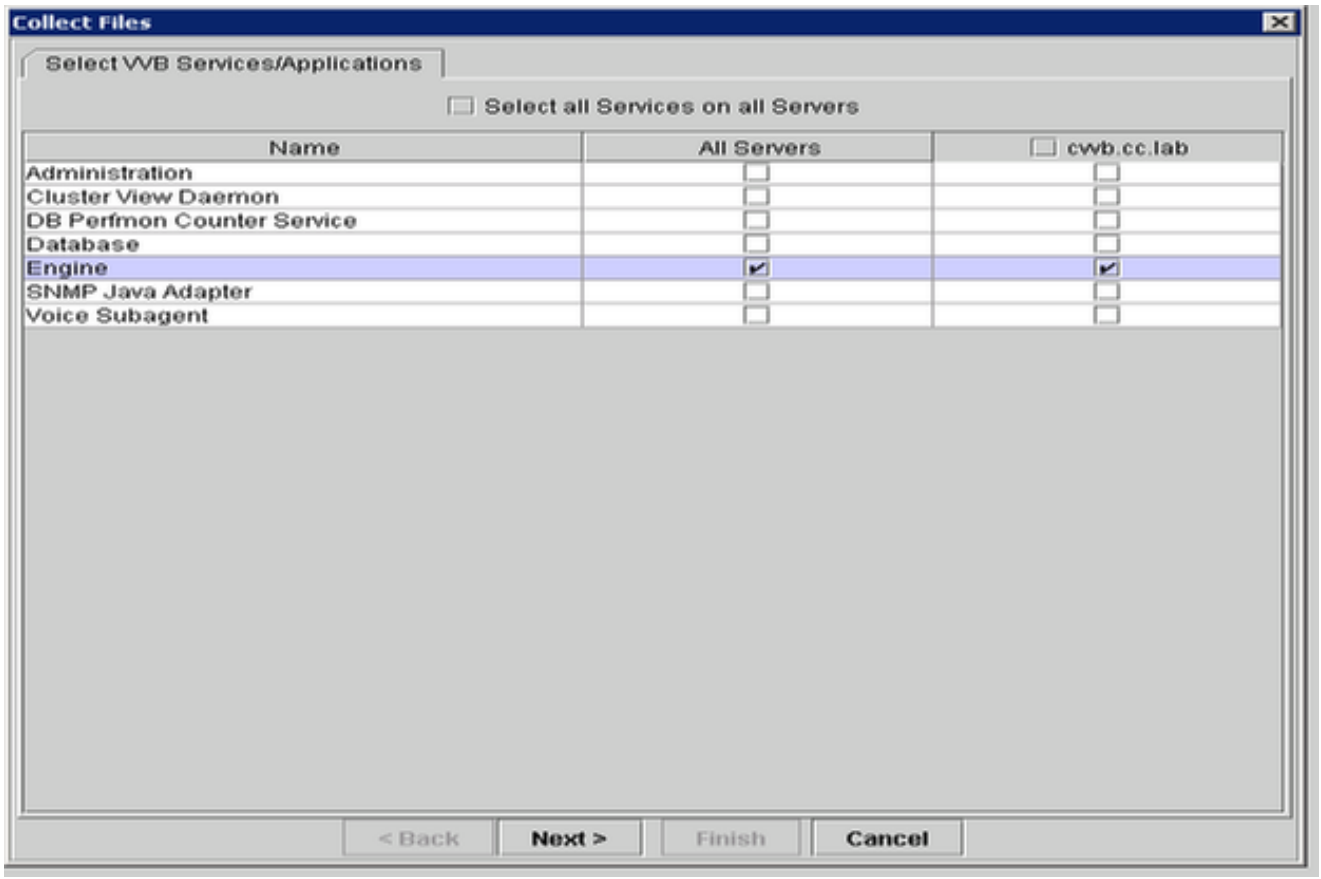
11. Laissez la configuration par défaut sélectionnée et cliquez sur OK.



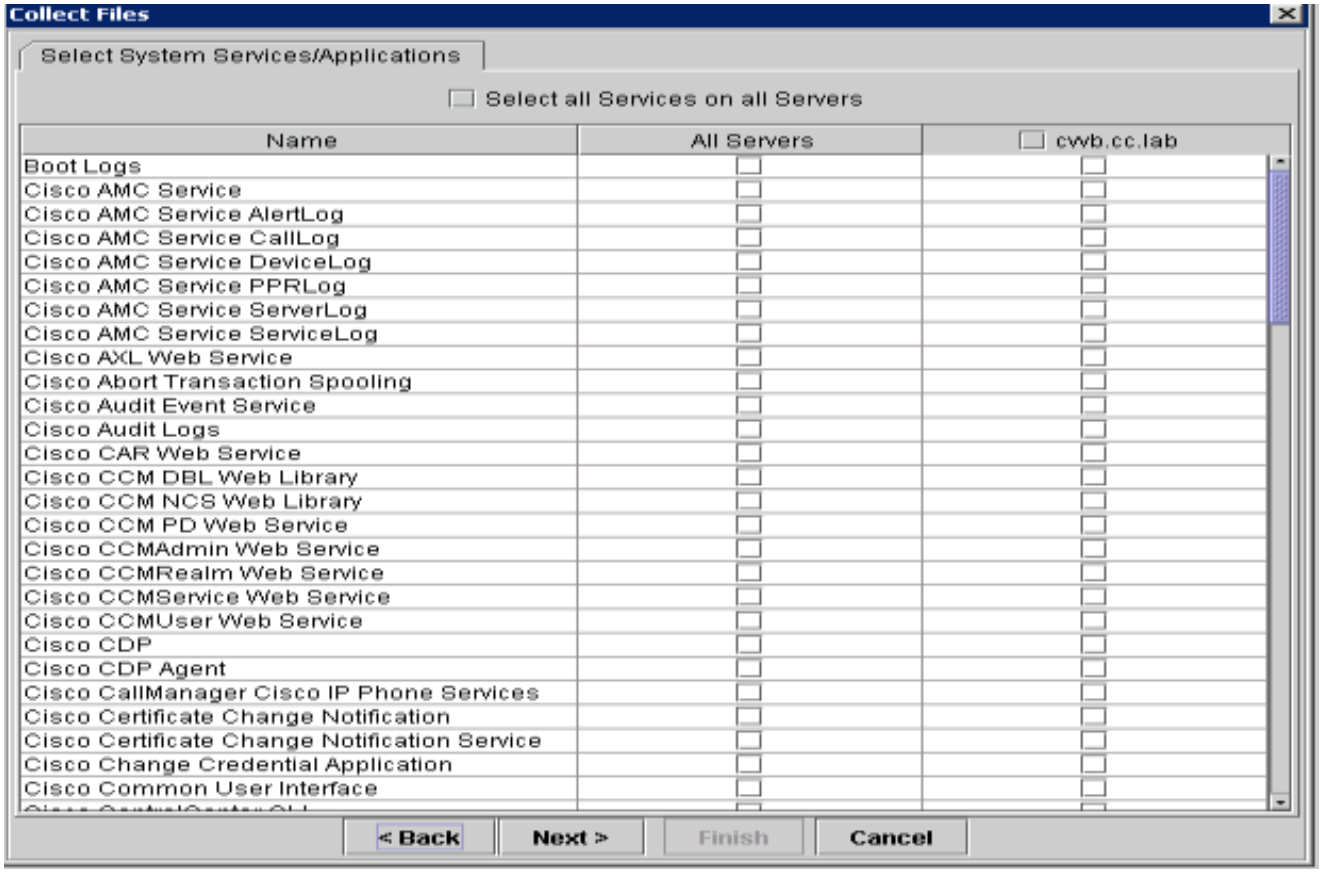
12. Sélectionnez Trace & Log Central, puis double-cliquez sur Collecter les fichiers.



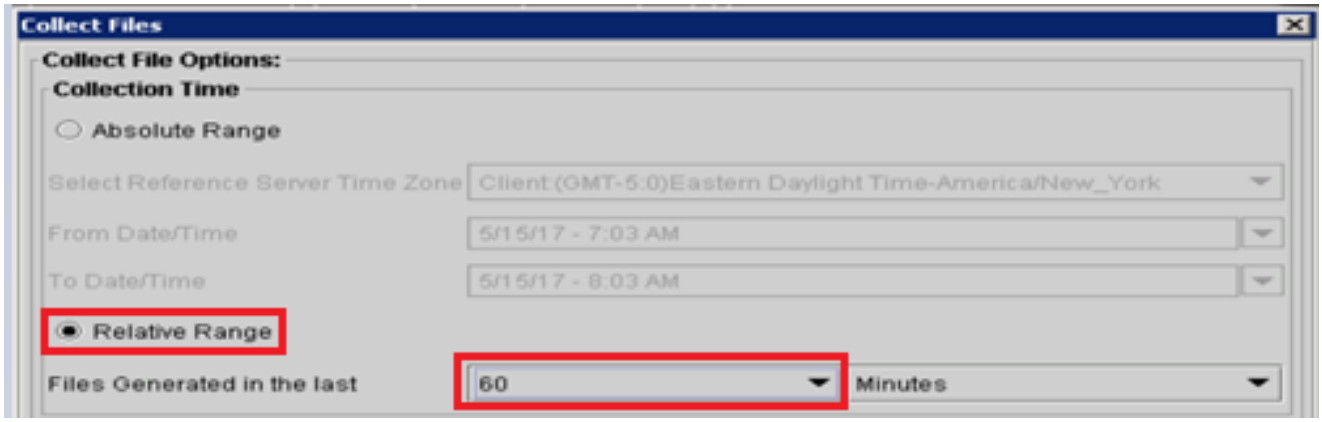
13. Dans la nouvelle fenêtre ouverte, sélectionnez le moteur et cliquez sur Suivant.



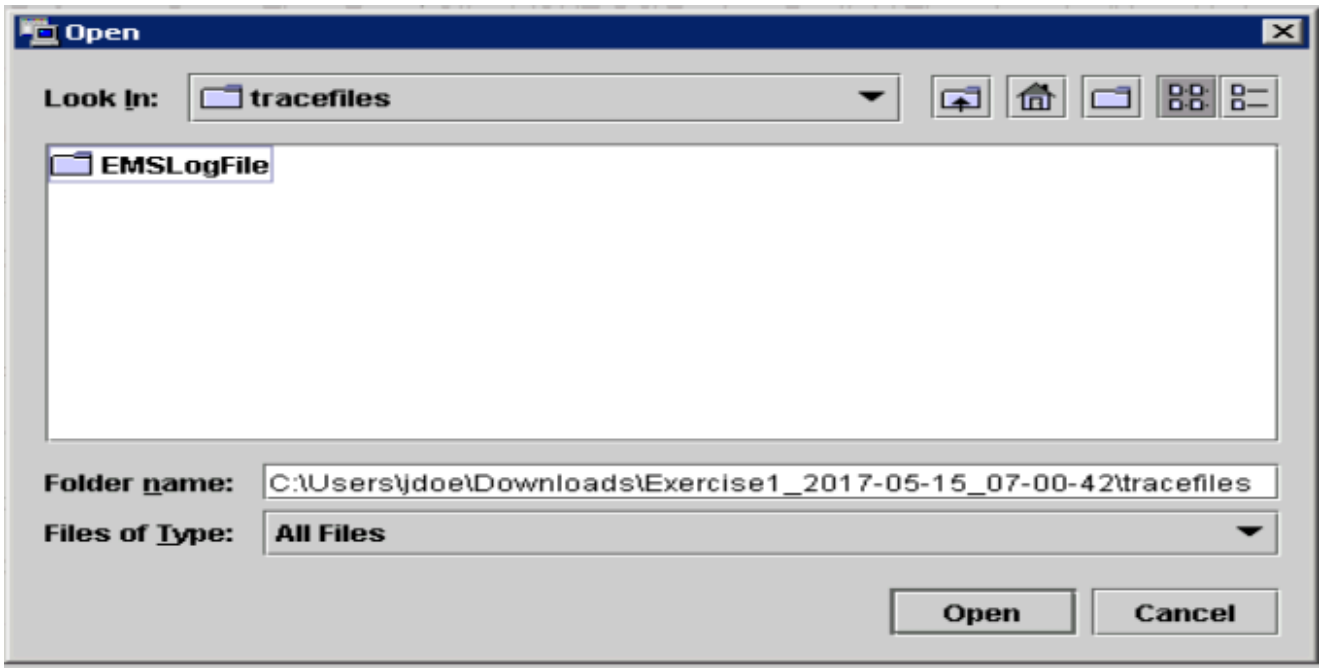
14. Cliquez à nouveau sur Next dans la fenêtre suivante.



