Configurations de suivi UCCE et collecte de log

Contenu

Introduction

Ce document décrit comment placer le suivi au Cisco Unified Contact Center Enterprise (UCCE) pour des clients, des services de passerelle d'accès aux périphériques (PAGE), le Customer

Voice Portal de Cisco (CVP), le numéroteur sortant de Cisco UCCE, le Cisco Unified Communications Manager (CallManager) (CUCM), et les passerelles Cisco.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Enterprise (UCCE)
- Cisco Agent Desktop (CAD)
- Serveur d'objet de couplage de la téléphonie et de l'informatique de Cisco (CTIOS)
- Cisco Finesse
- Customer Voice Portal de Cisco (CVP)
- Cisco Unified Communications Manager (CallManager) (CUCM)
- Passerelles Cisco

Configurations de suivi et collecte de log

> Remarques :
>
> Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.
>
> L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.
>
> Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Finesse

Ouvrez une session au serveur de finesse avec le Protocole Secure Shell (SSH) et sélectionnez ces commandes afin de collecter les logs que vous avez besoin. Vous êtes incité à identifier un serveur de FTP de SSH (SFTP) où les logs seront téléchargés.

Logs	Commande
Installez les logs	le fichier obtiennent installent desktop-install.log
Logs de bureau	le fichier obtiennent l'appareil de bureau d'activelog se reproduit compresse
Logs de Servm	le fichier obtiennent la plate-forme/log/servm* d'activelog. \ * compresse
Logs de Tomcat de plate-forme	le fichier obtiennent le chat/logs d'activelog se reproduit compresse
Le système d'exploitation de Voix (VOS) installent des logs	le fichier obtiennent installent install.log

Cisco Agent Desktop

Cette procédure décrit comment créer et collecter mettez au point les fichiers :

1. Sur l'ordinateur d'agent, allez à C:\Program Files\Cisco\Desktop\Config le répertoire et ouvrez le fichier Agent.cfg.

2. Changez le seuil de débogage d'HORS FONCTION **POUR DÉBUGGER**. Le SUIVI peut être utilisé pour un niveau plus profond.

   ```
   [Debug Log]
   Path=..\log\agent.dbg
   Size=3000000
   Threshold=DEBUG
   ```

3. Assurez Size=3000000 (six zéros).

4. Sauvegardez le fichier de configuration.

5. Arrêtez le programme d'agent.

6. Supprimez tous les fichiers dans le répertoire de C:\Program Files\Cisco\Desktop\log.

7. Commencez le programme d'agent, et recréez le problème.

8. Ceux-ci mettent au point des fichiers sont créés et placés dans C:\Program Files\Cisco\Desktop\log :

   agent0001.dbgctiosclientlog.xxx.log

Cisco Supervisor Desktop

Cette procédure décrit comment créer et collecter mettez au point les fichiers :

1. Sur l'ordinateur d'agent, allez à C:\Program Files\Cisco\Desktop\Config le répertoire et ouvrez le fichier supervisor.cfg.

2. Changez le SEUIL de débogage d'HORS FONCTION **POUR DÉBUGGER**. Le SUIVI peut être utilisé pour un niveau plus profond.

   ```
   [Debug Log]
   Path=..\log\supervisor.dbg
   Size=3000000
   THRESHOLD=DEBUG
   ```

3. Assurez Size=3000000 (six zéros).

4. Sauvegardez le fichier de configuration.

5. Arrêtez le programme d'agent.

6. Supprimez tous les fichiers dans le répertoire de C:\Program Files\Cisco\Desktop\log.

7. Commencez le programme d'agent, et recréez le problème. Un fichier de débogage nommé supervisor0001.dbg est créé et placé dans C:\Program Files\Cisco\Desktop\log.

Appareils de bureau de client CTIOS

Sur le PC client où le client CTIOS est installé, employez Regedt32 afin d'indiquer le suivi. Changez ces configurations :

Libérez	Emplacement de registre	Valeur par défaut	Modification
Releases plus tôt que 7.x	HKEY_LOCAL_MACHINE \ logiciel \ Cisco Systems \ Ctios \ se connecter \ TraceMask	0x07	Augmentez la valeur à 0xfff.
Version 7.x et ultérieures	HKEY_LOCAL_MACHINE \ LOGICIEL \ suivi de Cisco Systems, Inc. \ CTIOS	0x40000307	Placez la valeur à 0xfff pour le dépannage.

La sortie par défaut est créée et placé dans un fichier texte nommé CtiosClientLog dans les téléphones de bureau du client des systèmes de c:\Program Files\Cisco \ CTIOS \ CTIOS \ installez le répertoire.

