Configuration des suivis et collecte des journaux UCCE

Table des matières

Introduction

Ce document décrit comment définir des suivis dans Cisco UCCE, Finesse, Customer Voice Portal (CVP), UCCE Outbound Dialer et les passerelles Cisco.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Cisco Unified Contact Center Enterprise (UCCE)
- Package Contact Center Enterprise (PCCE)
- Cisco Finesse
- Portail vocal client Cisco (CVP)
- Navigateur vocal virtualisé Cisco (CVVB)
- Cisco Unified Border Element (CUBE)
- 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 11.5
- Serveur CVP 11.5
- Unified Contact Center Enterprise (UCCE) 11.5

- Navigateur vocal virtualisé Cisco 11.5

Ce document décrit comment définir des suivis dans Cisco Unified Contact Center Enterprise (UCCE), Cisco Finesse, Cisco Customer Voice Portal (CVP), Cisco UCCE Outbound Dialer et les passerelles Cisco.

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€™incidence possible des commandes.

Paramètres de suivi et finesse de la collecte des journaux

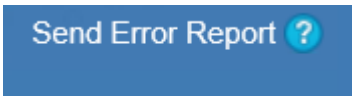
Client Finesse

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

Option 1 : Collectez les journaux du client avec le rapport d'erreurs d'envoi.

Étape 1. Connectez un agent.

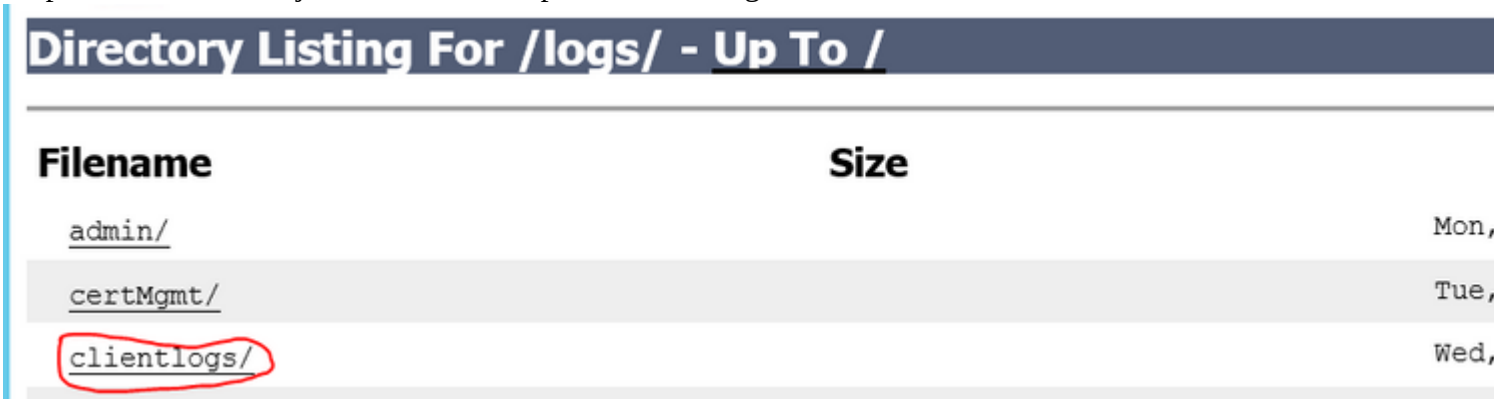
Étape 2. Si un agent rencontre un problème au cours d'un appel ou d'un événement multimédia, demandez à l'agent de cliquer sur le lien Envoyer un rapport d'erreur dans le coin inférieur droit du bureau Finesse.



Étape 3. L'agent voit le message Journaux envoyés avec succès.

Étape 4. Les journaux du client sont envoyés au serveur Finesse. Accédez à https://x.x.x.x/finesse/logs et connectez-vous avec un compte d'administration.

Étape 5. Collectez les journaux dans le répertoire clientlogs/.

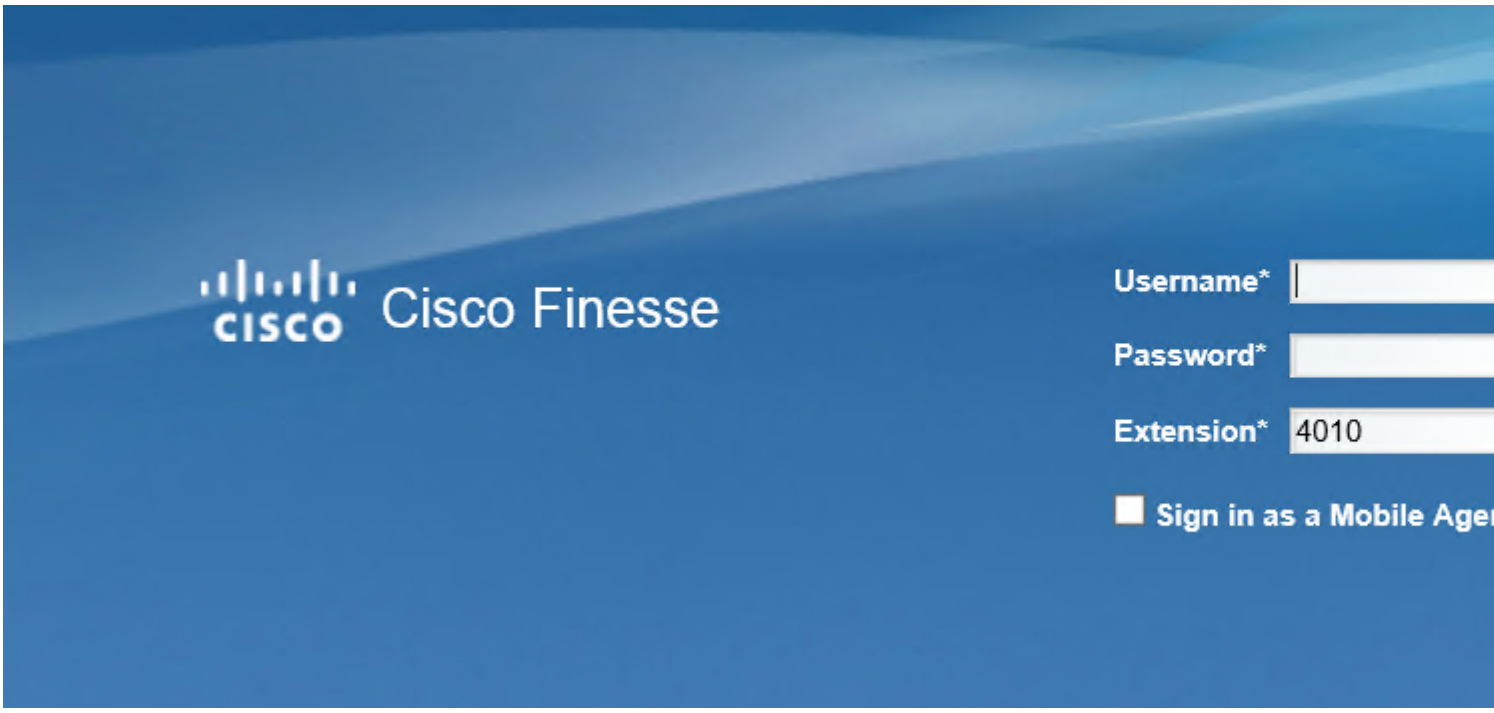


Option 2 : définition de la journalisation permanente

Étape 1. Accédez à https://x.x.x.x:8445/desktop/locallog.

Étape 2. Cliquez sur Connexion avec connexion permanente.

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



Étape 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 https://x.x.x.x:8445/desktop/locallog et copiez le contenu dans un fichier texte. Enregistrez le fichier pour une analyse plus approfondie.

.

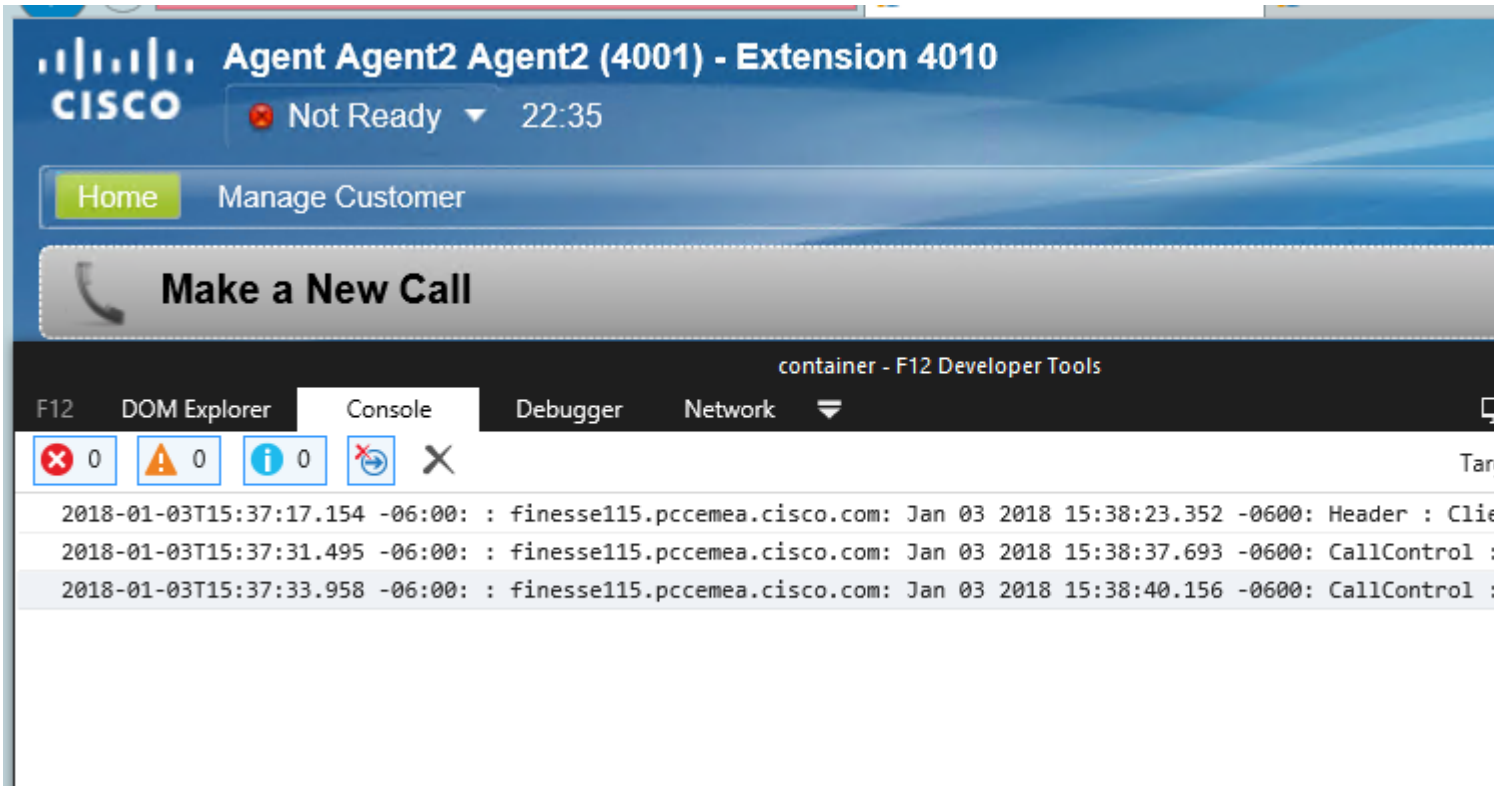
Remarque : il existe une mise en garde liée à la consignation permanente. Une fois la journalisation permanente activée, les informations ne sont pas envoyées aux journaux de stockage local. ID de bogue Cisco CSCvf93030 - La journalisation permanente ne parvient pas à capturer les journaux. Finesse 11.5(1) ES-2 et ultérieures. Pour plus d'informations sur cette mise en garde et sur les étapes à suivre pour y remédier, consultez le site

Option 3 : console du navigateur Web

Étape 1. Une fois qu'un agent se connecte, appuyez sur F12 pour ouvrir la console du navigateur.