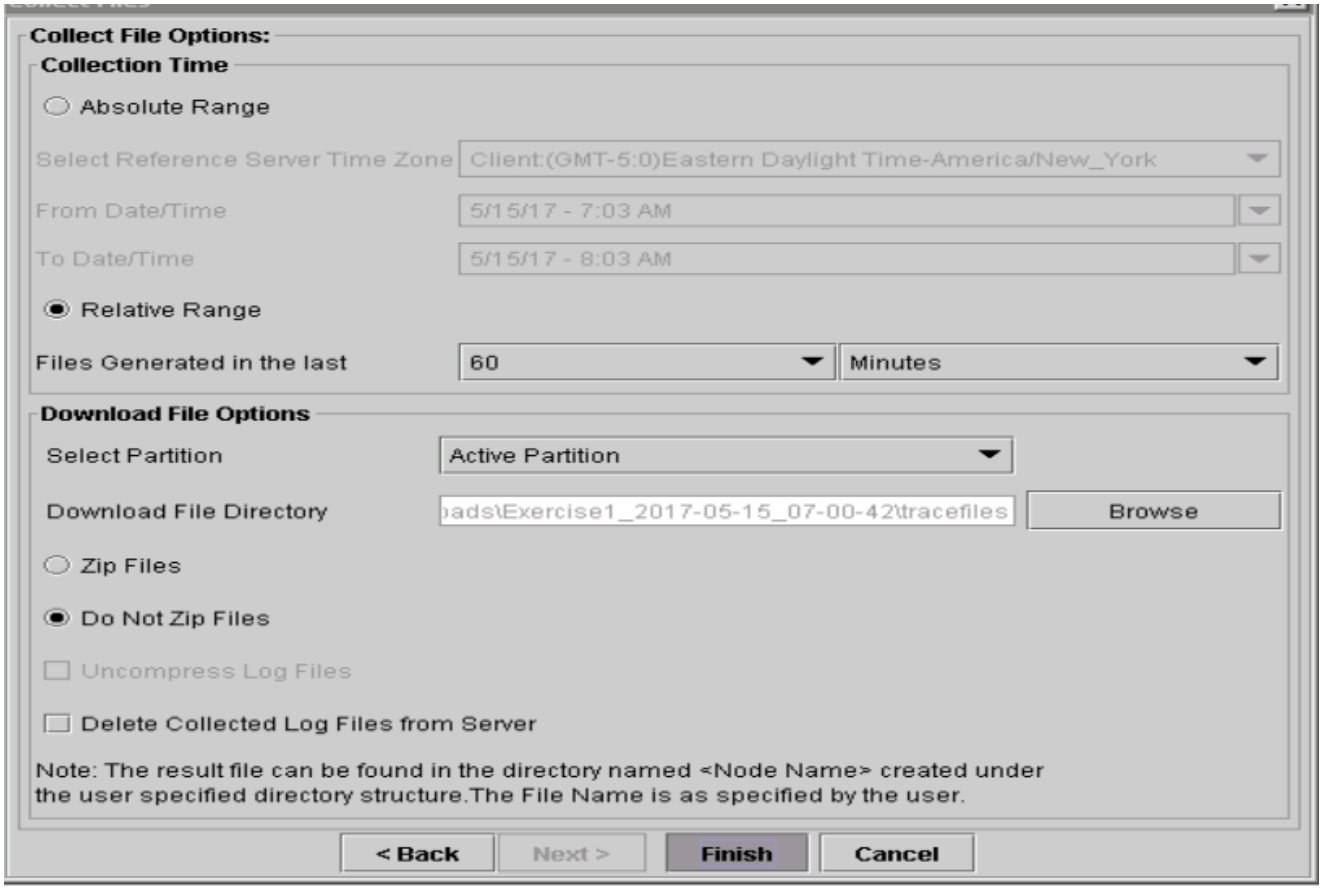
15. Sélectionnez Plage relative et assurez-vous de sélectionner l'heure pour couvrir l'heure de votre mauvais appel.



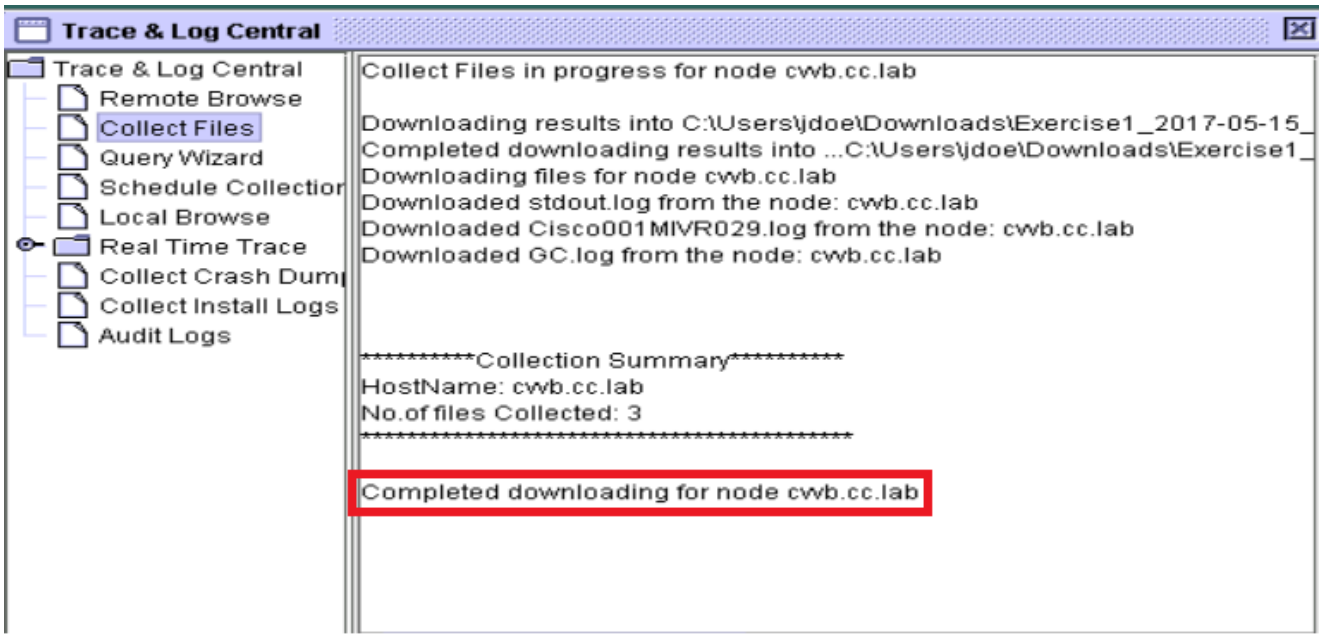
16. Dans les Options de téléchargement de fichier, cliquez sur Parcourir et sélectionnez le répertoire dans lequel vous voulez enregistrer le fichier, puis cliquez sur Ouvrir.



17. Une fois tout est sélectionné, cliquez sur Terminer bouton.



18. Les fichiers journaux sont ainsi collectés. Attendez que le message de confirmation s'affiche sur RTMT.

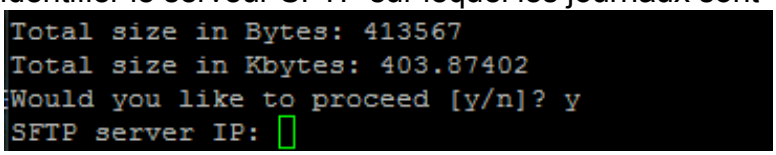


19. Accédez au dossier dans lequel les traces sont enregistrées.

20. Les journaux du moteur sont tout ce dont vous avez besoin. Pour les trouver, accédez au dossier \<horodatage>\uccx\log\MIVR.

Option 2 : Via SSH et SFTP - Option recommandée

1. Connectez-vous au serveur VVB avec le Secure Shell (SSH).
2. Entrez cette commande afin de collecter les journaux dont vous avez besoin. Les journaux sont compressés et vous êtes invité à identifier le serveur SFTP sur lequel les journaux sont téléchargés. **file get activelog /uccx/log/MIVR/***



3. Ces journaux sont stockés sur le chemin du serveur SFTP : <adresse IP>\<horodatage>\active_nnn.tgz, où nnn est l'horodatage au format long.

Définition des journaux de suivi et de collecte pour CUBE et CUSP

CUBE (SIP)

1. Définissez l'horodatage des journaux et activez le tampon de journalisation.

```
#conf  t
service timestamps debug datetime msec
service timestamps log datetime msec
service sequence-numbers
no logging console
no logging monitor
logging buffered 5000000 7
```

```
end
clear logging
```

Avertissement : Toute modification apportée à une passerelle de production du logiciel Cisco IOS® peut entraîner une panne.

2. Il s'agit d'une plate-forme très robuste qui peut gérer les débogages suggérés au volume d'appel fourni sans problème. Toutefois, Cisco vous recommande de :
   - Envoyez tous les journaux à un serveur syslog au lieu du tampon de journalisation.

```
logging <syslog server ip>
logging trap debugs
```

   - Appliquez les commandes debug une par une et vérifiez l'utilisation du CPU après chacune d'elles.

```
show proc cpu hist
```

Avertissement : Si le CPU obtient une utilisation du CPU allant jusqu'à 70-80 %, le risque d'un impact sur les performances du service est considérablement augmenté. Par conséquent, n'activez pas de débogages supplémentaires si la GW atteint 60 %.

3. Activez ces débogages :

```
debug voip ccapi inout
debug ccsip mess
After you make the call and simulate the issue, stop the debugging:
```

4. Reproduisez le problème.
5. Désactivez les suivis.

```
#undebug all
```

6. Collectez les journaux.

```
term len 0
show ver
show run
show log
```

CUSPIDE

1. Activez les suivis SIP sur CUSP.

```
(cusp)> config
(cusp-config)> sip logging
(cusp)> trace enable
(cusp)> trace level debug component sip-wire
```

2. Reproduisez le problème.
3. Désactivez la connexion une fois que vous avez terminé.

Collecter les journaux

1. Configurez un utilisateur sur le CUSP (par exemple, test).
2. Ajoutez cette configuration à l'invite CUSP.

```
username <userid> create
username <userid> password <password>
username <userid> group pfs-privusers
```

3. Passez à l'adresse IP CUSP par FTP. Utilisez le nom d'utilisateur (test) et le mot de passe définis à l'étape précédente.
4. Remplacez les répertoires par /cusp/log/trace.
5. Obtenez le log_<nom de fichier>.

Définition des journaux de suivi et de collecte UCCE

Cisco recommande de définir des niveaux de suivi et de collecter les suivis via le Portique de structure de diagnostic ou les outils de CLI système.

Remarque : Pour plus d'informations sur Diagnostic Framework Portico et l'interface de ligne de commande du système, consultez le chapitre Diagnostic tools dans le document Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5(1).

Lorsque vous dépannez la plupart des scénarios UCCE, si le niveau de traces par défaut ne fournit pas suffisamment d'informations, définissez le niveau de traces sur 3 dans les composants requis (à quelques exceptions près).

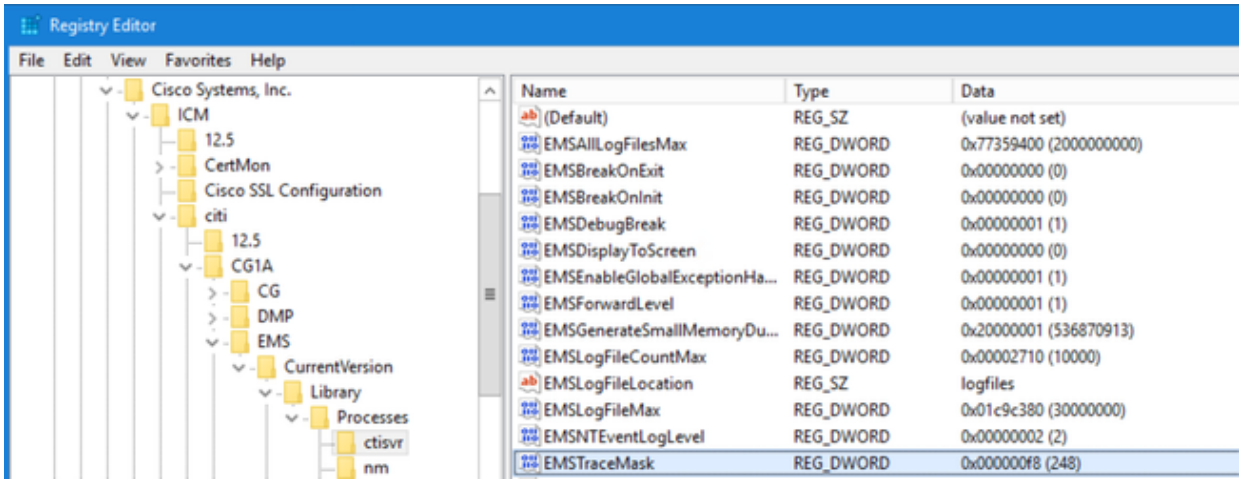
Remarque : Pour plus d'informations, consultez la section Trace Level sur le Guide de facilité de maintenance pour Cisco Unified ICM/Contact Center Enterprise, version 12.5(1).

Par exemple, si vous dépannez des problèmes de numérotation sortante, le niveau de suivi doit être défini sur le niveau 2 si le numéroteur est occupé.