Questions liées au client avec la PAGE de suivi et de logins

Service de sync du debug CAD

Ce sont les configurations pour mettre au point le service de sync CAD :

Établissement	Valeur
Fichier de configuration	DirAccessSynSvr.cfg
Emplacement par défaut	C:\Program Files\Cisco\Desktop\config
Problèmes généraux	Threshold=DEBUG
Fichiers de sortie	DirAccessSynSvr.log

Débuggez le serveur de VAURIEN CAD 6.0(X)

Ce sont les configurations pour mettre au point le serveur de VAURIEN CAD 6.0(X) :

Établissement	Valeur
Fichier de configuration	FCRasSvr.cfg
Emplacement par défaut	C:\Program Files\Cisco\Desktop\config
Problèmes généraux	Plage = 1-4, 50, 3000-8000
questions liées à la LDAP :	Plage = 4000-4999
questions liées LRM :	Plage = 1999-2000
questions liées à la base de données	Plage = 50-59
Fichiers de sortie	FCRasSvr.log, FCRasSvr.dbg
Emplacement par défaut	C:\Program Files\Cisco\Desktop\log

Serveur de conversation de debug

Ce sont les configurations pour mettre au point le serveur de conversation :

Établissement	Valeur
Fichier de configuration	FCCServer.cfg
Emplacement par défaut	C:\Program Files\Cisco\Desktop\config
Problèmes généraux	Threshold=DEBUG
Fichiers de sortie	FCCServer.log, FCCServer.dbg
Emplacement par défaut	C:\Program Files\Cisco\Desktop\log

D'autres suivi et logs liés à la page

Voir l'utilitaire Dumplog d'utilisation pour tirer des logs pour la collecte de log.

Suivi d'enable du CallManager PIM

Employez l'utilitaire de surveillance de processus (procmon) afin de tourner des niveaux de suivi en marche et en arrêt. Ces commandes activent le suivi du gestionnaire d'interface périphérique de CallManager (PIM) :

```
C:\procmon <Customer_Name> <PG_Name> <ProcessName>
>>>trace tp* !-- Turns on third party request tracing
>>>trace precall !-- Turns on precall event tracing
>>>trace *event !-- Turns on agent and call event tracing
>>>trace csta* !-- Turns on CSTA call event tracing
>>>ltrace !-- Output of all trace bits
>>>q !-- Quits
```

Cette commande de procmon arrête le suivi du CallManager PIM :

```
>>>trace * /off
```

Suivi d'enable sur le CUCM

Cette procédure décrit comment activer le suivi CUCM :

1. Allez à l'utilité unifiée de gestionnaire d'appel.
2. Sélectionnez le **suivi/configuration**.
3. **Services** choisis **cm**.
4. **CTIManager** choisi **(actif)**.
5. Dans la **configuration** en haut à droite et choisie **SDL**.
6. Enable tout excepté la jolie copie de débronchement du suivi SDL.
7. Laissez le nombre de fichiers et de leurs tailles aux valeurs par défaut.

8. Dans l'outil de suivi en temps réel (RTMT), collectez le Cisco Call manager et le gestionnaire du couplage de la téléphonie et de l'informatique de Cisco (CTI). Chacun des deux ont l'interface diagnostique de système (SDI) et la couche de distribution de signal (SDL) se connecte.

Passerelle de l'interface de programmation de téléphonie de Javas d'enable (JTAPI) (JGW)

Ces commandes de procmon activent le suivi JGW :

```
C:\procmon <Customer_Name> <node> process
>>>trace JT_TPREQUESTS !-- Turns on third-party request traces
>>>trace JT_JTAPI_EVENT_USED !-- Turns on traces for the JTAPI Events the PG uses
>>>trace JT_ROUTE_MESSAGE !-- Turns on routing client traces
>>>trace JT_LOW*  !-- Traces based on the underlying JTAPI and CTI layers
```

Un exemple de commande est l'**ipcc pg1a jgw1 de procmon**.

Suivi du serveur CTI d'enable (CTISVR) de côté actif

Cette procédure décrit comment activer le suivi CTISVR du côté actif :

1. Employez l'éditeur de registre afin d'éditer HKLM \ logiciel \ Cisco Systems, Inc\icm\<cust_inst>\CG1(a et b) \ SME \ CurrentVersion \ bibliothèque \ processus \ ctisvr.

2. Placez EMSTraceMask = f8.

Enable traçant VRU PIM

> Remarque: Les commandes distinguent les majuscules et minuscules. La PAGE de l'unité de réponse de The Voice (VRU) est différente que la PAGE de Cisco CallManager (CCM).