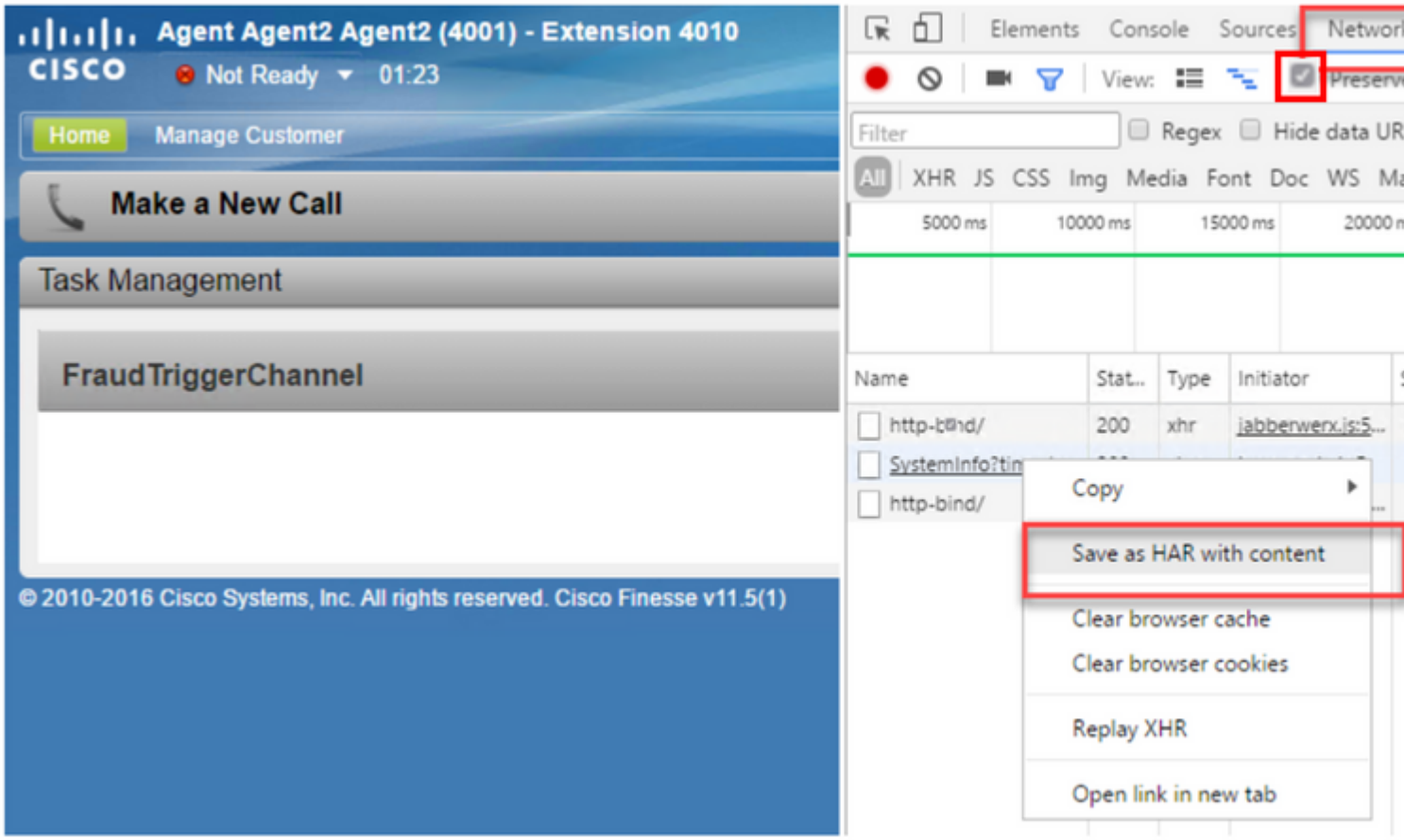
Étape 2. Sélectionnez l'onglet Console.

Étape 3. Vérifiez les erreurs sur la console du navigateur. Copiez le contenu dans un fichier texte et enregistrez-le.



Étape 4. Sélectionnez l'onglet Réseau et activez l'option Conserver le journal.

Étape 5. Cliquez avec le bouton droit sur l'un des événements de nom de réseau et sélectionnez Enregistrer en tant que HAR avec le contenu.



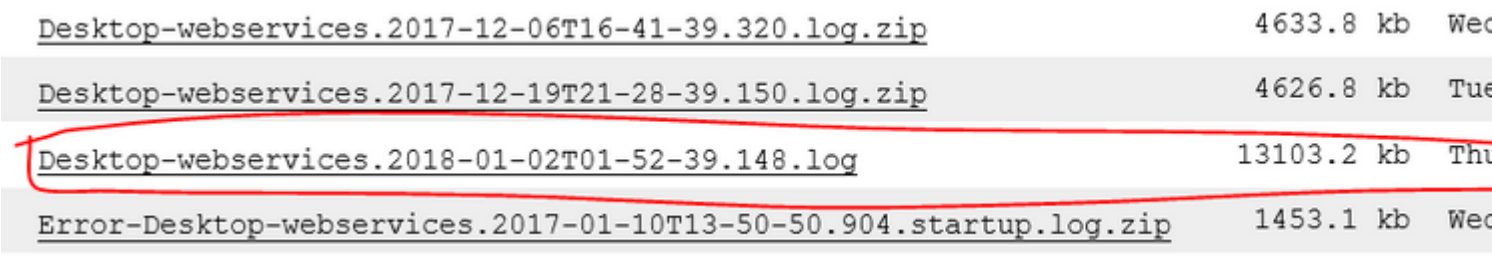
Serveur Finesse

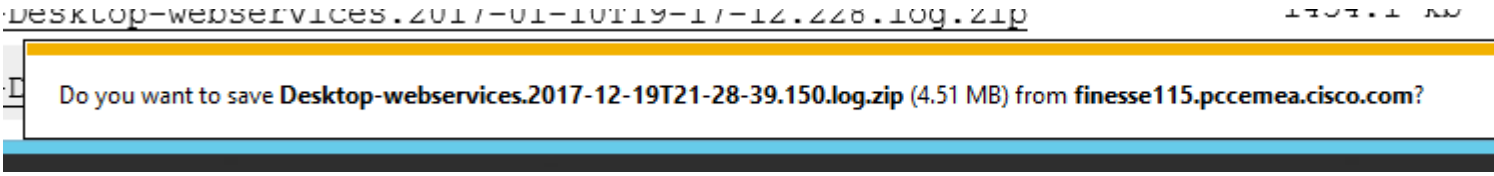
Option 1 : via l'interface utilisateur (UI) - services Web (requis) et journaux supplémentaires

Étape 1. Accédez à https://x.x.x.x/finesse/logs et connectez-vous avec le compte d'administration.

Étape 2. Développez le répertoire webservices/

Étape 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 permettant d'enregistrer le fichier.





Étape 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

Étape 1. Connectez-vous au serveur Finesse à l'aide de Secure Shell (SSH).

Étape 2. Entrez cette commande afin de collecter les journaux dont vous avez besoin. Les journaux sont

compressés et ont un temps relatif de 2 heures. Vous êtes invité à identifier le serveur SFTP sur lequel les journaux sont téléchargés.

fichier get activelog desktop recurs compress reltime hours 2.

```
Total size in Bytes: 413567
Total size in Kbytes: 403.87402
Would you like to proceed [y/n]? y
SFTP server IP:
```

Étape 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.

Étape 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

Guide d'administration de Cisco Finesse version 11.5(1)

Remarque : pour plus d'informations sur SFTP pour les fichiers de transfert Finesse, consultez ce document Finesse Backup and Upgrade Configuration with SFTP

Paramètres de suivi et collecte de journaux CVP et CVVB

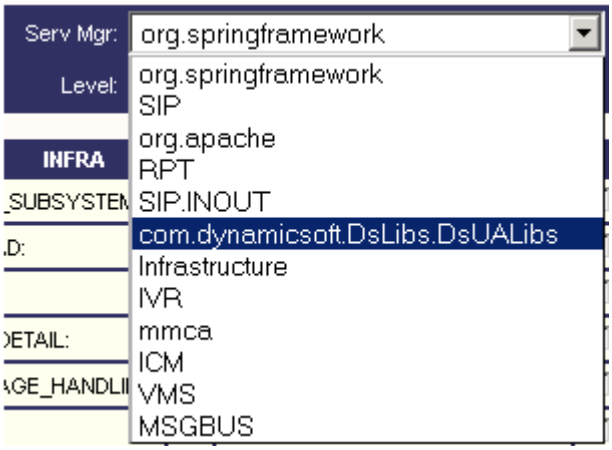
Serveur d'appels CVP

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

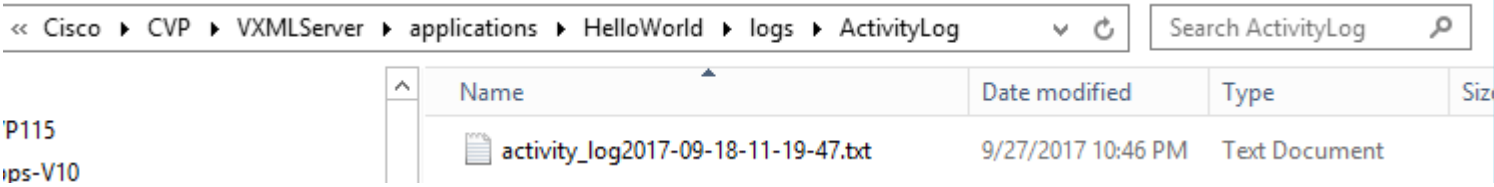
Étape 1. Accédez à l'URL de la page Web CVP CallServer Diag http://cvp.cc.lab:8000/cvp/diag.

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

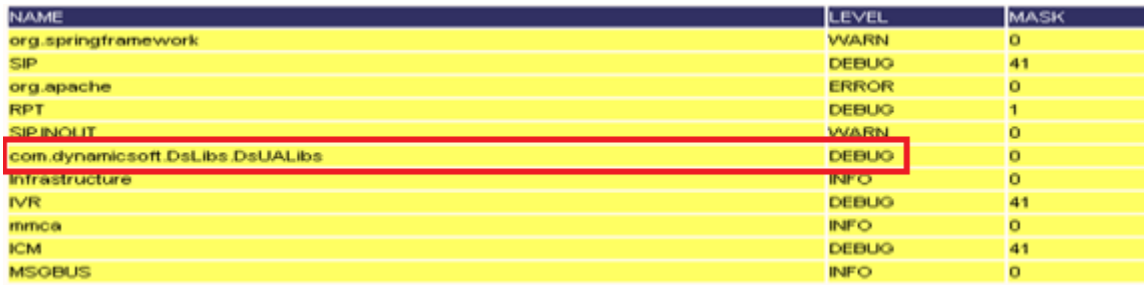
Étape 2. Sélectionnez com.dynamicsoft.DsLibs.DsUALibs dans le Serv. Menu déroulant Mgr dans l'angle supérieur gauche



Étape 3. Cliquez sur le bouton Définir.

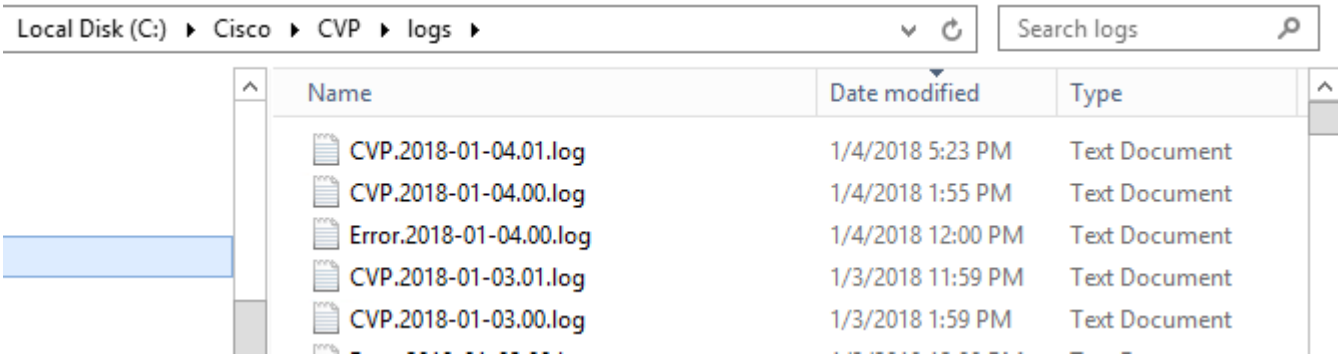


Étape 4. Faites défiler la fenêtre de trace vers le bas afin de vous assurer que le niveau de trace a été défini correctement. Voici vos paramètres de débogage.



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

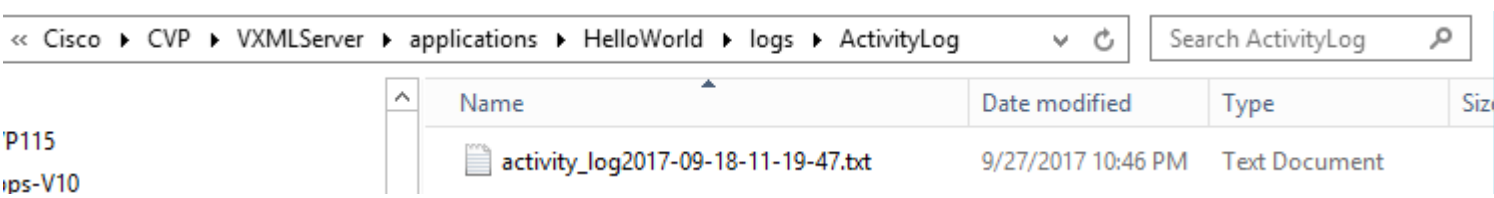
Étape 5. Lorsque vous reproduisez le problème, collectez les journaux à partir de C:\Cisco\CVP\logs et sélectionnez le fichier journal CVP en fonction de l'heure à laquelle le problème s'est produit.