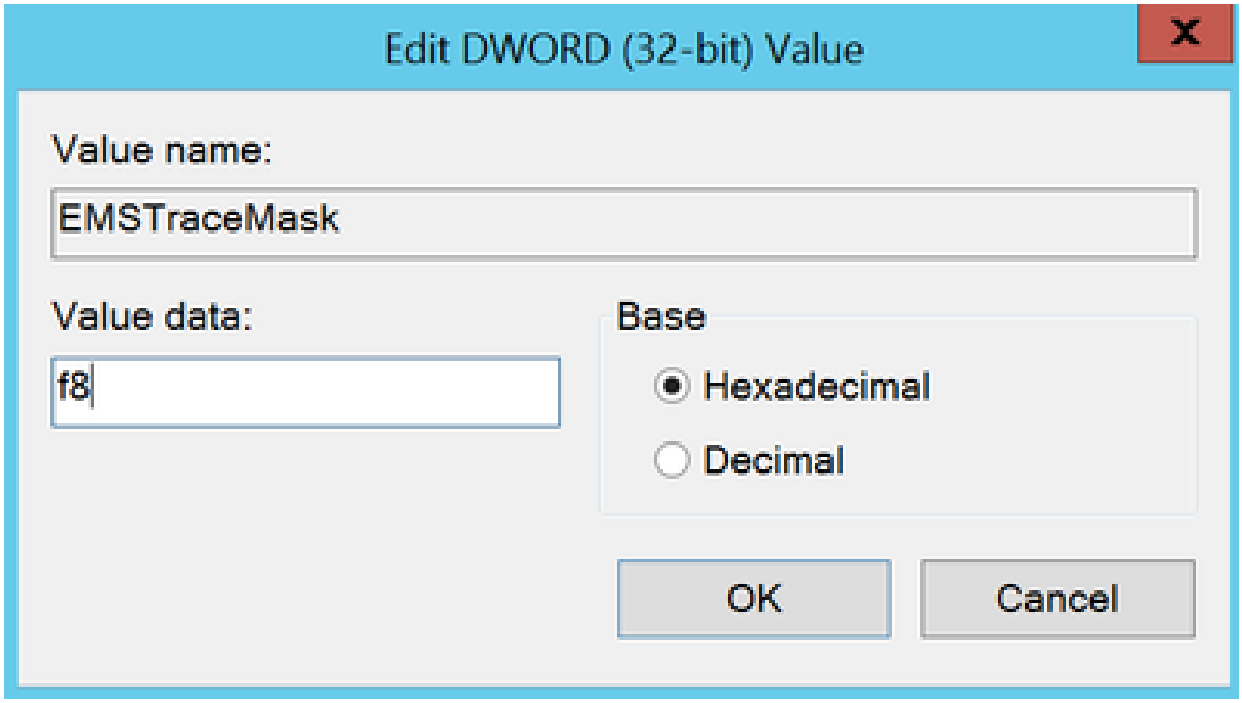
Pour CTISVR (CTISVR), les niveaux 2 et 3 ne définissent pas le niveau de registre exact recommandé par Cisco. Le registre de suivi recommandé pour CTISVR est 0XF8.

1. Dans la page PG de l'agent UCCE, ouvrez l'Éditeur du Registre (Regedit).

2. Accédez à HKLM\software\Cisco Systems, Inc\icm\<cust_inst>\CG1(a et b)\EMS\CurrentVersion\library\Processes\ctisvr.



3. Double-cliquez sur EMSTraceMask et définissez la valeur sur f8.

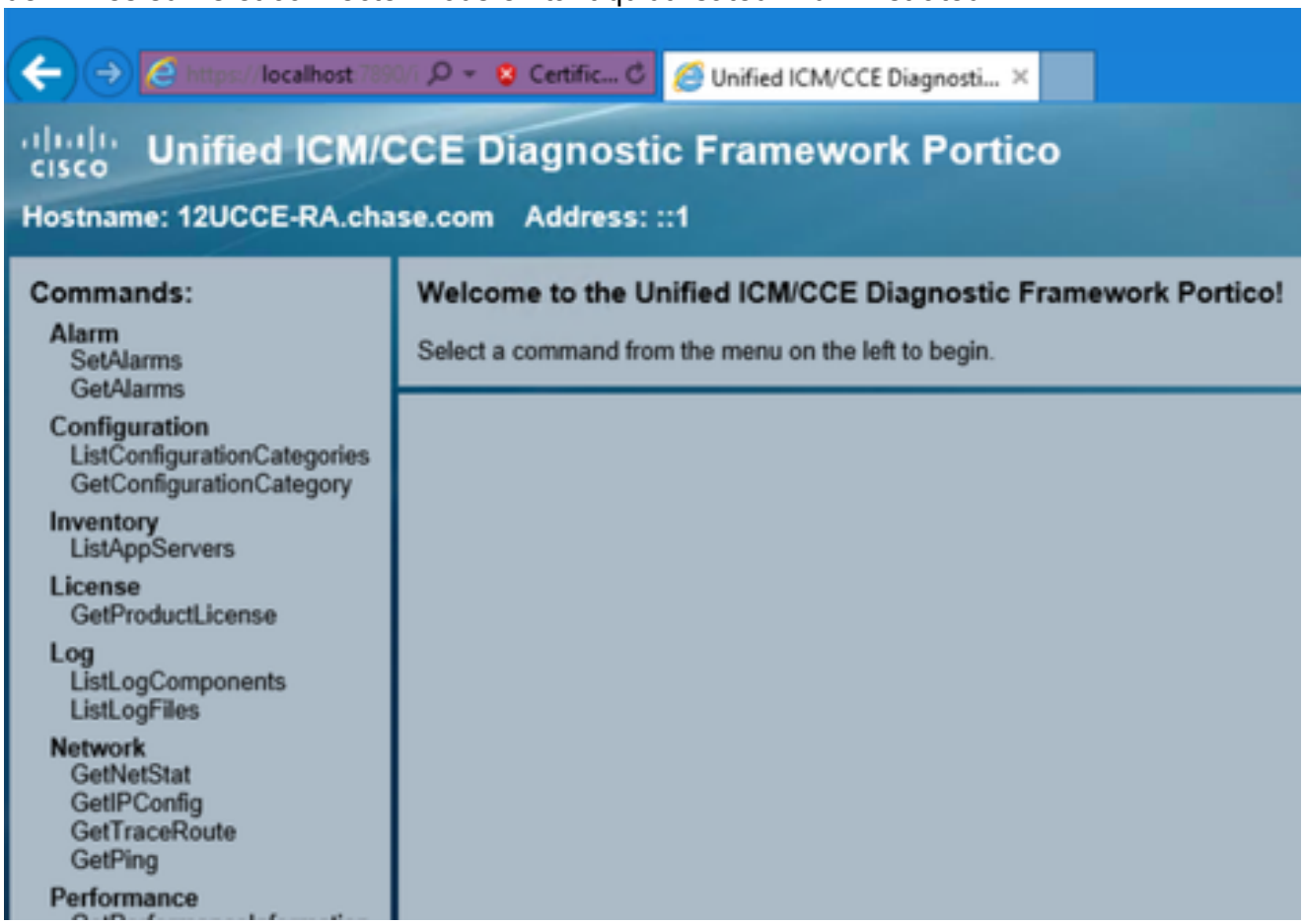


4. Cliquez sur Ok et fermez l'Éditeur du Registre. Il s'agit des étapes permettant de définir n'importe quel suivi de composant UCCE (le processus RTR est utilisé à titre d'exemple).

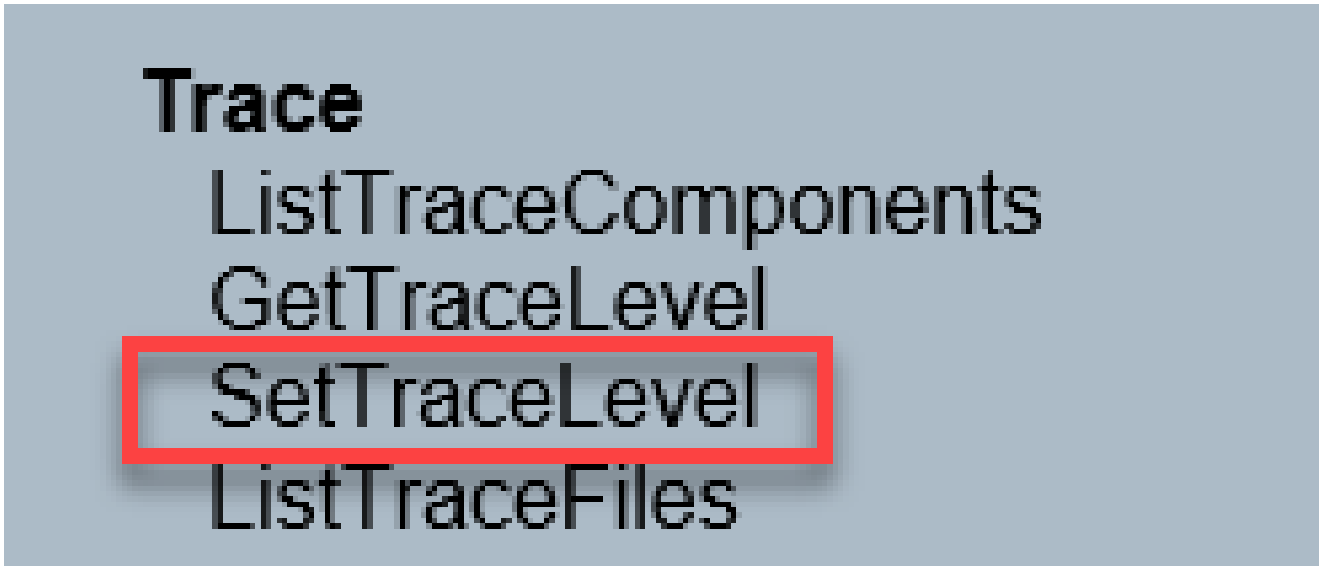
Définir le niveau de trace

1. Ouvrez le portlet Infrastructure de diagnostic à partir du serveur dont vous avez besoin pour

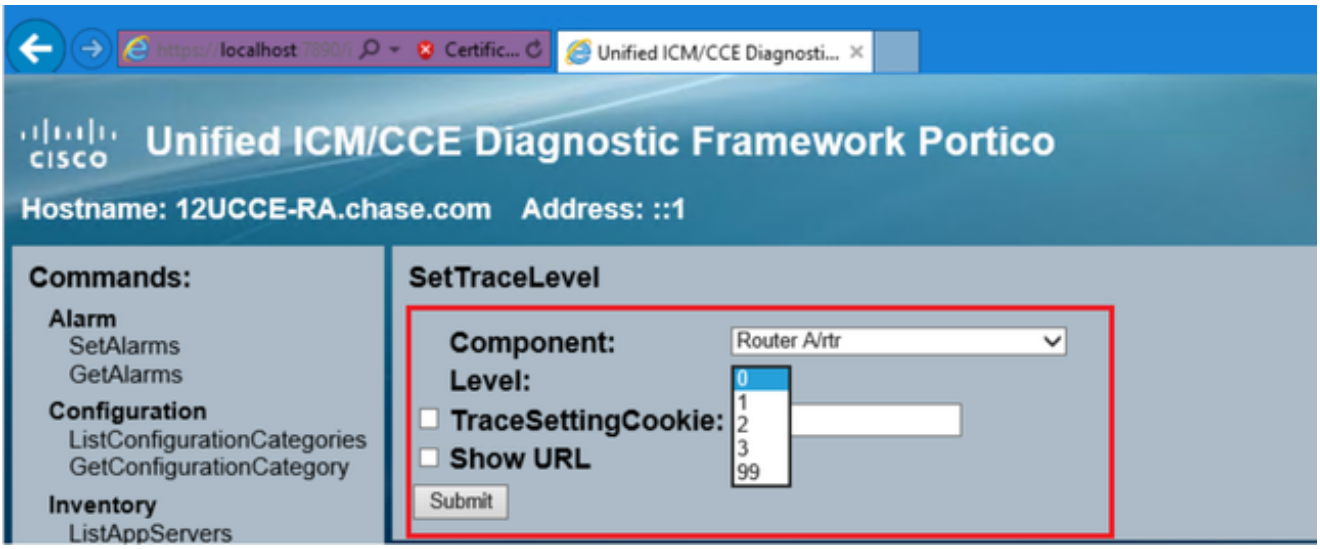
définir les suivis et connectez-vous en tant qu'utilisateur Administrateur.



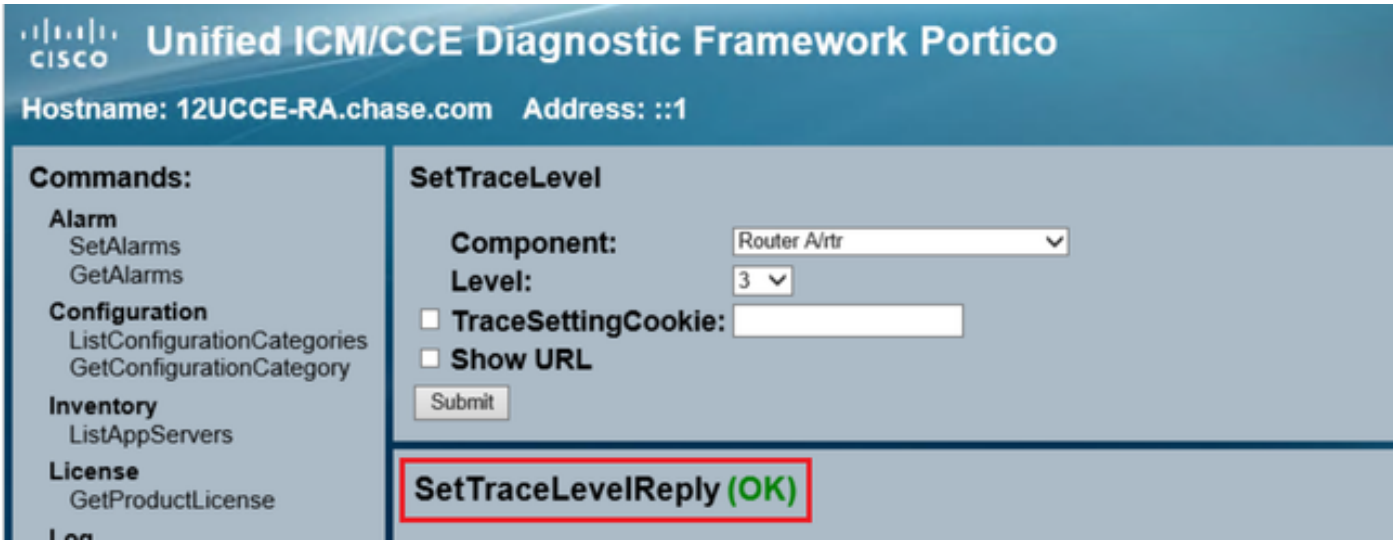
2. Dans la section Commands, accédez à Trace et sélectionnez SetTraceLevel.