Application CVP Voice XML (VXML)

Dans de très rares cas, vous devez augmenter le niveau de traces des applications de 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 :

Étape 1. Sauvegardez %CVP_HOME%\conf\oamp.properties .

Étape 2. Modifier %CVP_HOME%\conf\oamp.properties

omgr.traceMask=-1

omgr.logLevel=DEBUG
org.hibernate.logLevel=DEBUG
org.apache.logLevel=ERREUR
net.sf.ehcache.logLevel=ERREUR

Étape 3. Redémarrez OPSConsoleServer.

Informations sur le niveau de suivi

Niveau de suivi	Description	Niveau de consignation	Masque de suivi
0	Installation du produit par défaut. A un impact nul/minimal sur les performances.	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 + 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	DÉBOGUER	MISC +

Niveau de suivi	Description	Niveau de consignation	Masque de suivi
	impact très important sur les performances.		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 + 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 :

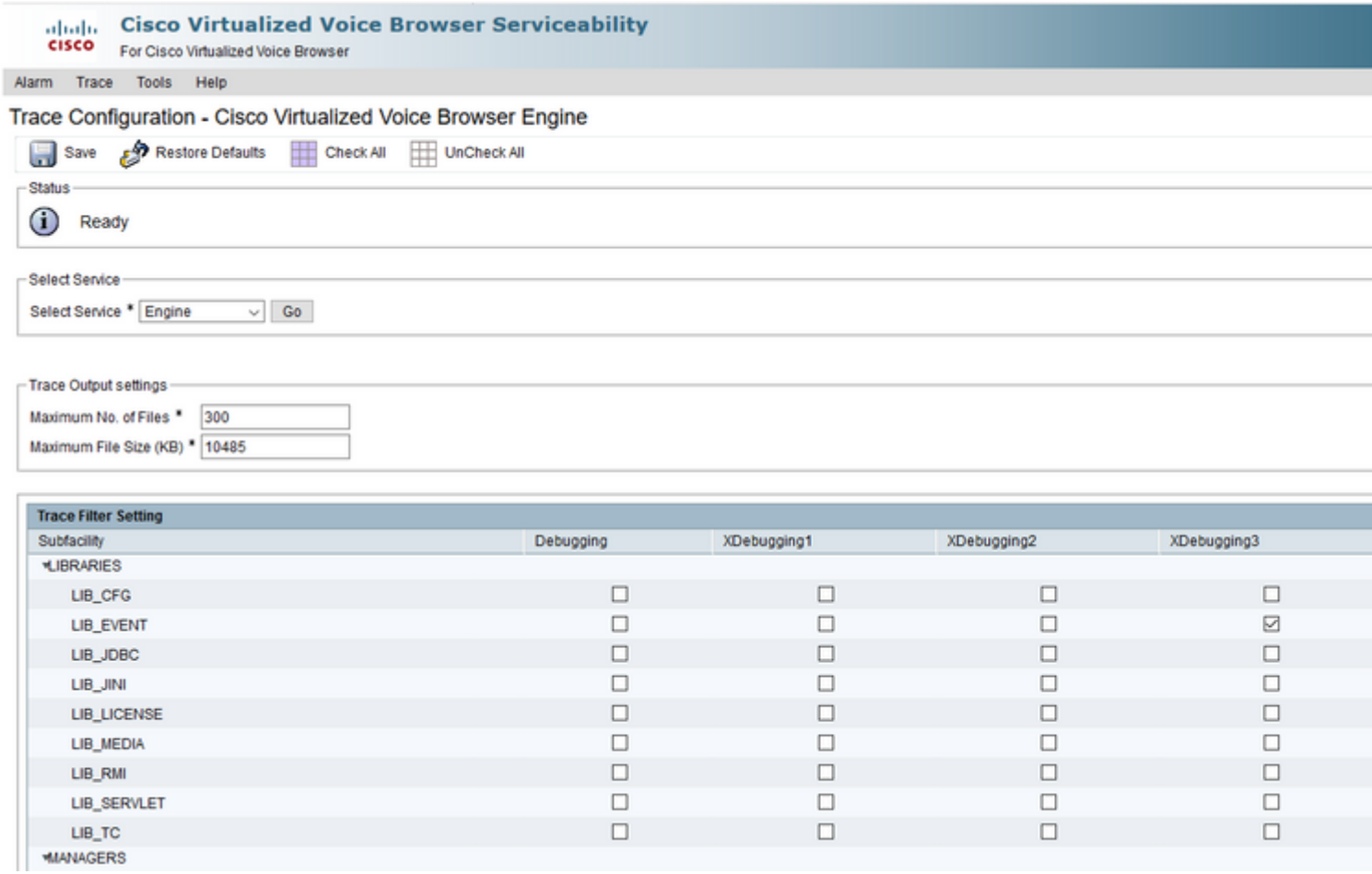
- Suivis « Administration » de Cisco VVB appelés journaux MADM
- Suivis du « moteur » Cisco VVB appelés journaux MIVR

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

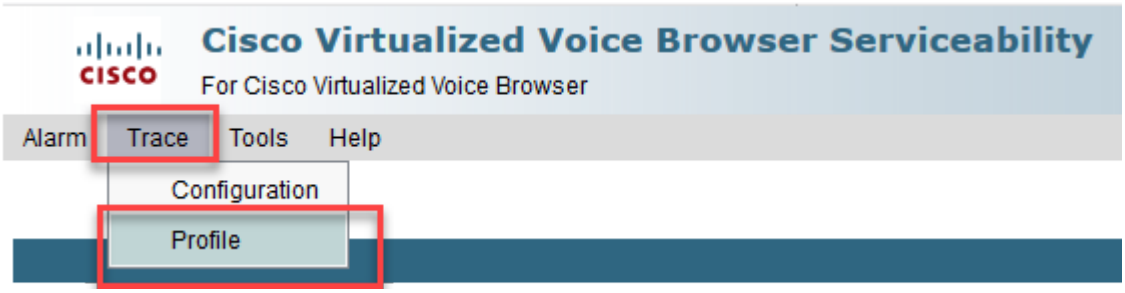
Les journaux les plus courants que vous devez collecter sont le moteur. Le niveau de suivi par défaut des suivis du moteur CVB est suffisant pour résoudre la plupart des problèmes. Toutefois, si vous devez modifier le niveau de suivi d'un scénario spécifique, Cisco vous recommande d'utiliser les profils prédéfinis du journal système

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.

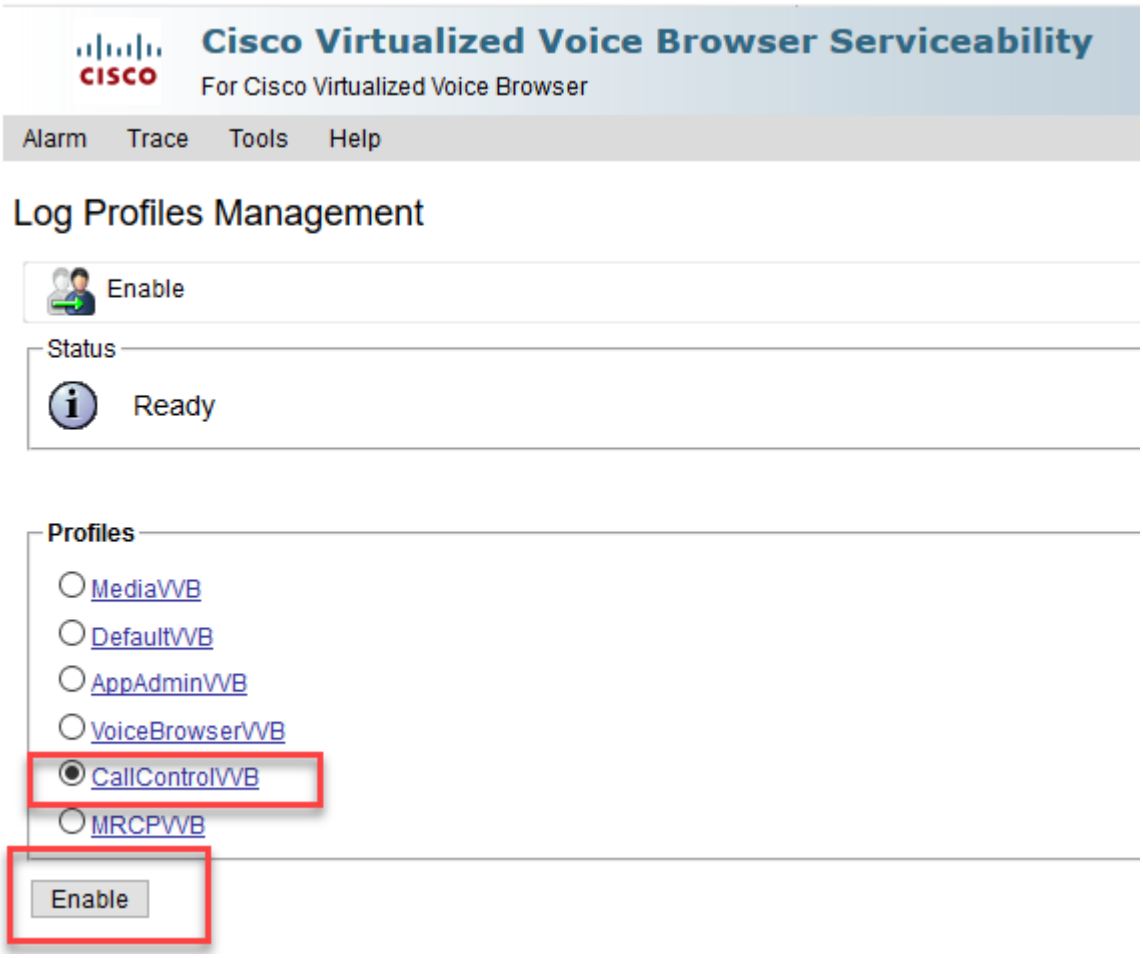
MRCPVB	Pour les problèmes d'interaction ASR/TTS avec Cisco VVB.
ContrôleAppelVB	Pour les problèmes liés à la signalisation SIP sont publiés dans le journal.

Étape 1. Ouvrez la page principale de CVVB (https://X.X.X.X/uccxservice/main.htm) , accédez à la page Cisco VVB Serviceability et connectez-vous avec le compte d'administration

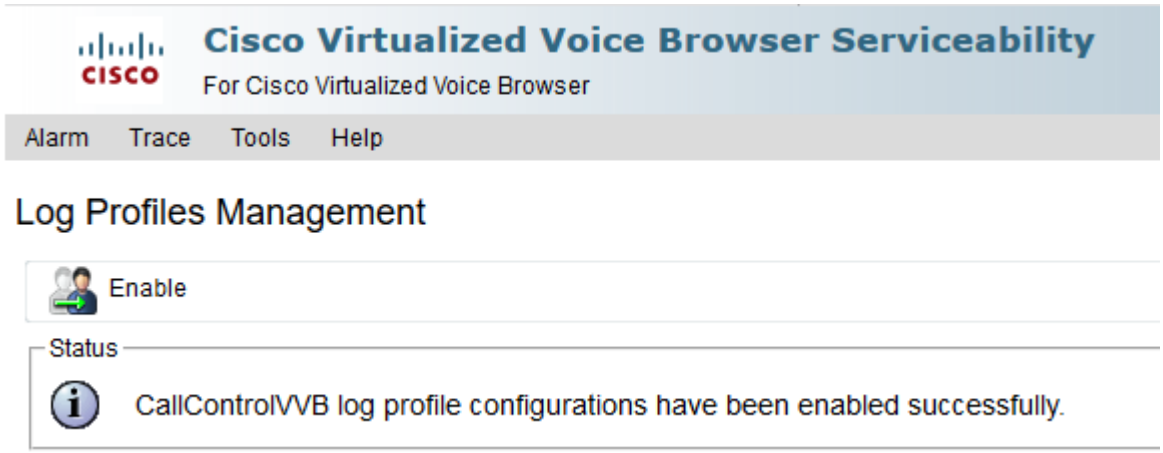
Étape 2. Sélectionnez Trace -> Profil



Étape 3. Cochez le profil que vous souhaitez activer pour le scénario spécifique et cliquez sur le bouton Enable (Activer). 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).



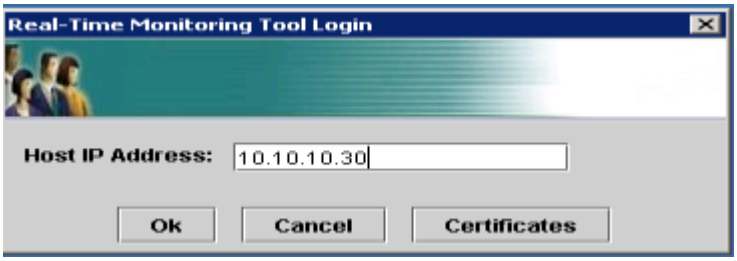
Vous voyez le message de réussite après avoir cliqué sur le bouton enable.



Étape 4. Une fois le problème reproduit, collectez les journaux. Utilisez l'outil RTMT (Real Time Monitor Tool) fourni avec le CVVB pour collecter les journaux.

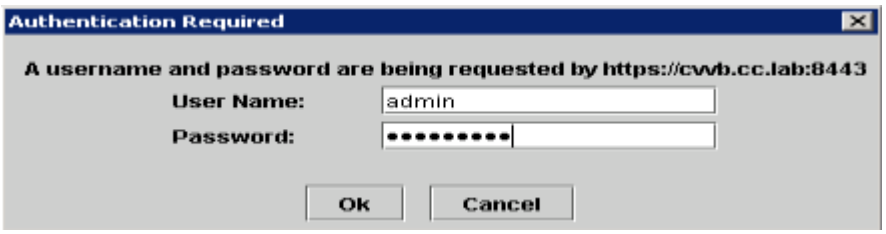
Étape 5. Cliquez sur l'icône Cisco Unified Real-Time Monitoring Tool sur votre bureau (si vous avez déjà téléchargé cet outil depuis le CVVB)

Étape 6. Fournissez l'adresse IP de la VVB et cliquez sur OK.



Étape 7. Acceptez les informations de certificat si elles sont affichées.

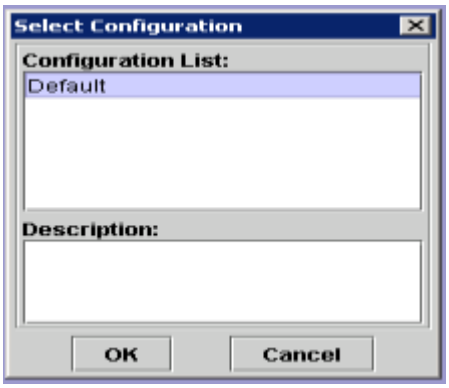
Étape 8. Saisissez les informations d'identification et cliquez sur OK.



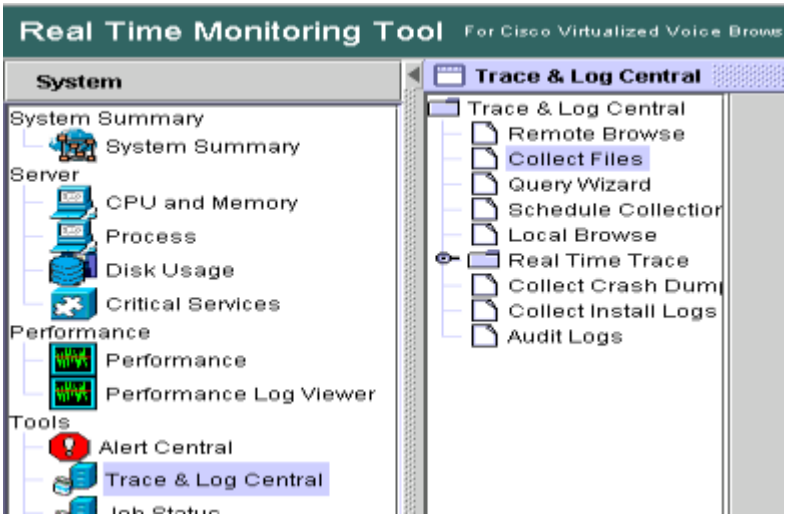
Étape 9. Si vous recevez un Avertissement de non-concordance de fuseau horaire, cliquez sur OUI et continuez.

Étape 10. Si vous avez reçu l'erreur TimeZone, RTMT se ferme probablement après avoir cliqué sur le bouton Yes (Oui). Relancez l'outil RTMT.

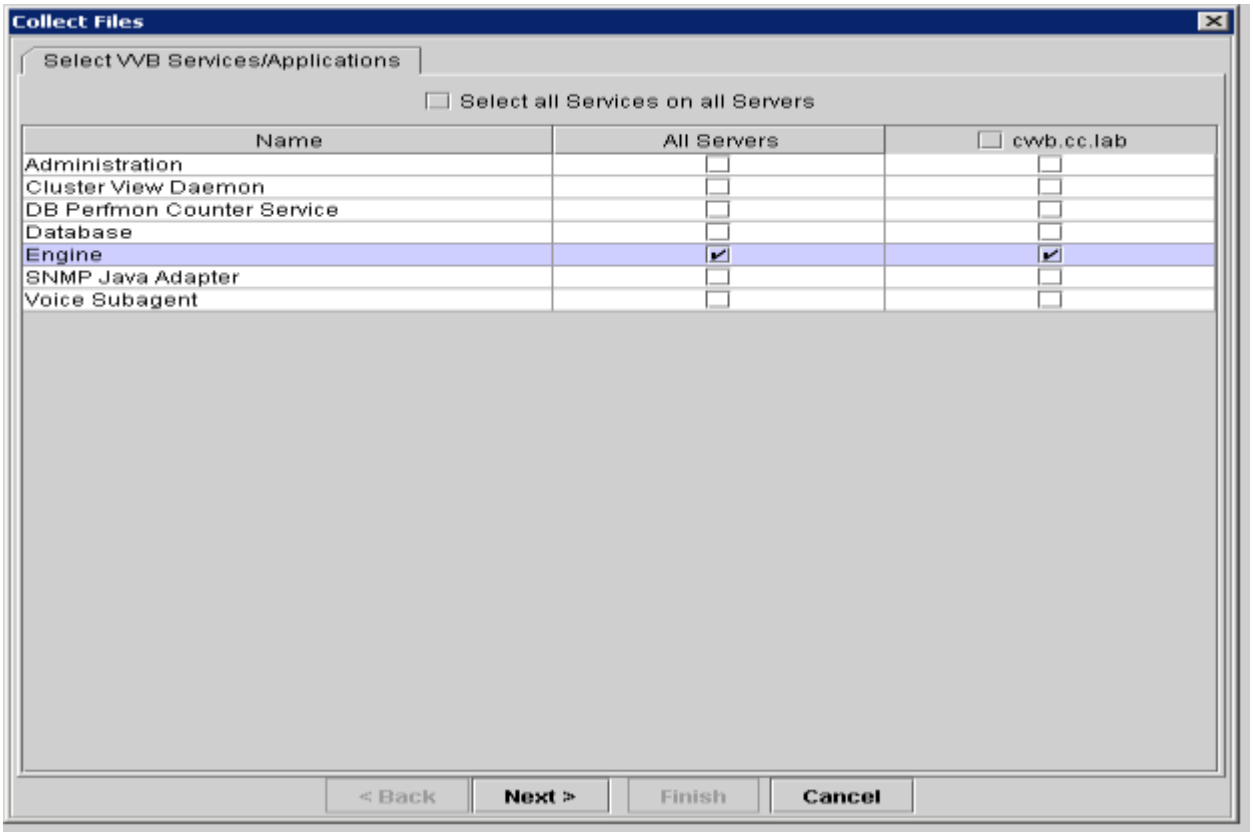
Étape 11. Laissez la configuration par défaut sélectionnée et cliquez sur OK



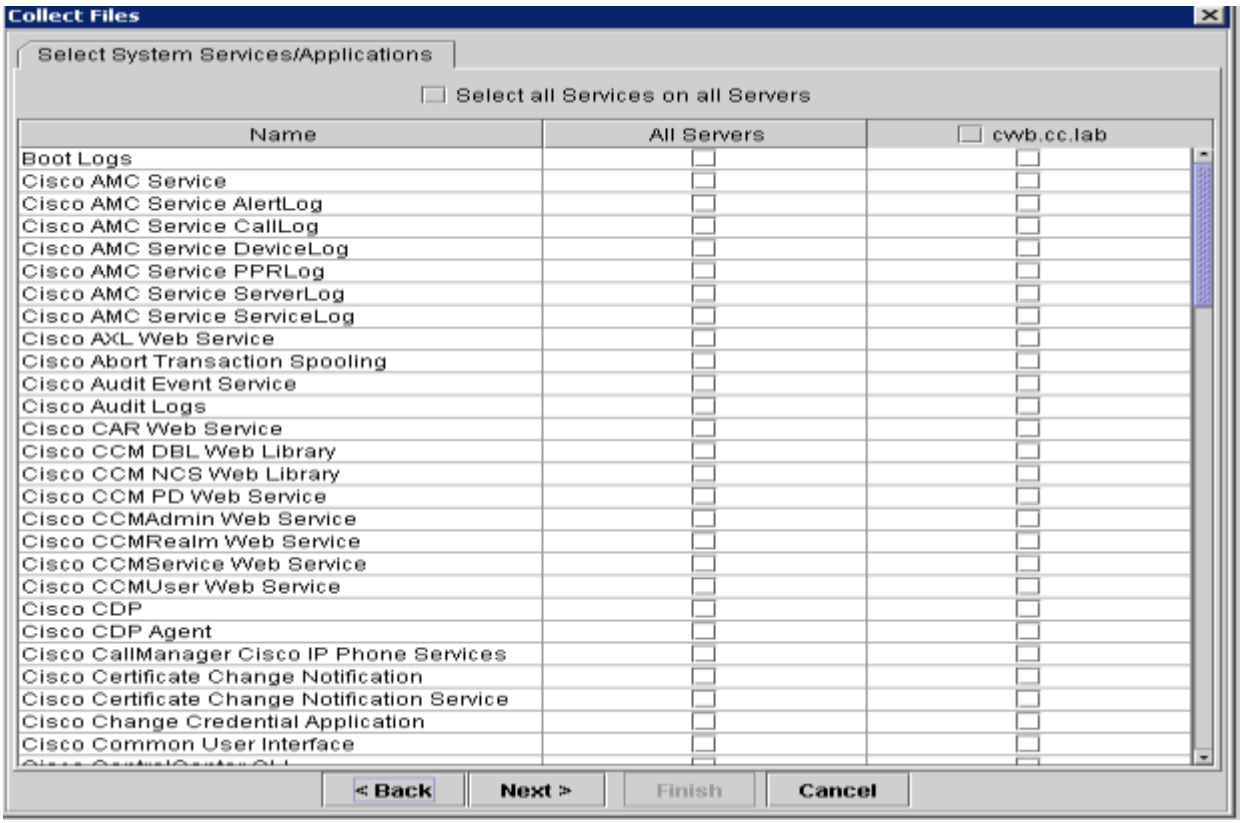
Étape 12. Sélectionnez Trace & Log Central, puis double-cliquez sur Collecter les fichiers



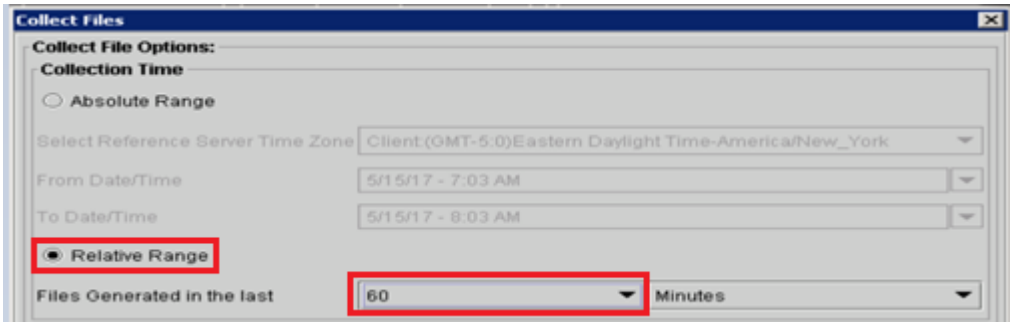
Étape 13. Dans la nouvelle fenêtre ouverte, sélectionnez le moteur et cliquez sur Next (Suivant)