3. Dans la fenêtre DéfinirNiveauTrace, sélectionnez le composant et le niveau.



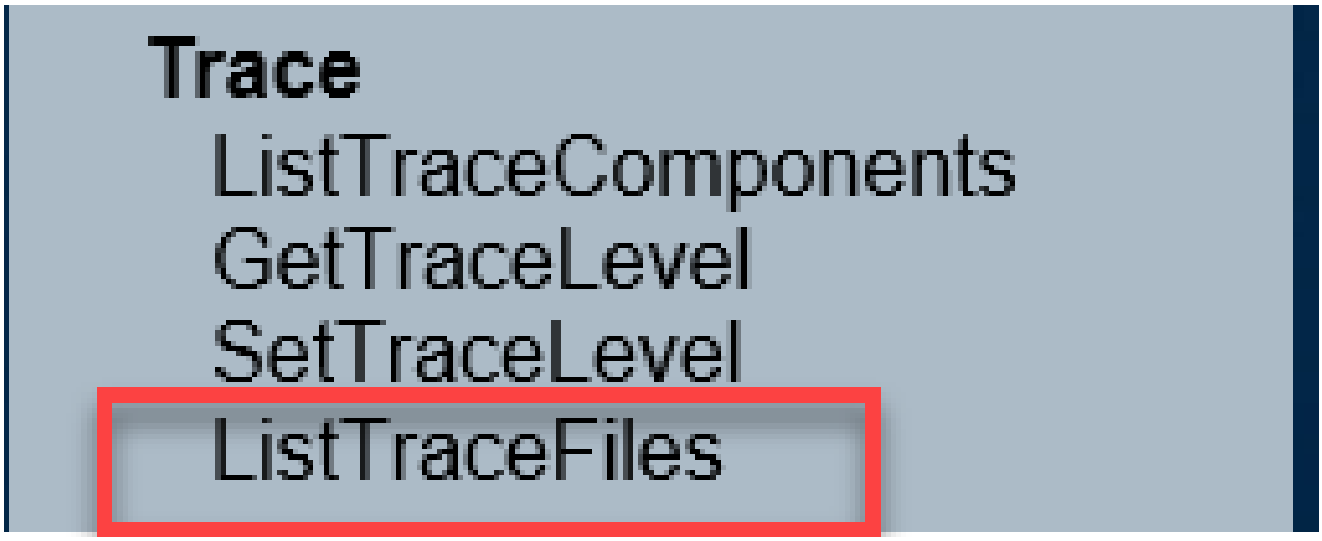
4. Cliquez sur Submit. Lorsque vous avez terminé, le message Ok s'affiche.



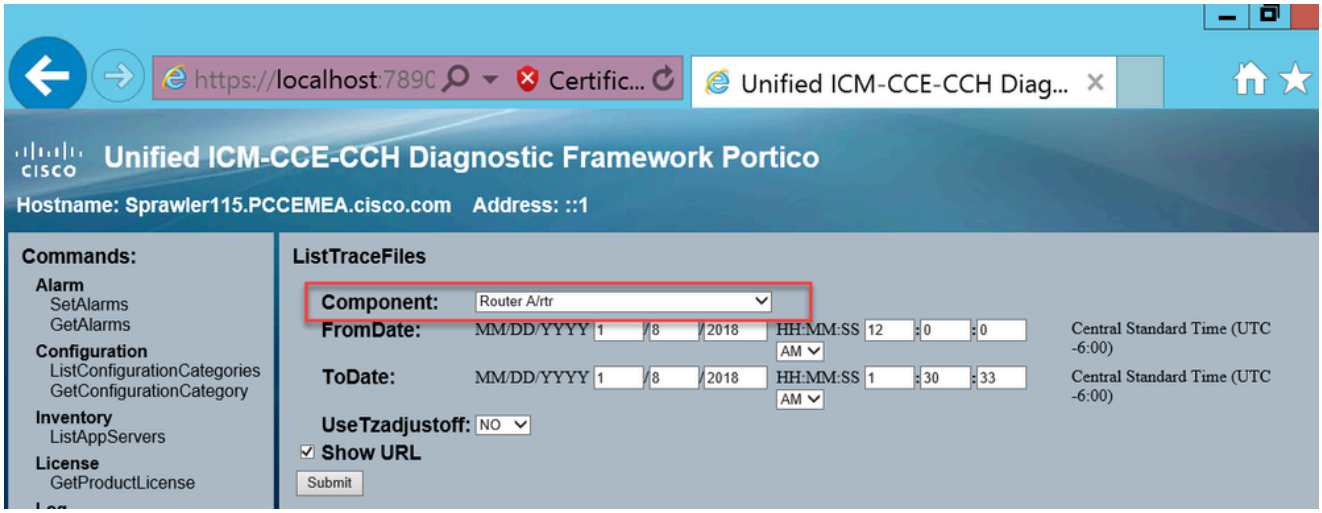
Avertissement : Définissez le niveau de suivi au niveau 3 lorsque vous tentez de reproduire le problème. Une fois le problème reproduit, définissez le niveau de trace sur default. Soyez particulièrement prudent lorsque vous définissez les suivis JTAPIGW, car les niveaux 2 et 3 définissent les suivis de bas niveau, ce qui peut avoir un impact sur les performances. Définissez le niveau 2 ou le niveau 3 dans le JTAPIGW en dehors de la période de production ou dans un environnement de laboratoire.

Collecte des journaux

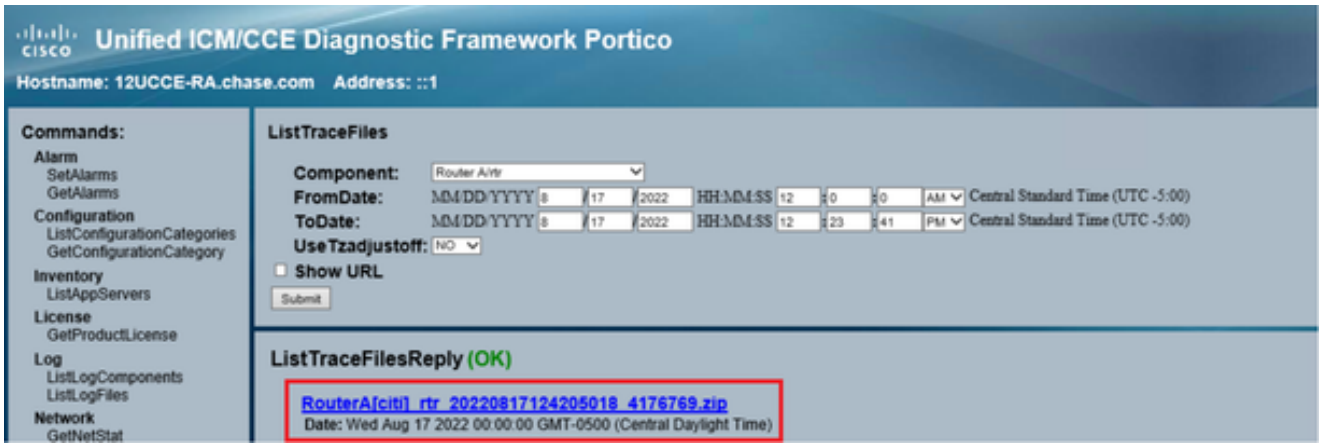
1. Dans le portlet Infrastructure de diagnostic, dans la section Commands, accédez à Trace et sélectionnez ListTraceFile.



2. Dans la fenêtre ListTraceFile, sélectionnez Component, FromDate et ToDate. Cochez la case Show URL, puis cliquez sur Submit.