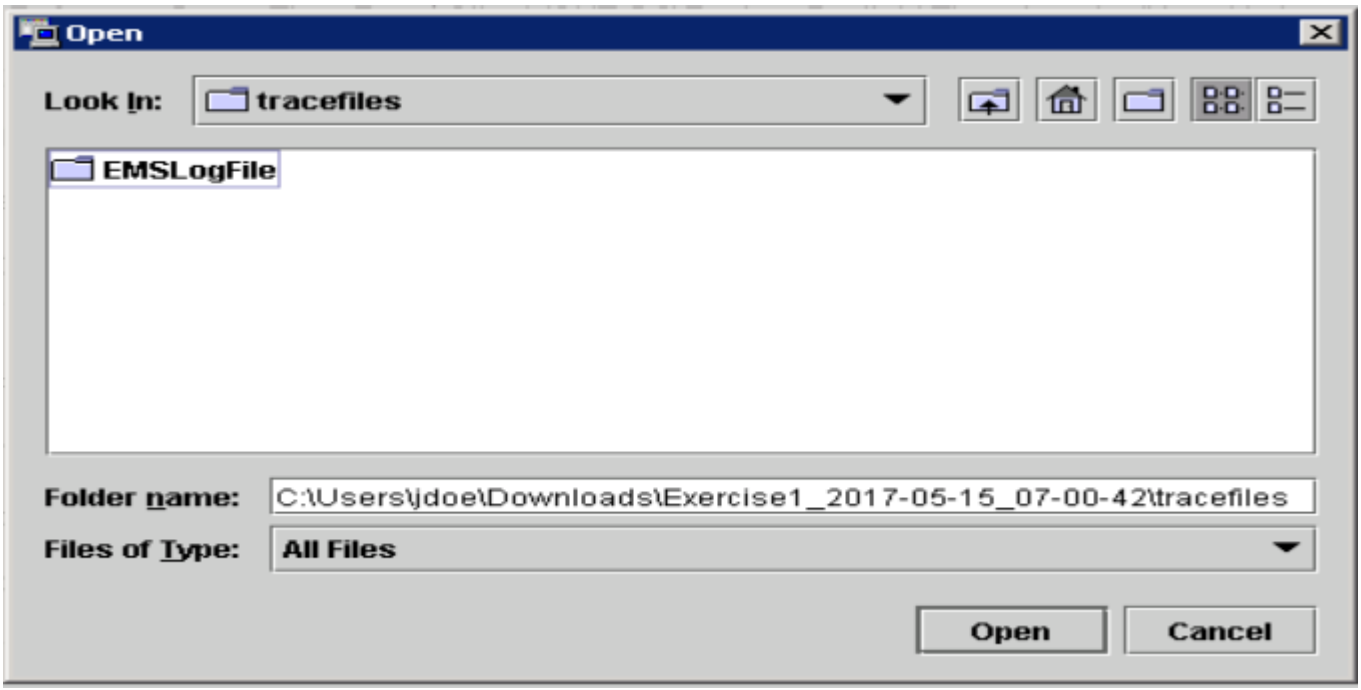
Étape 14. Cliquez à nouveau sur Suivant dans la fenêtre suivante



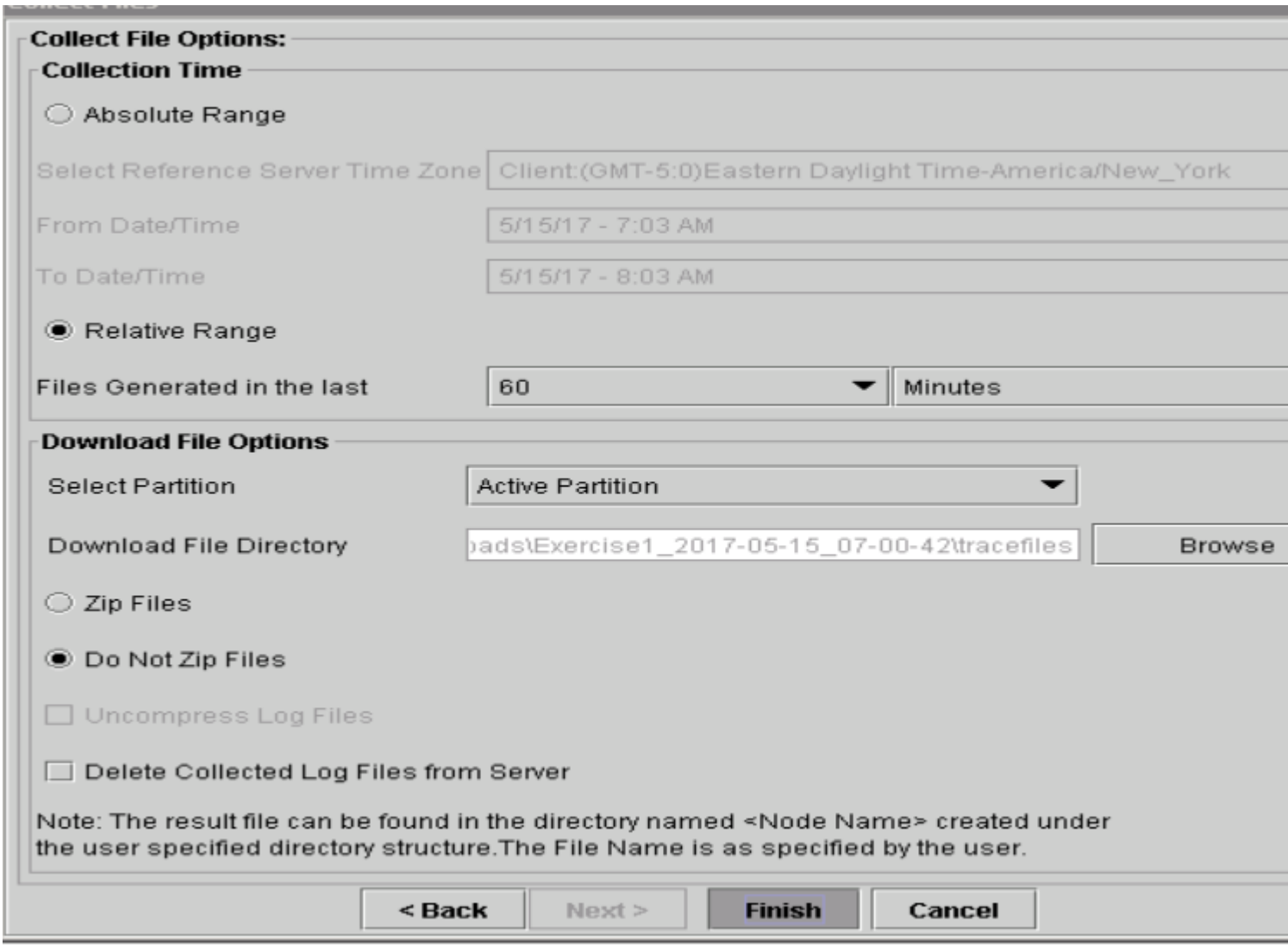
Étape 15. Sélectionnez Plage relative et assurez-vous de sélectionner l'heure pour couvrir l'heure de votre mauvais appel



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

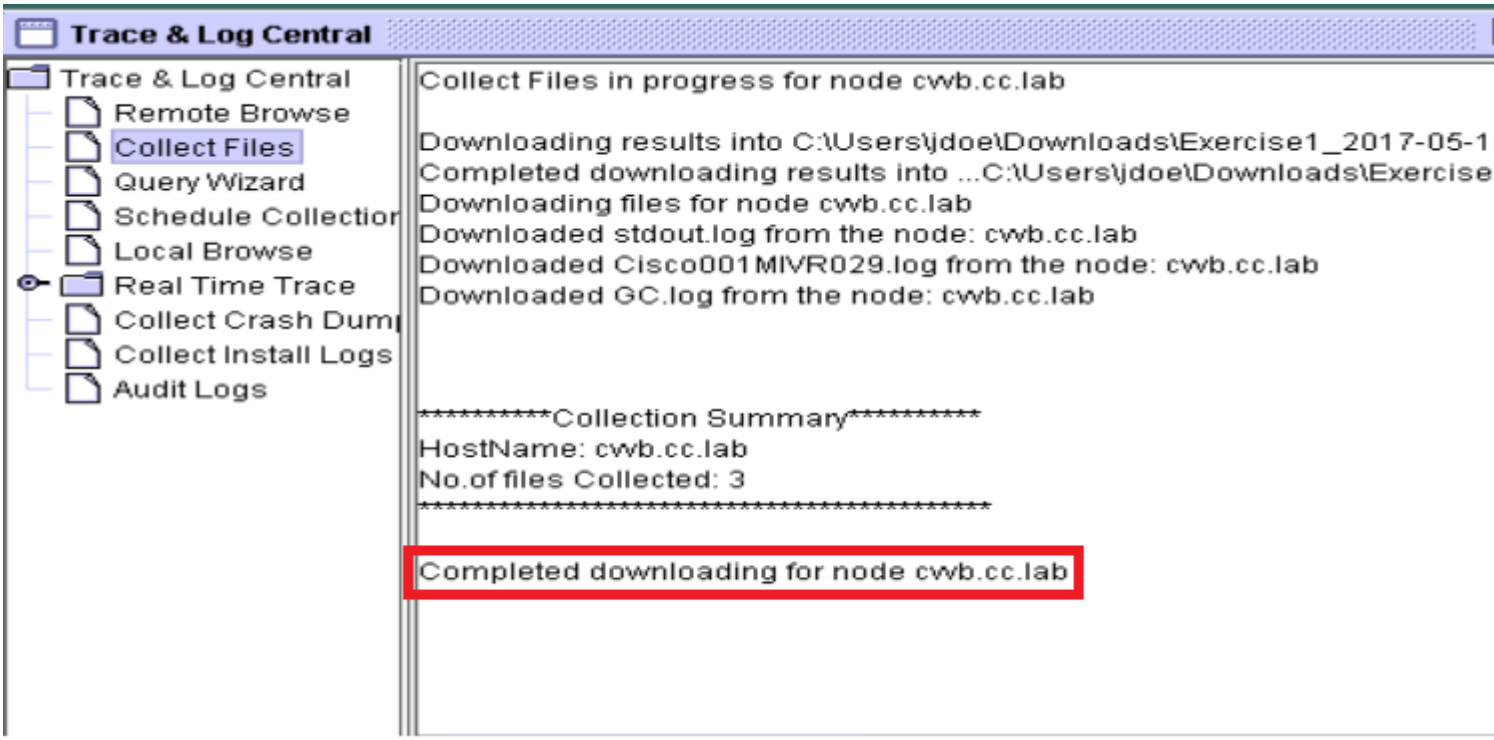


Étape 14. Une fois que tout est sélectionné, cliquez sur le bouton Terminer



Étape 15. Les fichiers journaux sont ainsi collectés. Attendez que le message de confirmation s'affiche sur

RTMT



Étape 16. Accédez au dossier dans lequel les traces sont enregistrées.

Étape 17. Les journaux du moteur sont tous requis. Pour les trouver, accédez au dossier \<horodatage>\uccx\log\MIVR.

Paramètres de suivi et collecte de journaux pour CUBE et CUSP

CUBE (SIP)

Étape 1. Définir l'horodatage des journaux et activer la mémoire 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 la plate-forme logicielle de production Cisco IOS® GW peut entraîner une panne.

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 jusqu'à 70-80% d'utilisation du CPU, le risque d'un impact sur les performances du service est fortement augmenté. Par conséquent, n'activez pas de débogages supplémentaires si le GW atteint 60 %

Étape 2. Activez ces débogages :

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

Étape 3. Reproduisez le problème.
Étape 4. Désactivez les traces.

```
#undebug all
```

Étape 5. Collectez les journaux.

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

CUSPIDE

Étape 1. Activez les suivis SIP sur CUSP.

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

Étape 2. Reproduisez le problème.

Étape 3. Désactivez la connexion une fois que vous avez terminé.

Collectez les journaux.

Étape 1. Configurez un utilisateur sur le CUSP (par exemple, test).

Étape 2. Ajoutez cette configuration à l'invite CUSP.

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

Étape 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.

Étape 4. Remplacez les répertoires par /cusp/log/trace.

Étape 5. Obtenez le log_<nom de fichier>.

Paramètres de suivi et collecte de journaux UCCE

Cisco recommande de définir des niveaux de suivi et de collecter les suivis via les outils Diagnostics Framework Portico ou System CLI

Remarque : pour plus d'informations sur Diagnostic Framework Portico et l'interface de ligne de commande du système, consultez le chapitre Diagnostic tools sur le document Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise, Release 11.5(1).

Lors du dépannage de 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).