3. Une fois la requête terminée, le message OK contenant le lien du fichier journal ZIP s'affiche.

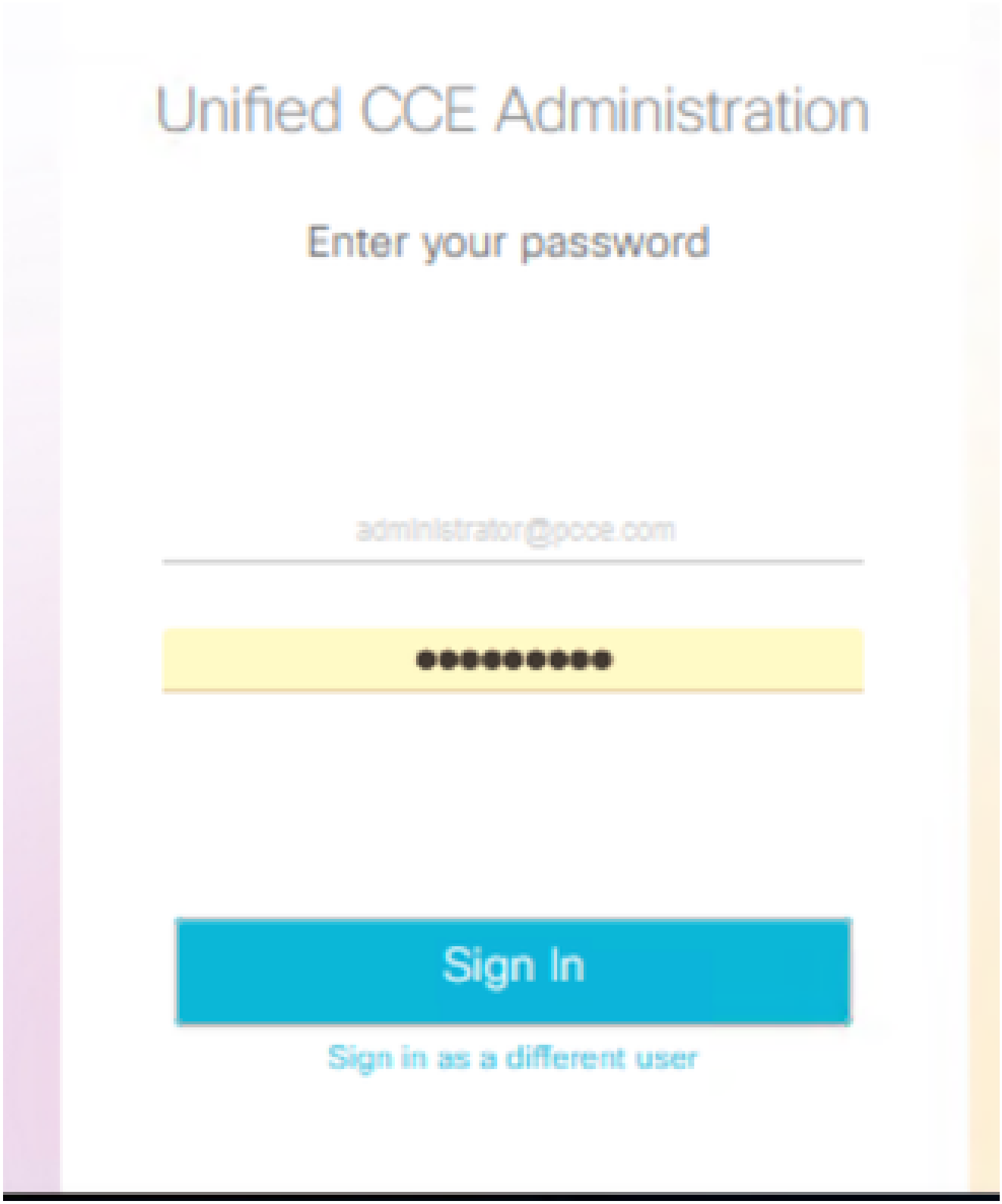


4. Cliquez sur le lien Fichier ZIP et Enregistrez le fichier à l'emplacement que vous choisissez.

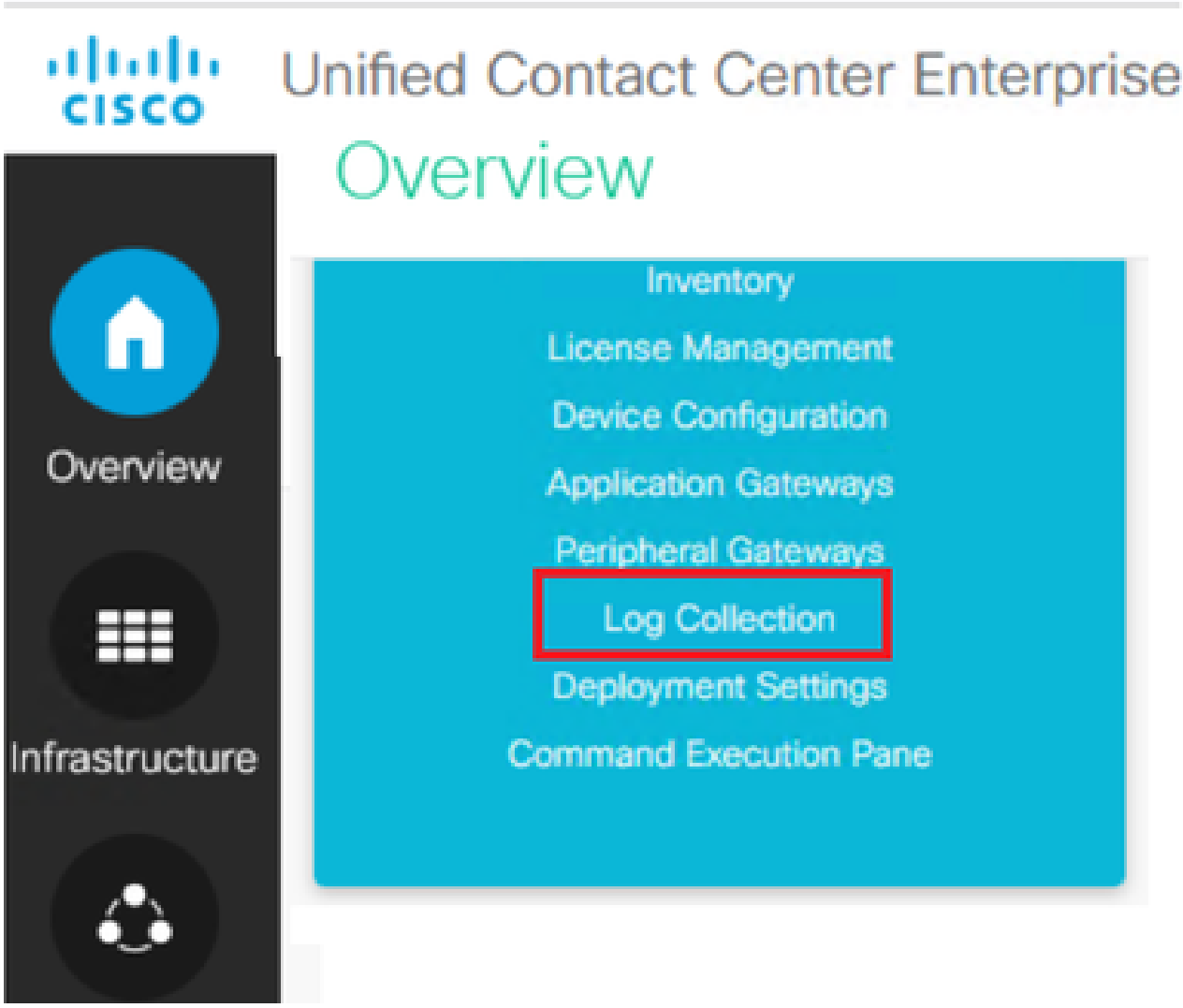
Définition des journaux PCCE de suivi et de collecte

PCCE dispose de son propre outil pour configurer les niveaux de suivi. Il ne s'applique pas à l'environnement UCCE dans lequel le portlet de cadre de diagnostic ou l'interface de ligne de commande du système sont les méthodes privilégiées pour activer et collecter les journaux.

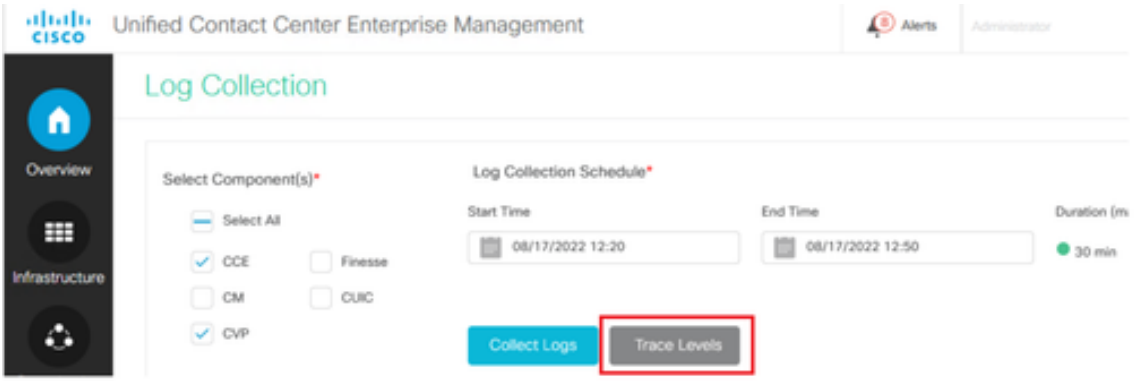
1. À partir du serveur PCCE AW, ouvrez l'outil Unified CCE Web Administration et connectez-vous au compte Administrateur.



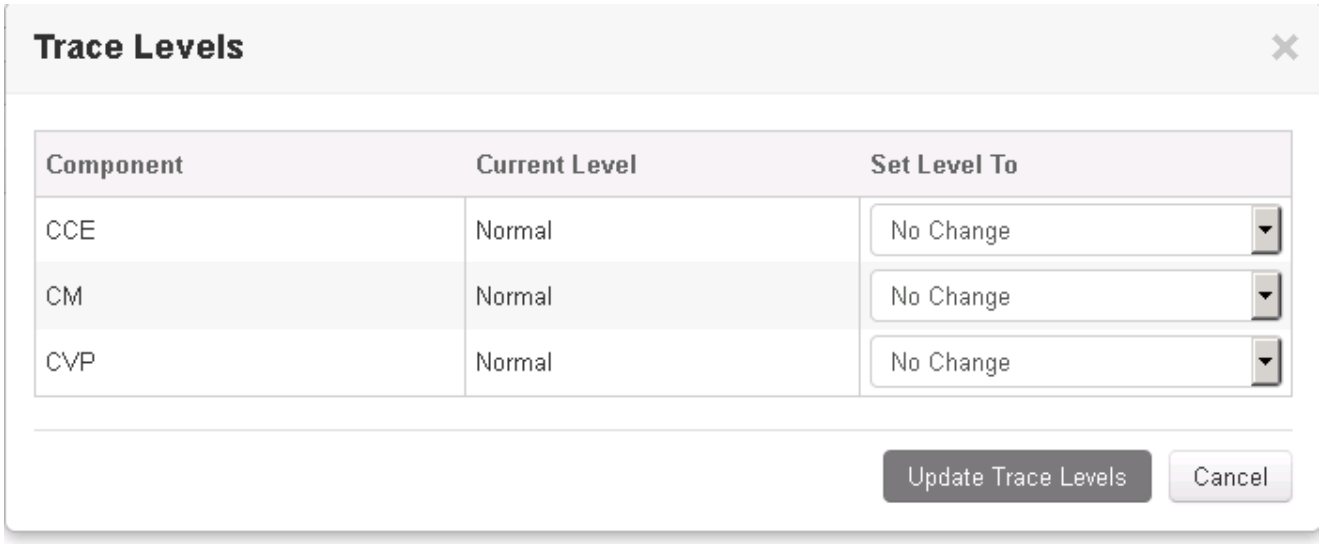
2. Accédez à Overview > Infrastructure Settings > Log Collection afin d'ouvrir la page Log Collection.



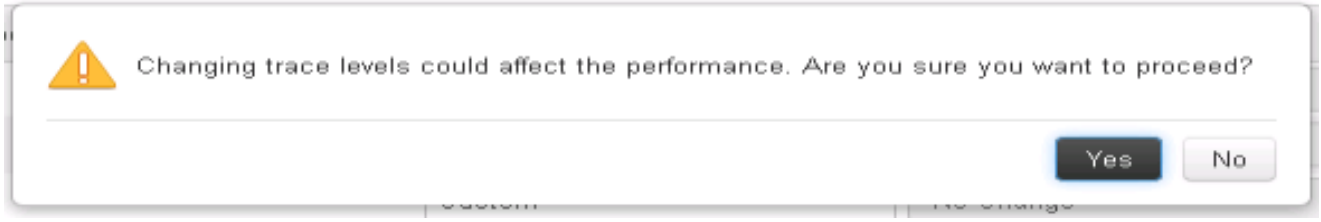
3. Sur la page Collecte des journaux, cliquez sur Niveaux de suivi pour ouvrir la boîte de dialogue Niveaux de suivi.



4. Définissez le niveau de suivi sur Détaillé sur CCE et laissez-le sur Aucune modification pour CM et CVP, puis cliquez sur Mettre à jour les niveaux de suivi.



5. Cliquez sur Yes pour accuser réception de l'avertissement.



6. Une fois le problème reproduit, ouvrez Unified CCE Administration et revenez à System > Log Collection.
7. Sélectionnez CCE et CVP dans le volet Composants.
8. Sélectionnez la durée de collecte du journal appropriée (la valeur par défaut est les 30 dernières minutes).
9. Cliquez sur Collecter les journaux et sur Oui pour afficher l'avertissement de la boîte de dialogue. La collection de journaux démarre. Attendez quelques minutes avant que ça ne finisse.



10. Une fois terminé, cliquez sur le bouton Download dans la colonne Actions pour télécharger un fichier zippé contenant tous les journaux. Enregistrez le fichier zip à l'emplacement approprié.

Définition des journaux CUIC/Live Data/IDS de suivi et de collecte

Télécharger les journaux avec SSH

1. Connectez-vous à la ligne de commande SSH (CLI) de CUIC, LD et IDS.

2. Exécutez la commande afin de collecter les journaux associés à CUIC.

file get activelog /cuic/logs/cuic/*.* recurs compress reltime hours 1

file get activelog /cuic/logs/cuicsrvr/*.* recurs compress reltime hours 1

file get activelog tomcat/logs/*.* recurs compress

3. Exécutez la commande afin de collecter les journaux associés à LD.

file get activelog livedata/logs/*.*

4. Exécutez la commande afin de collecter les journaux associés aux IDs.

file get activelog ids/log/*.* recurs compress reltime days 1

5. Ces journaux sont stockés sur le chemin du serveur SFTP : <adresse IP>\<horodatage>\active_nnn.tgz , où nnn est l'horodatage au format long.

Télécharger les journaux avec RTMT

1. Téléchargez RTMT depuis la page OAMP. Connectez-vous à https://<ADRESSE D'HÔTE>/oamp où ADRESSE D'HÔTE est l'adresse IP du serveur.

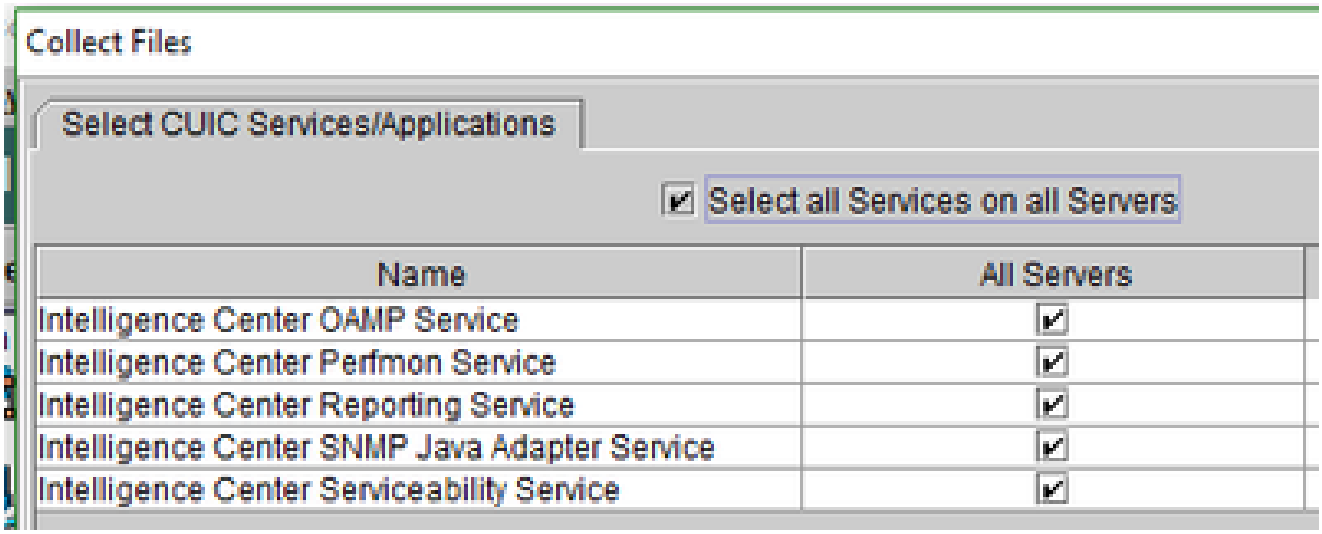
2. Naviguez jusqu'à Tools > RTMT plugin download. Téléchargez et installez le plugin.