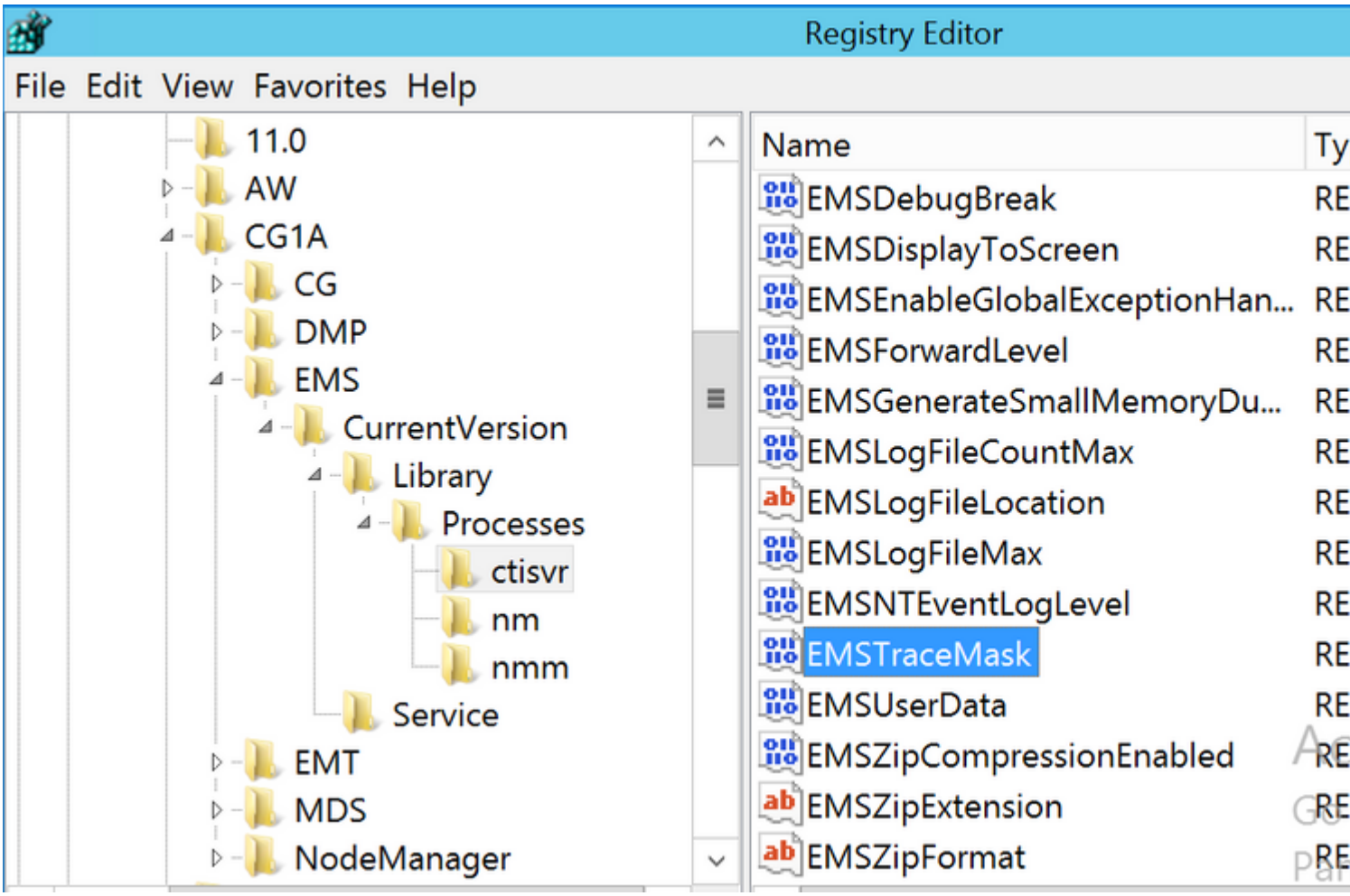
Remarque : consultez la section Trace Level du Guide de maintenance pour Cisco Unified ICM/Contact Center Enterprise, version 11.5(1) pour plus d'informations.

Par exemple, lors du dépannage de problèmes liés à Outbound Dialer, définissez le niveau de suivi sur le niveau 2 si le numéroteur est occupé.

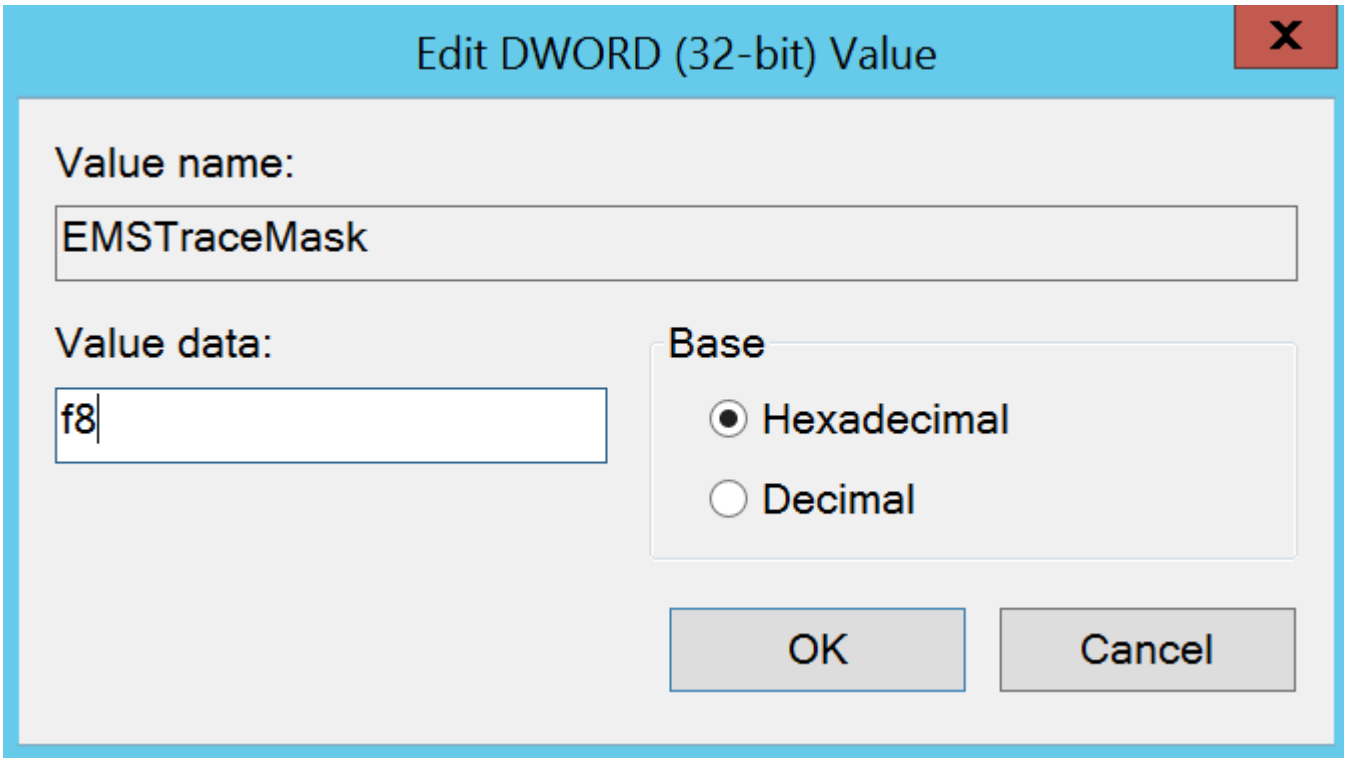
Pour CTISVR (CTISVR), les niveaux 2 et 3 ne définissent pas le niveau de registre exact recommandé par Cisco. Le registre de suivi recommandé pour CTISVR est 0XF8.

Étape 1. Sur la page UCCE Agent PG, ouvrez l'Éditeur du Registre (Regedit).

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



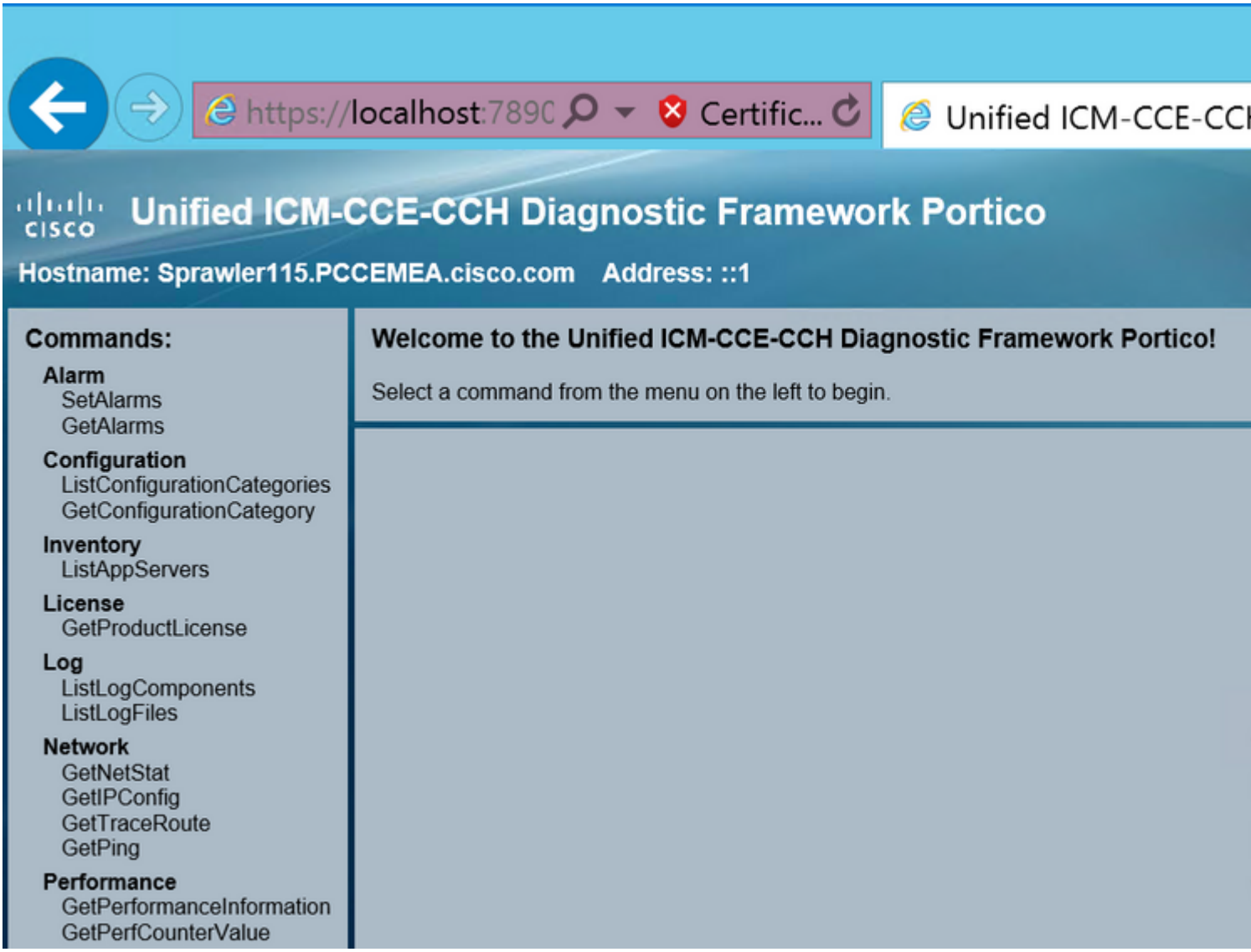
Étape 3. Double-cliquez sur le masque EMSTraceMask et définissez la valeur sur f8.



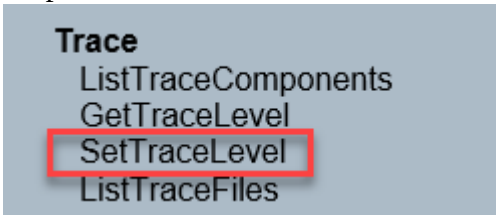
Étape 4. Cliquez sur OK et fermez l'Éditeur du Registre

Il s'agit des étapes permettant de définir n'importe quel suivi de composant UCCE (le processus RTR étant

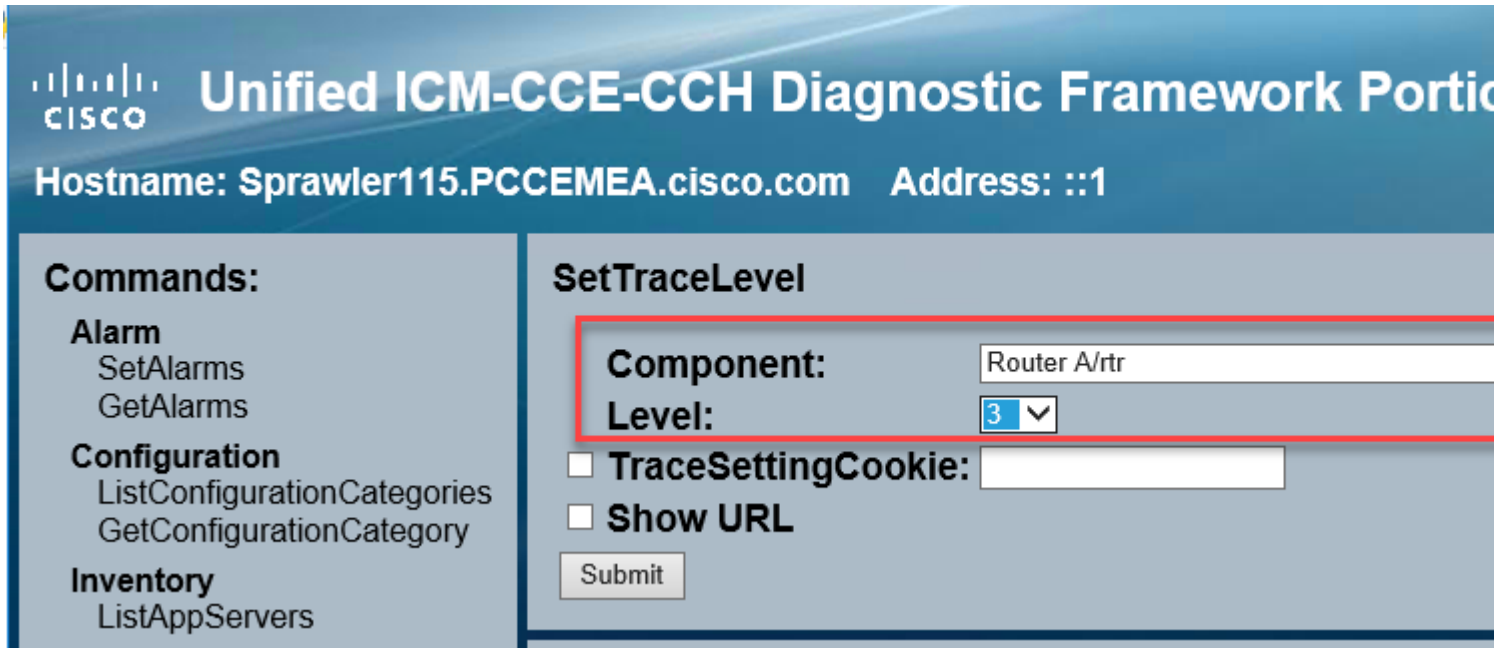
utilisé à titre d'exemple).
Étape 1. Ouvrez le Portique de cadre de diagnostic à partir du serveur dont vous avez besoin pour définir les suivis. connectez-vous avec l'utilisateur Administrateur.