3. Lancez RTMT et connectez-vous au serveur avec les informations d'identification admin.

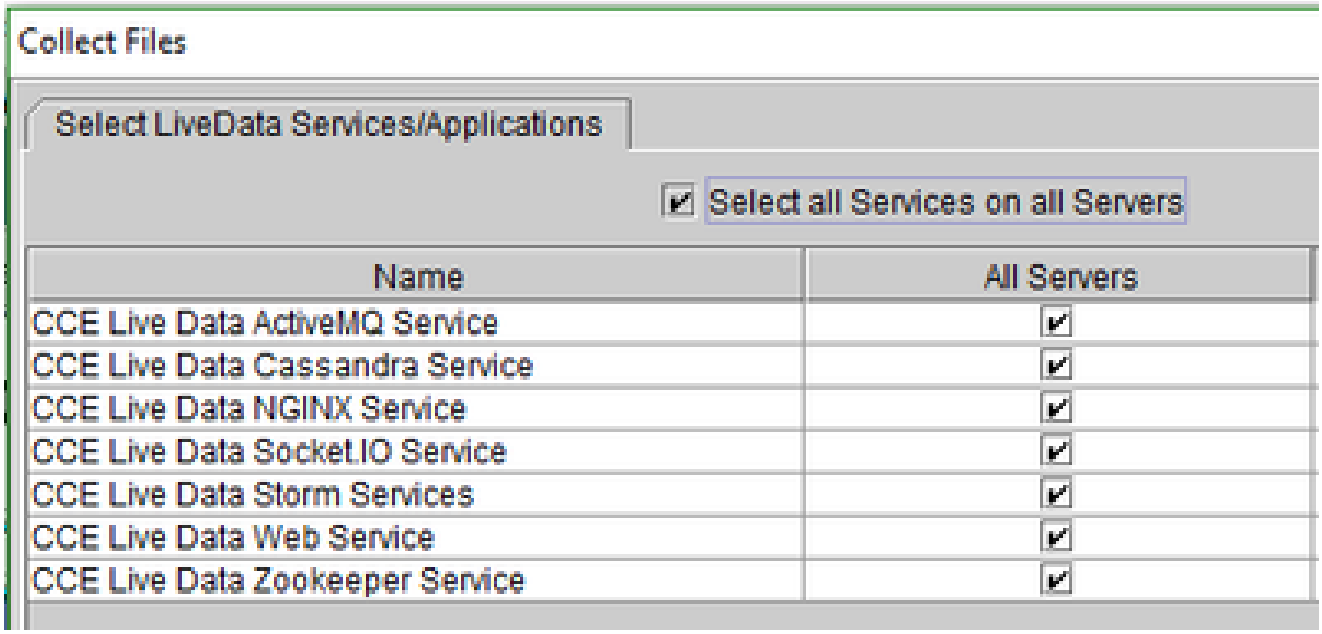
4. Double-cliquez sur Trace and Log Central puis double-cliquez sur Collecter les fichiers.

5. Vous pouvez voir ces onglets pour les services spécifiques. Vous devez sélectionner tous les services/serveurs pour CUIC, LD et IDS.

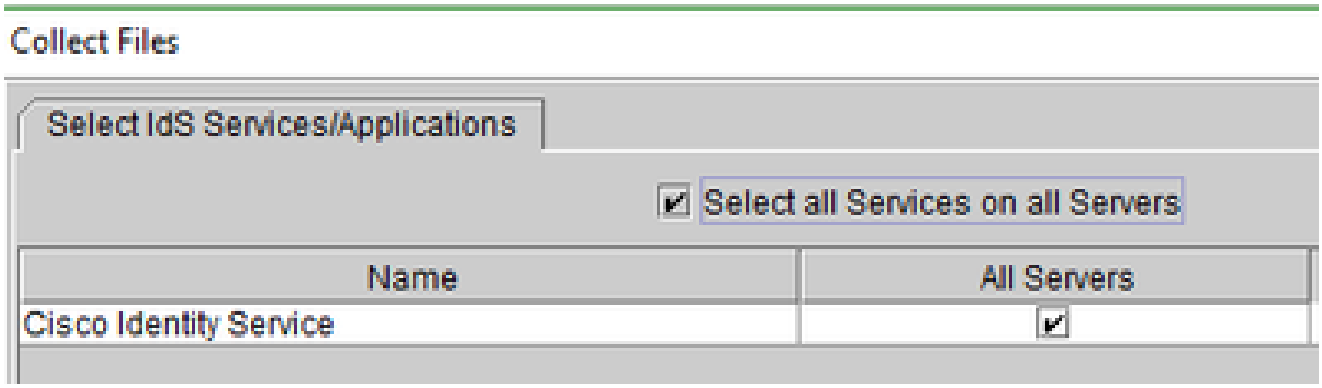
   Pour CUIC :



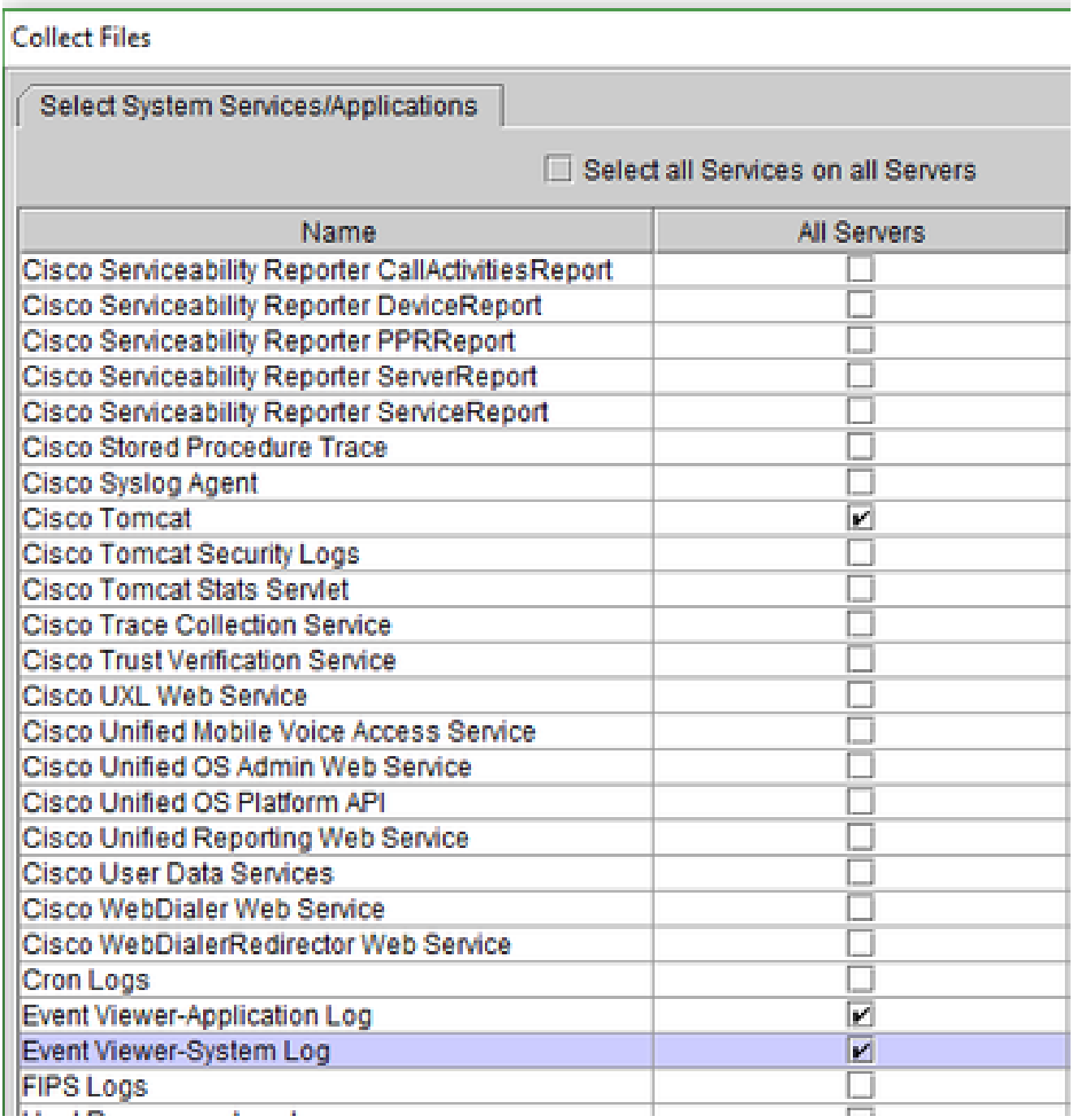
   Pour LD :



Pour IDS :



Pour les services de la plate-forme, il est généralement conseillé de sélectionner les journaux **Tomcat** et **Event** Viewer :

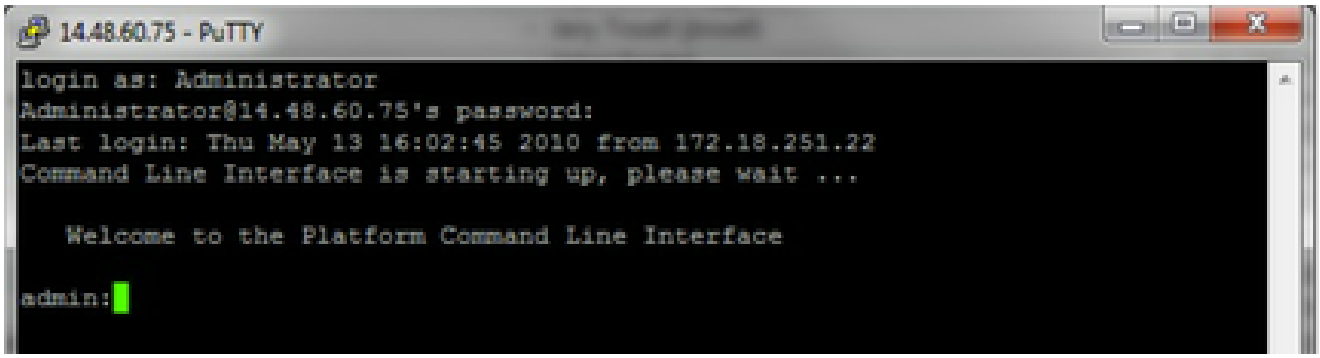


6. Sélectionnez la date et l'heure ainsi que le dossier de destination afin d'enregistrer les journaux.

Capture de paquets sur VoS (Finesse, CUIC, VVB)

1. Démarrage de la capture

   Pour démarrer la capture, établissez une session SSH pour que le serveur VOS s'authentifie avec le compte d'administrateur de plate-forme.

2. 

1 bis. Syntaxe de commande

La commande est **utils network capture**et la syntaxe est la suivante :

<#root>

```
    Syntax:

utils network capture

 [options]
options  optional
page,numeric,file fname,count num,size bytes,src addr,dest addr,port
num,host protocol addr
options are:
page
- pause output
numeric               - show hosts as dotted IP
addresses
file fname            - output the information to a file

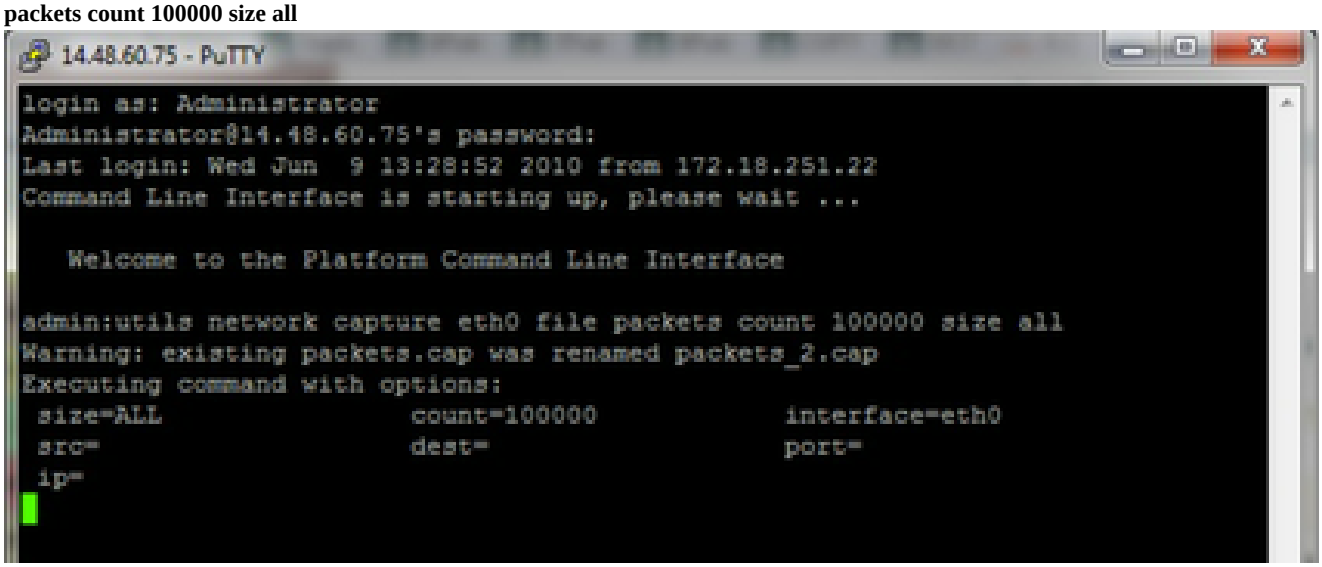
Note: The file is saved in platform/cli/fname.cap

fname should not contain the "." character
count num             - a
count of the number of packets to capture
    Note: The maximum count
for the screen is 1000, for a file is 100000
size bytes            -
the number of bytes of the packet to capture
    Note: The maximum
number of bytes for the screen is 128
          For a file it can be
any number or ALL
src addr              - the source address of the
packet as a host name or IPV4 address
dest addr             - the
destination address of the packet as a host name or IPV4 address
port
num              - the port number of the packet (either src or dest)
host
protocol addr    - the protocol should be one of the following:
ip/arp/rarp/all. The host address of the packet as a host name or IPV4
address. This option  will display all packets to and from that address.
```

```
Note: If "host" is provided, do not provide "src" or "dest"
```