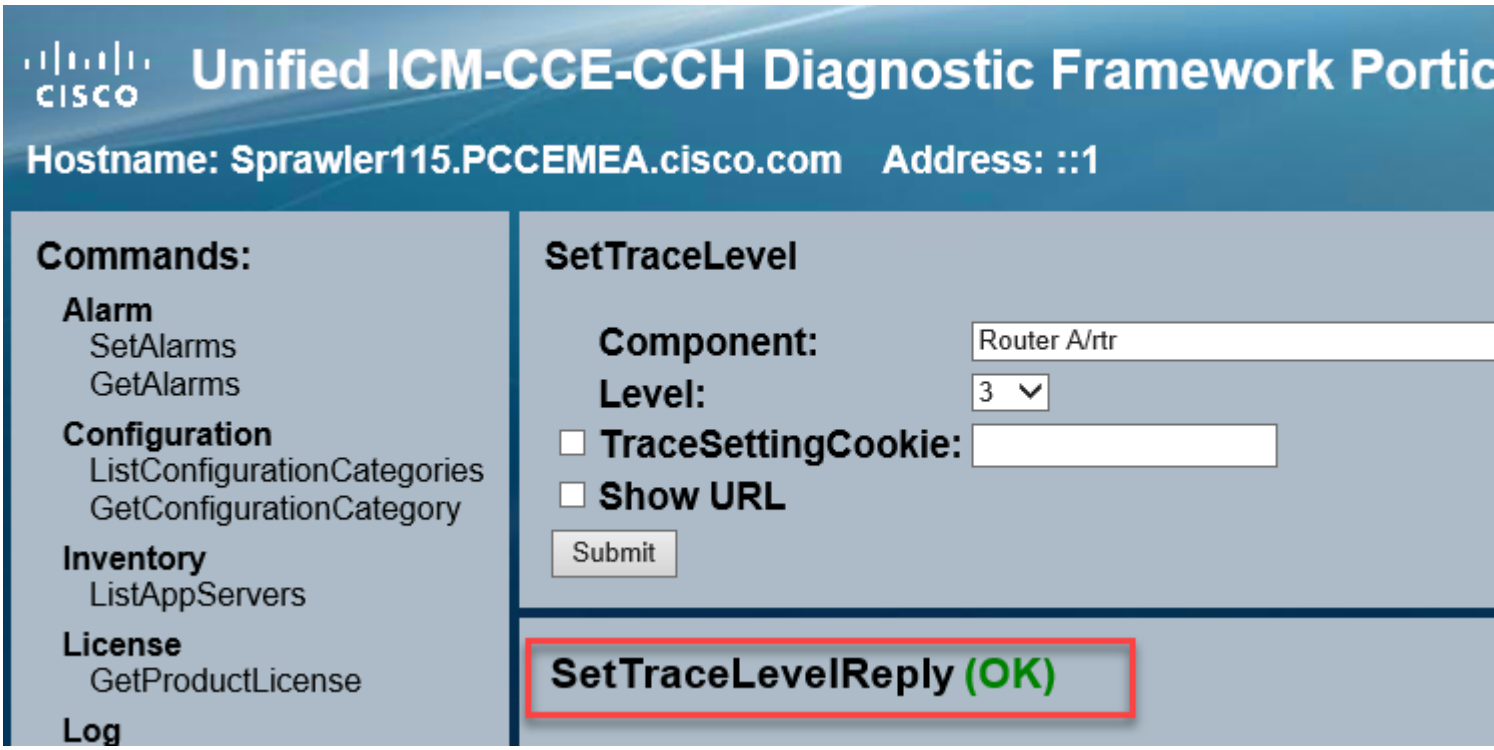
Étape 2. Dans la section Commands, accédez à Trace et sélectionnez SetTraceLevel.



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

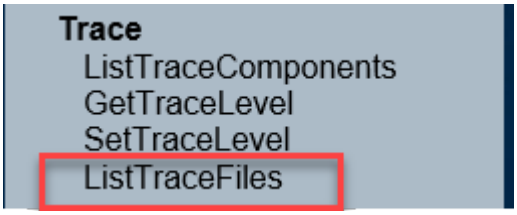


Étape 4. Cliquez sur Submit. Lorsque vous avez terminé, le message Ok s'affiche.

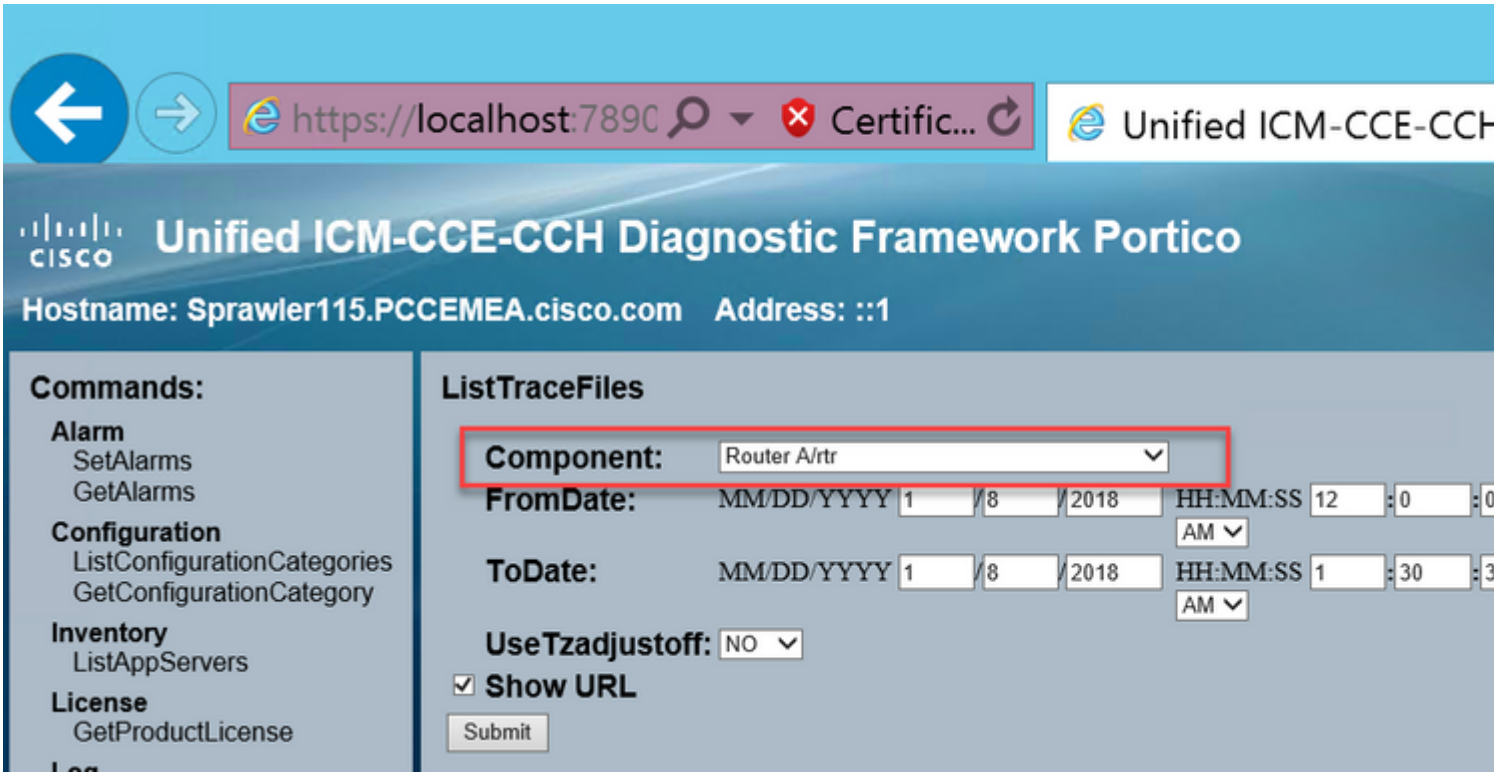


Avertissement : définissez le niveau de suivi sur 3 pendant que vous tentez de reproduire le problème. Une fois le problème reproduit, définissez le niveau de trace sur default. Soyez particulièrement prudent lorsque vous définissez les suivis JTAPIGW, car les niveaux 2 et 3 définissent les suivis de niveau inférieur, 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.

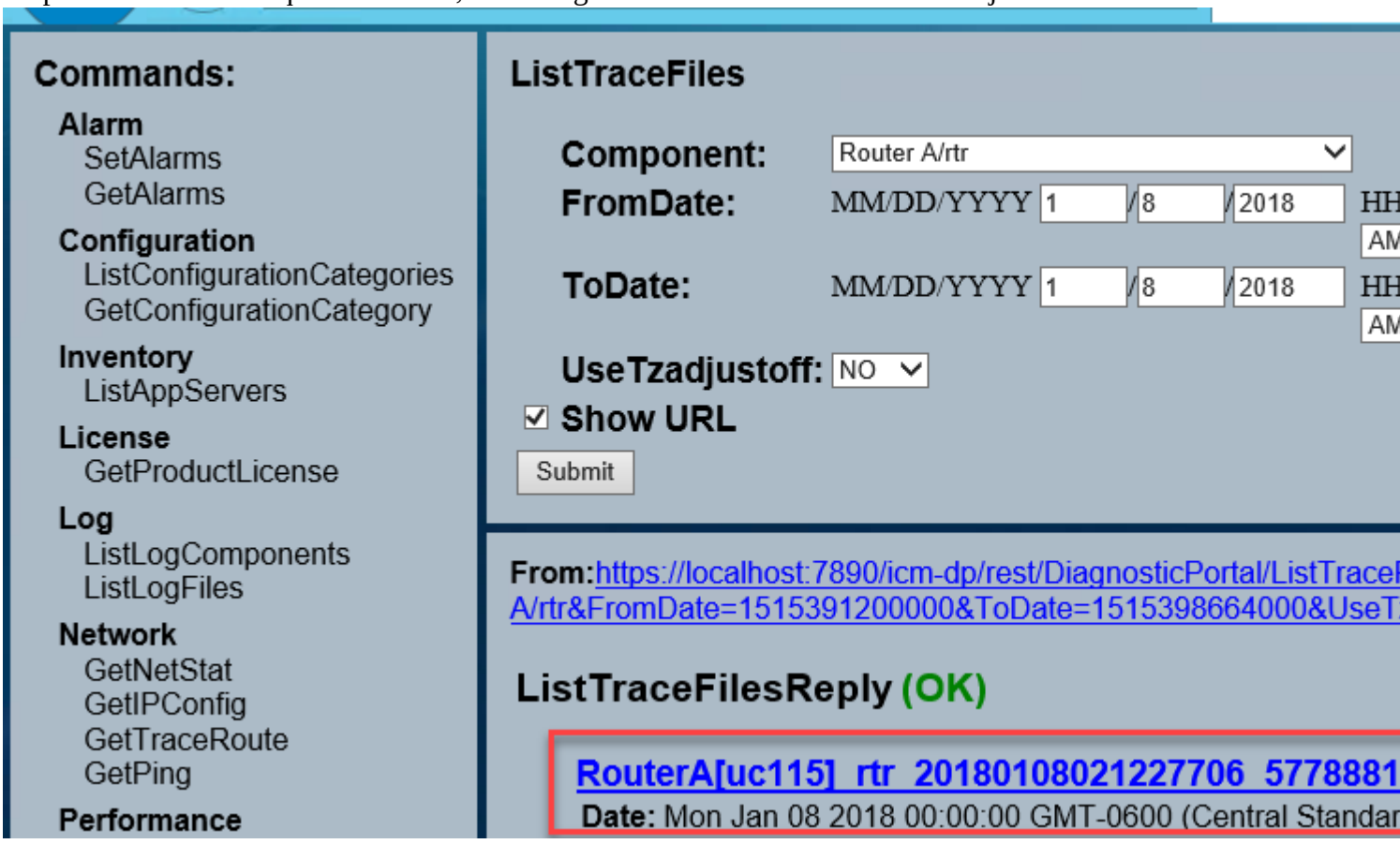
Collecte des journaux
Étape 1. Dans le portlet Diagnostic Framework, dans la section Commands, accédez à Trace et sélectionnez ListTraceFile.



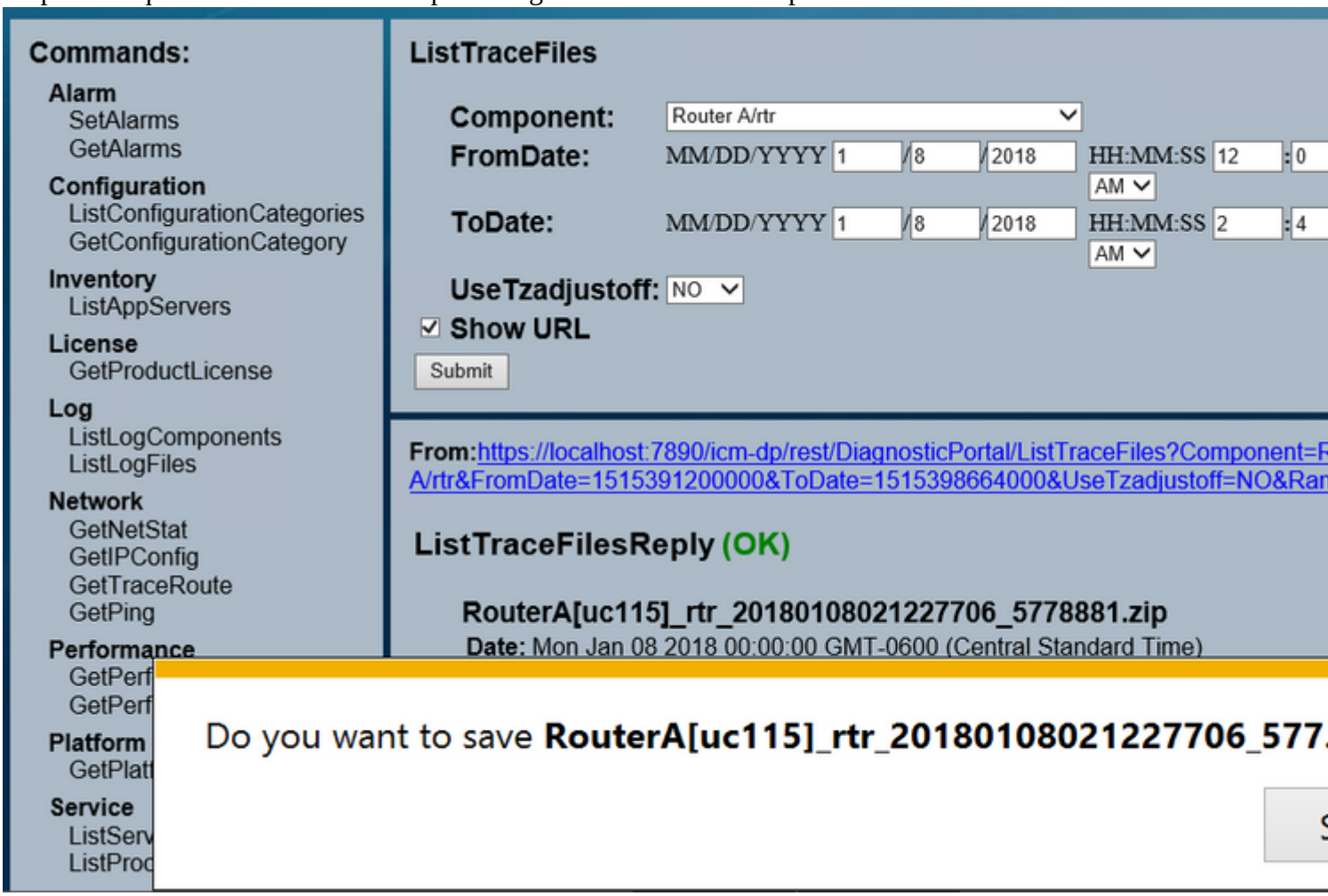
Étape 2. Dans la fenêtre ListTraceFile, sélectionnez Component, FromDate et ToDate. Cochez la case Afficher l'URL, puis cliquez sur Envoyer.



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



Étape 4. Cliquez sur le lien Fichier Zip et enregistrez le fichier à l'emplacement de votre choix.

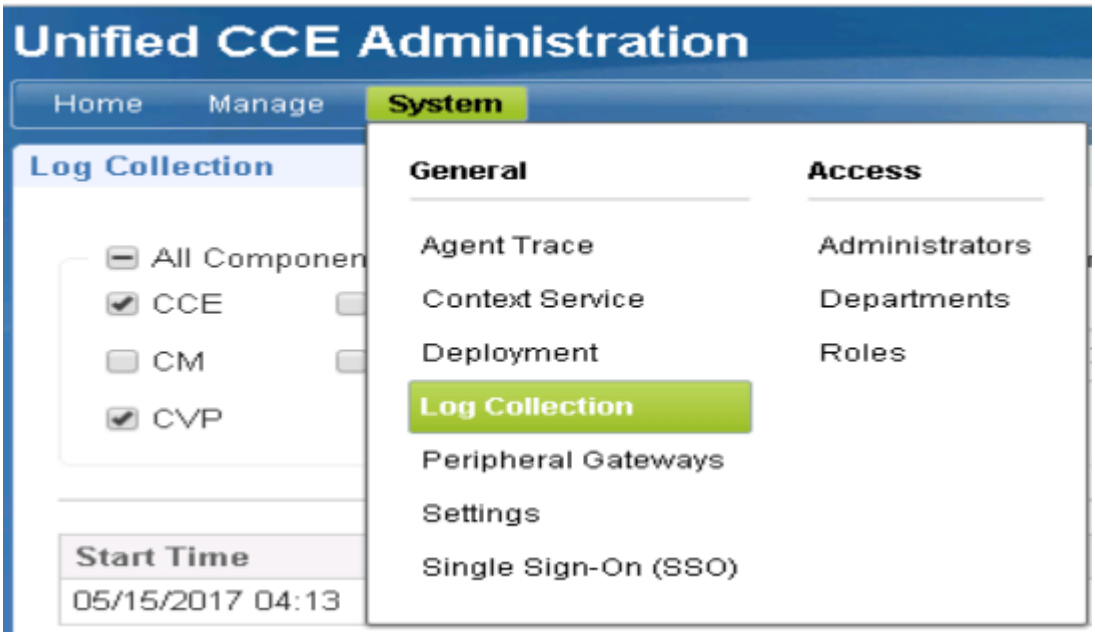


Paramètres de suivi et collecte de journaux PCCE

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.

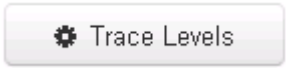
Étape 1. À partir du serveur PCCE AW, ouvrez l'outil Unified CCE Web Administration et connectez-vous avec le compte admin.

Étape 2. Accédez à Système ->Collecte de journaux.

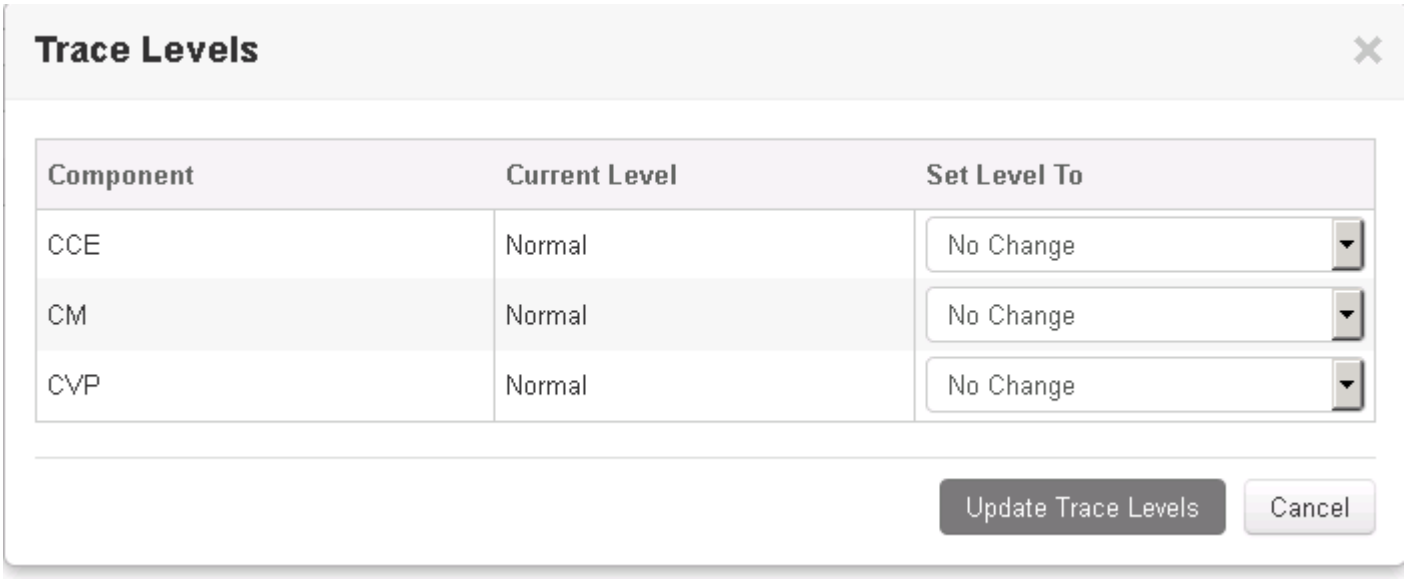


Étape 3. La page Log Collection s'ouvre.

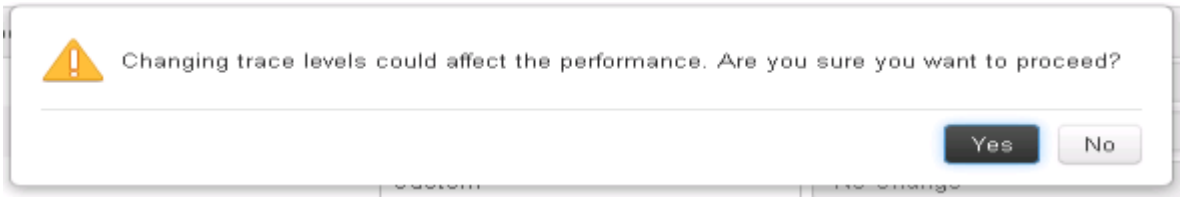
Étape 4. Cliquez sur , Niveaux de suivi, une boîte de dialogue contextuelle se charge



Étape 5. Définissez le niveau de suivi sur Détaillé sur CCE, laissez Aucun changement pour CM, CVP. Et cliquez sur Mettre à jour les niveaux de suivi



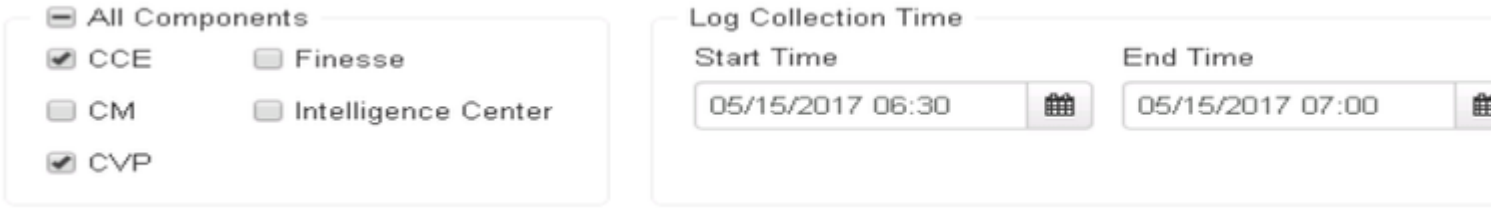
Étape 6. Cliquez sur Oui pour accuser réception de l'avertissement.



Étape 7. Une fois le problème reproduit, ouvrez Unified CCE Administration et revenez à System -> Log Collection.

Étape 8. Sélectionnez CCE et CVP dans le volet Composants.

Étape 9. Sélectionnez la durée de collecte du journal appropriée (par défaut, les 30 dernières minutes).



Remarque : actualisez la page pour l'heure de fin afin de la mettre à jour avec l'heure actuelle

Étape 10. Cliquez sur Collecter les journaux et sur Oui pour afficher l'avertissement. La collection de journaux démarre. Attendez quelques minutes avant que ça ne finisse.

Étape 11. Lorsque vous avez terminé, cliquez sur le bouton Download (Télécharger) dans la colonne Actions pour télécharger un fichier zippé contenant tous les journaux. Enregistrez le fichier zip à l'emplacement approprié.

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.