1 ter. Capturer tous les trafics

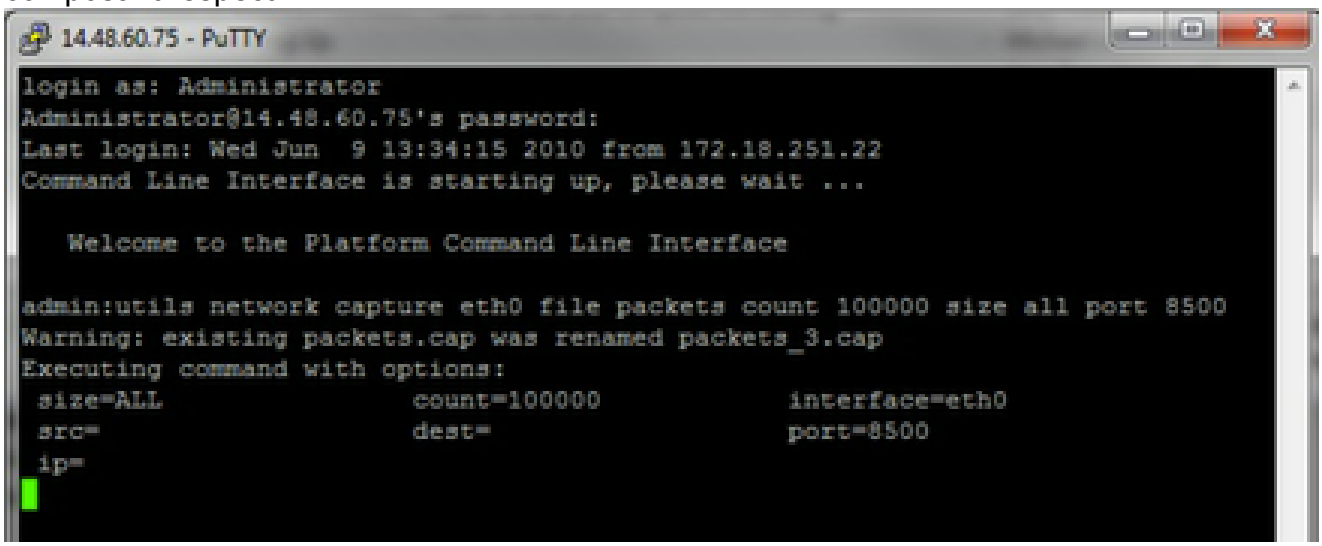
Pour une capture typique, on peut collecter TOUS les paquets de TOUTES les tailles de et vers TOUTES les adresses dans un fichier de capture appelé packets.cap. Pour ce faire, exécutez simplement sur l'interface de ligne de commande admin **utils network capture eth0 file packets count 100000 size all**



1 quater. Capture basée sur le numéro de port

Afin de résoudre un problème de communication avec le gestionnaire de cluster, il peut être souhaitable d'utiliser l'option de port pour effectuer une capture en fonction d'un port spécifique (8500).

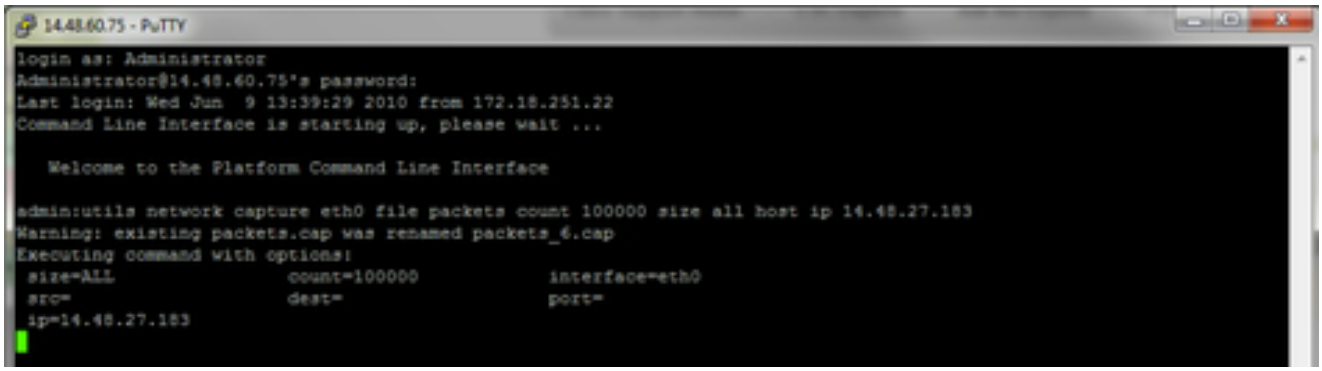
Pour plus d'informations sur les services qui nécessitent des communications sur chaque port, référez-vous au Guide d'utilisation des ports TCP et UDP pour la version applicable du composant respectif.



1 quinquies. Capture basée sur l’hôte

Pour résoudre un problème avec VOS et un hôte particulier, il peut être nécessaire d'utiliser l'option « host » pour filtrer le trafic en provenance et à destination d'un hôte particulier.

Il peut également être nécessaire d'exclure un hôte particulier, dans ce cas utilisez un "!" devant l'IP. Un exemple de ceci serait : **utils network capture eth0 file packets count 100000 size all host ip !10.1.1.1**

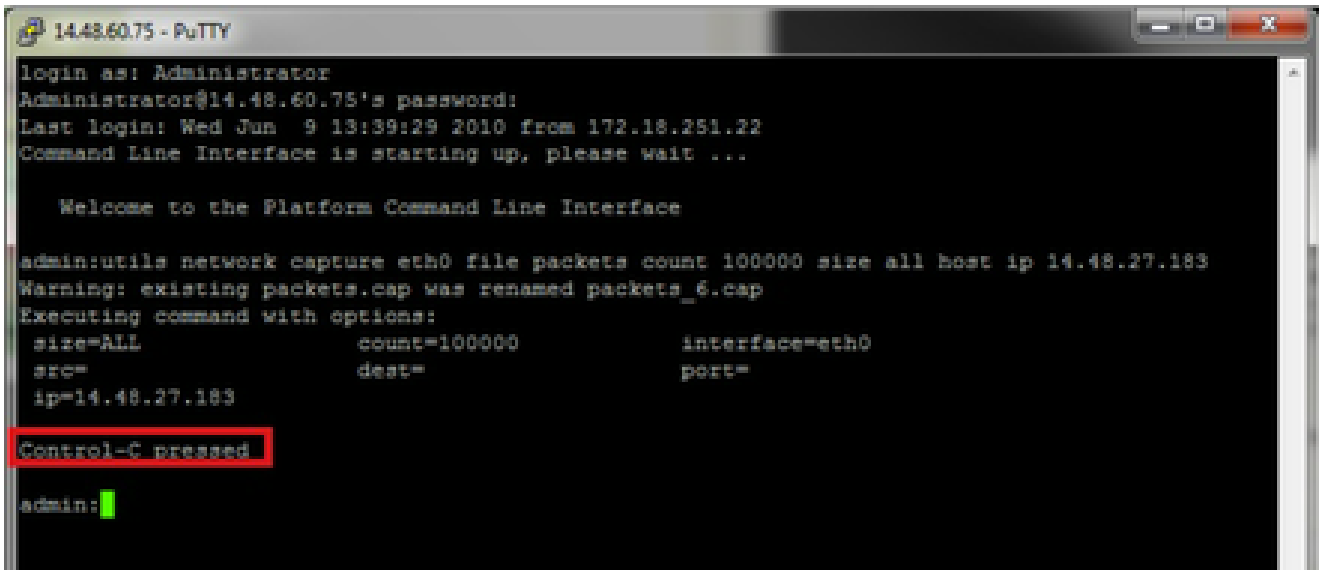


3. Reproduire le symptôme du problème

   Pendant que la capture a commencé à reproduire le symptôme ou la condition du problème de sorte que les paquets nécessaires sont inclus dans la capture. Si le problème est intermittent, il peut être nécessaire d'exécuter la capture pendant une période prolongée. Si la capture se termine, c'est parce que la mémoire tampon est remplie. Redémarrez la capture et la capture précédente est automatiquement renommée afin de ne pas la perdre. Si une capture est nécessaire pendant une période prolongée, utilisez une session de surveillance sur un commutateur pour effectuer la capture au niveau du réseau.

4. Arrêter la capture

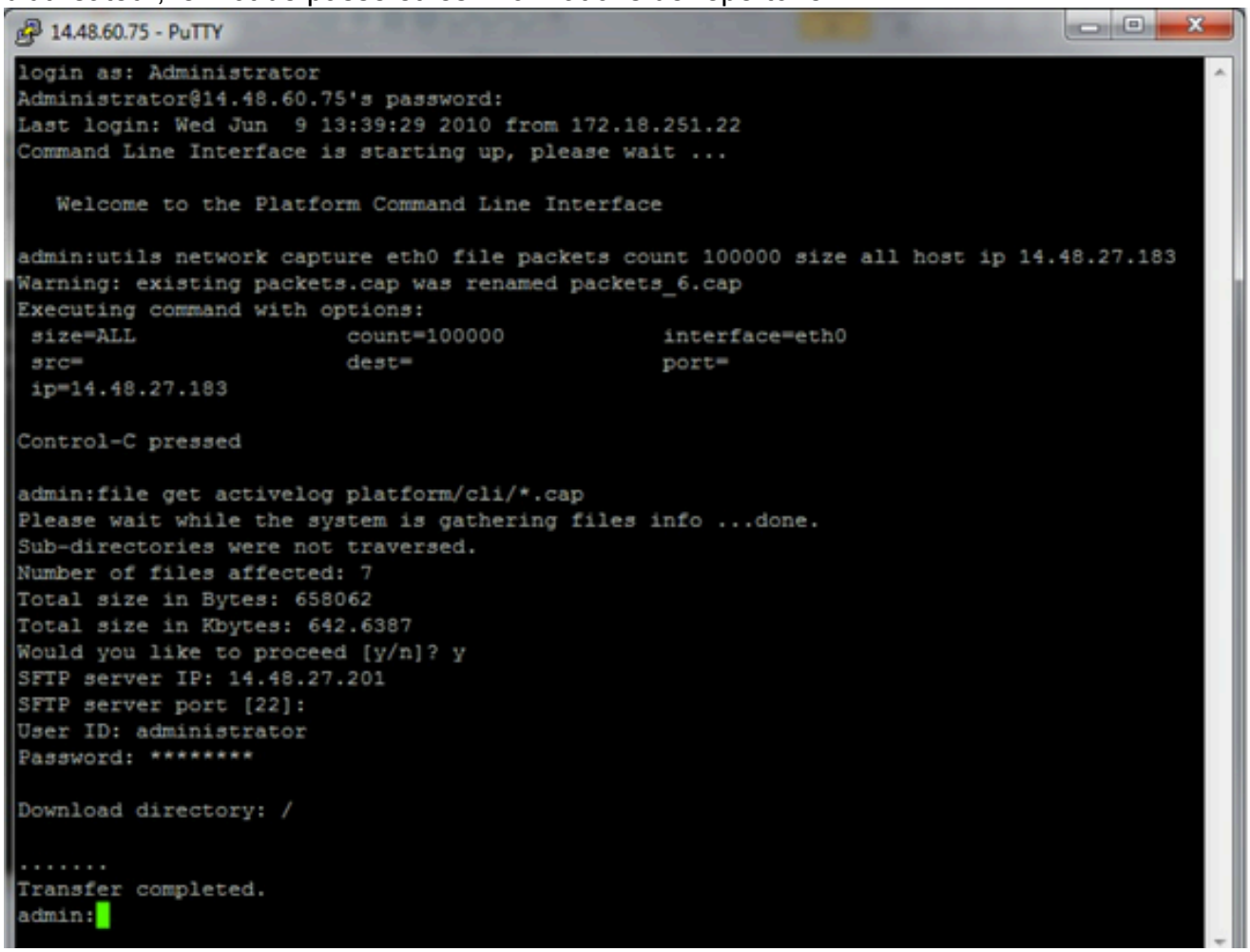
   Pour arrêter la capture, maintenez la touche Ctrl enfoncée et appuyez sur C du clavier. Cela entraîne la fin du processus de capture et aucun nouveau paquet n'est ajouté au vidage de capture.

5. 

Une fois cette opération terminée, un fichier de capture est stocké sur le serveur à l'emplacement « activelog platform/cli/ »

6. Collecter la capture à partir du serveur
   Les fichiers de capture sont stockés sur la plate-forme/l'interface de ligne de commande active du serveur. Vous pouvez transférer les fichiers via l'interface de ligne de commande vers un serveur SFTP ou vers l'ordinateur local à l'aide du RTMT.

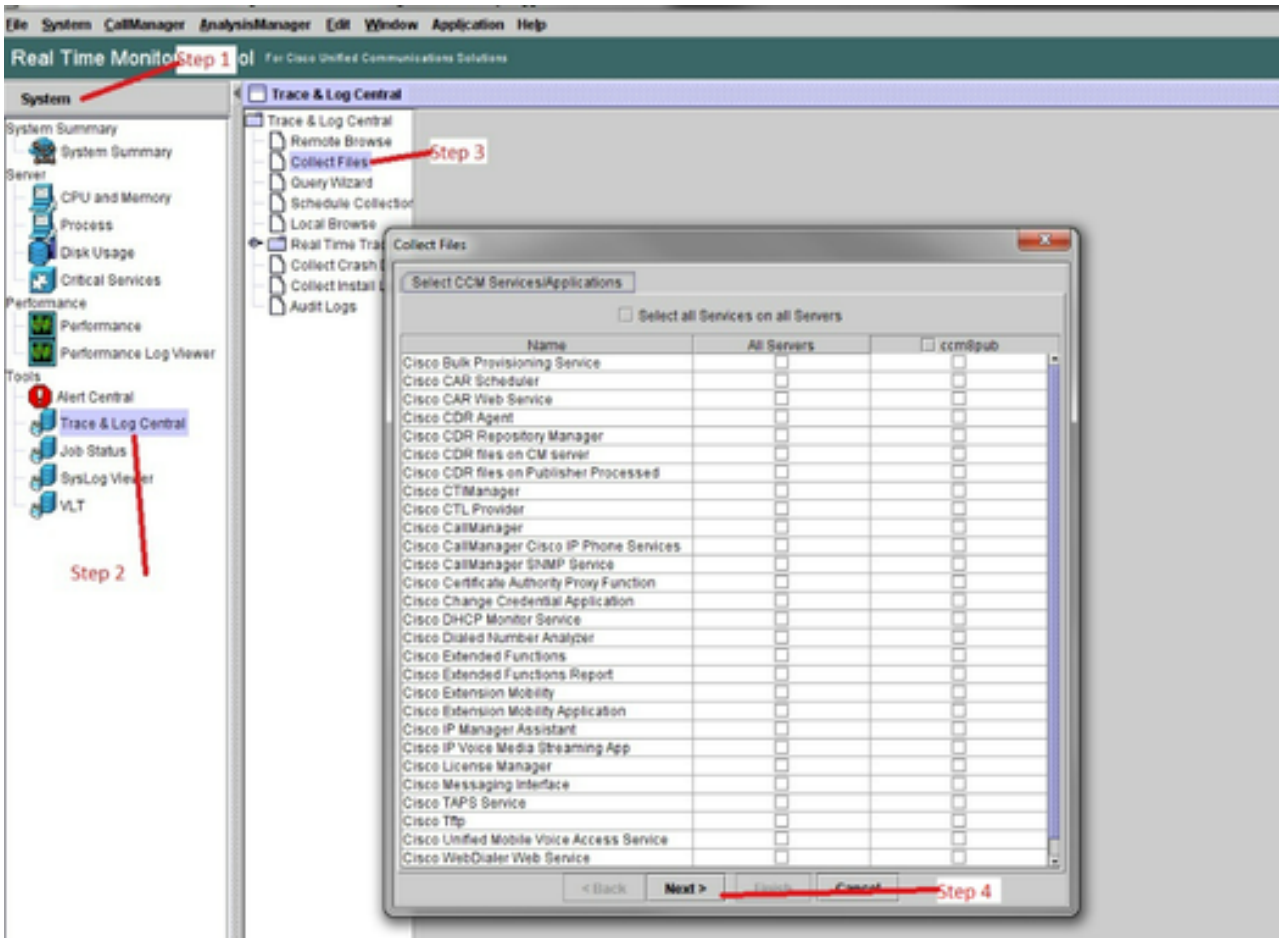
   4 bis. Transférer le fichier de capture via l'interface de ligne de commande vers un serveur SFTP
   Utilisez la commande **file get activelog platform/cli/packets.cap** pour collecter le fichier packets.cap sur le serveur SFTP.
   Vous pouvez également collecter tous les fichiers .cap stockés sur le serveur et utiliser le fichier get activelog platform/cli/*.cap.
   Enfin, indiquez l'adresse IP/le nom de domaine complet du serveur SFTP, le port, le nom d'utilisateur, le mot de passe et les informations de répertoire :



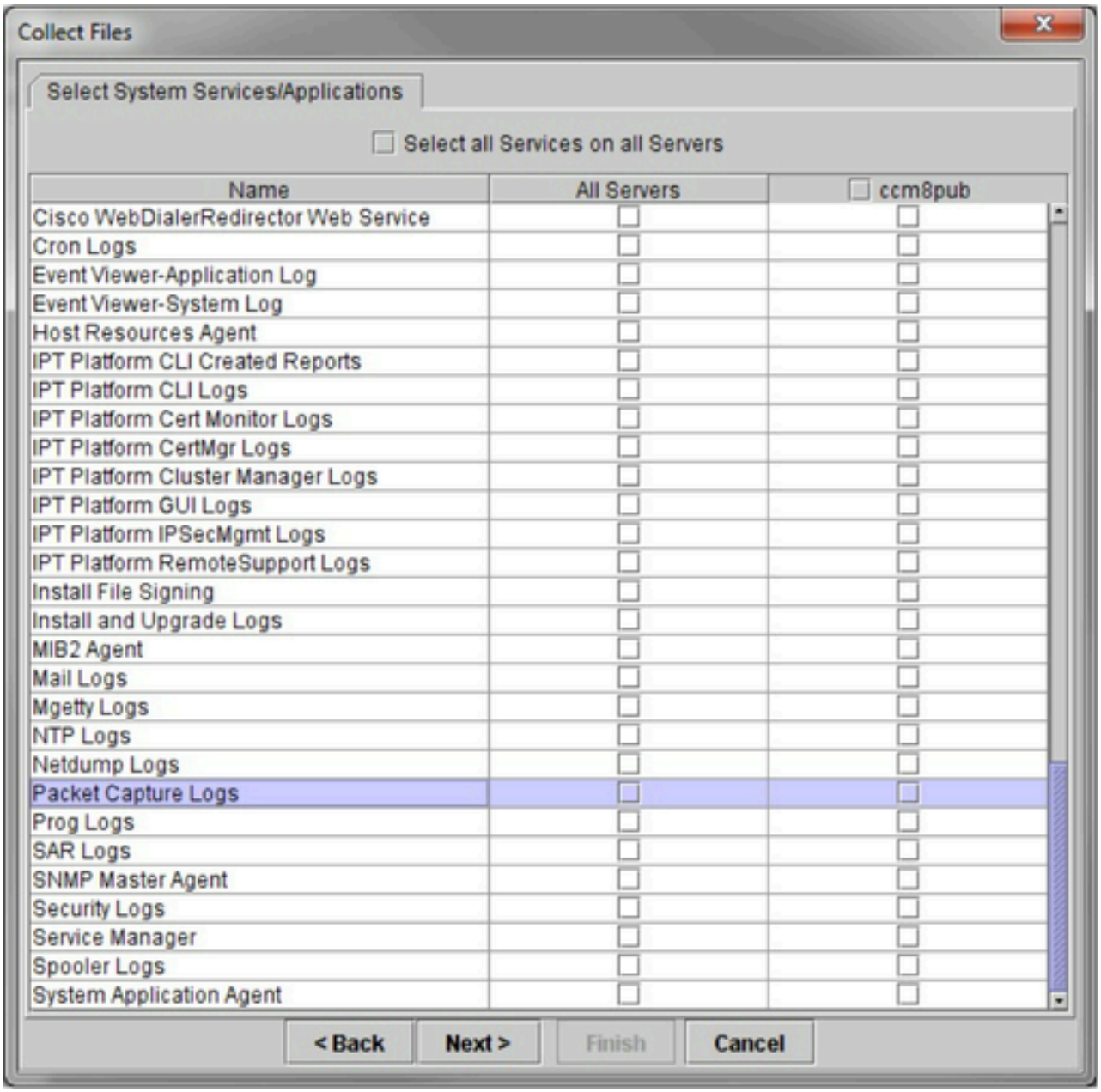
   L'interface de ligne de commande indique la réussite ou l'échec du transfert de fichiers vers le serveur SFTP.

4 ter. Utilisez RTMT pour transférer un fichier de capture vers un PC local.
Lancez RTMT. S'il n'est pas installé sur le PC local, installez la version appropriée à partir de la page Administration de VOS, puis accédez au menu Applications > Plugins. Cliquez sur System, puis sur Trace & Log Central, puis double-cliquez sur Collect Files. Cliquez sur Next

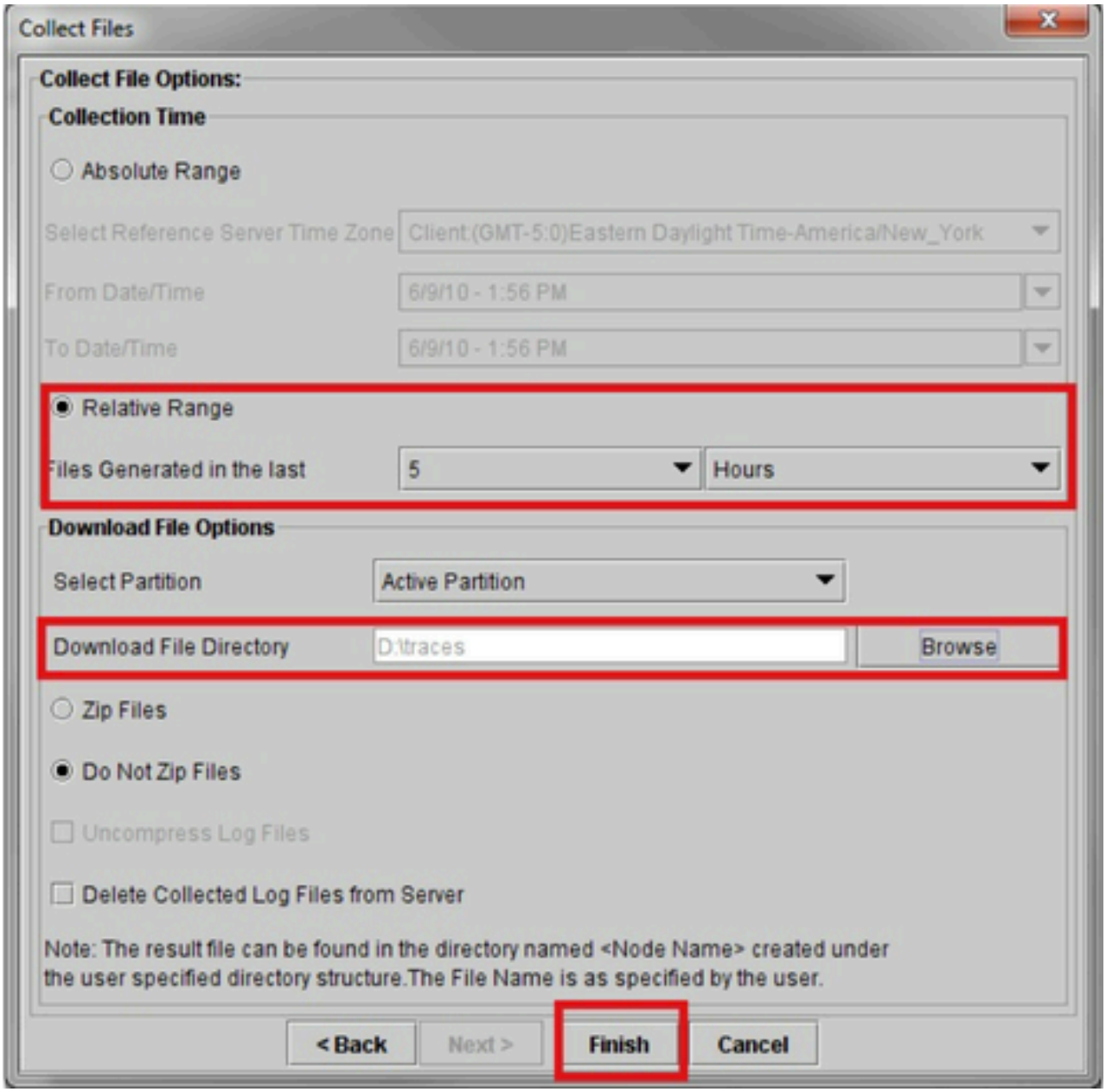
dans le premier menu.



Dans le deuxième menu, cochez la case Packet Capture Logs sur le serveur sur lequel la capture a été effectuée, puis cliquez sur Next.



Dans l'écran final, choisissez une plage temporelle lors de la capture et un répertoire de téléchargement sur le PC local.



RTMT ferme cette fenêtre et collecte le fichier et le stocke sur le PC local à l'emplacement spécifié.

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.