Ces commandes de procmon activent le suivi pour VRU PIM :

```
C:\procmon <Customer_Name> <PG_Name> <ProcessName>
procmon>>>trace *.* /off !-- Turns off
procmon>>>trace !-- Verifies what settings are on/off
procmon>>>trace cti* /onprocmon>>>trace opc* /on
procmon>>>trace *ecc* /onprocmon>>>trace *session* /off
procmon>>>trace *heartbeat* /off
procmon>>>ltrace /traceprocmon>>>quit
```

Cette commande de procmon arrête le suivi VRU PIM :

```
>>>trace * /off
```

Suivi de serveur de l'enable CTIOS sur les deux serveurs CTIOS

Cette procédure décrit comment activer le suivi sur les deux serveurs CTIOS :

1. Notez le suivi en cours masquer pour une utilisation ultérieure.

2. Employez l'éditeur de registre afin d'éditer HLKM >> logiciel \ Cisco Systems Inc. \ missile aux performances améliorées \ <cust_inst \ CTIOS \ SME \ CurrentVersion \ bibliothèque \ processus \ ctios.

3. Positionnement :

   - EMSTraceMask = 0x60A0F
   - EMSTraceMask à une de ces valeurs, selon la release :
     - 0x0A0F pour la version 6.0 et plus tôt
     - 0x20A0F pour la version 7.0 et 7.1(1)
     - 0x60A0F pour la version 7.1(2) et ultérieures

Le masque par défaut de suivi est 0x3 dans des toutes les releases excepté la version 7.0(0), où c'est 0x20003.

Si le masque de suivi a une valeur élevée (0xf ou plus élevé), il y a une grande incidence sur le débit de fin de performance des serveurs et d'appel CTIOS. Placez le masque de suivi à une valeur élevée seulement quand vous mettez au point un problème ; une fois que vous avez collecté les logs nécessaires, vous devez placer le masque de suivi de nouveau à sa valeur par défaut.

Pour le dépannage des buts, a placé le masque de suivi de serveur CTIOS à :

- 0x0A0F pour la version 6.0 et plus tôt
- 0x20A0F pour la version 7.0, et 7.1(1)
- 0x60A0F pour la version 7.1(2) et ultérieures

Suivi périphérique ouvert du contrôleur d'enable (OPC) à la PAGE active

Ces commandes opctest activent le suivi OPC à une PAGE active :

```
opctest /cust <cust_inst> /node <node>
opctest:debug /agent /routing /cstacer /tpmsg /closedcalls
```

C'est un exemple d'un environnement de travaux pratiques :

```
C:\Documents and Settings\ICMAdministrator>opctest /cust cc1 /node pg1a
OPCTEST Release 8.0.3.0 , Build 27188
opctest: debug /agent /routing /cstacer /tpmsg /closedcalls !-- Use debug /on in
order to restore default tracing levels
opctest: quit
```

Les exemples supplémentaires sont :

```
opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg
!-- General example

opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg /NCT
!-- Network transfer example

opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg /task /passthru
!-- Multimedia example

opctest:debug /agent /routing /cstacer /rcmsg /closedcalls /inrcmsg /passthru
!-- VRU PG example
```

Suivi d'Eagtpim d'enable à la PAGE active

Ces commandes de procmon activent le suivi d'eagtpim à une PAGE active :

```
C:\>procmon <cust_inst> <node> pim<pim instance
>>>>trace tp* /on
>>>trace precall /on
>>>trace *event /on
>>>trace csta* /on
```

C'est un exemple d'un environnement de travaux pratiques :

```
C:\Documents and Settings\ICMAdministrator>procmon cc1 pg1a pim1
>>>>trace tp* /on
>>>>trace precall /on
>>>>trace *event /on
>>>>trace csta* /on
>>>>quit
```

Utilitaire Dumplog d'utilisation pour tirer des logs

Référez-vous à comment utiliser l'utilitaire Dumplog pour des détails supplémentaires. Employez la commande de **cdlog** afin d'obtenir aux fichiers journal le répertoire, suivant les indications de cet exemple :

```
c:\cdlog <customer_name> pg1a   !-- Or, pgXa to depending on the PG number (X)
c:\icm\<customer_name>\<<PG#>>\logfiles\
```

Ces exemples affichent comment placer la sortie dans le fichier par défaut ; dans des tous les cas, vous pouvez employer */of* afin de définir un nom spécifique pour le fichier de sortie :

```
c:\icm\<customer_name>\<PG#>\logfiles\dumplog pim1 /bt <HH:MM> /et <HH:MM> /ms /o
!-- This PIM example places output in a default pim1.txt file

c:\icm\<customer_name>\<PG#>\logfiles\dumplog opc /bt <HH:MM> /et  <HH:MM> /ms /o
!-- This OPC example places output in a default opc.txt file

c:\icm\<customer_name>\<PG#>\logfiles\dumplog jgw1 /bt <HH:MM> /et <HH:MM> /ms /o
c:\cdlog <customer_name> cg1a
c:\icm\<customer_name>\<cg#>\logfiles\
!-- This JTAPI example places output in a default jgw1.txt file

c:\icm\<customer_name>\cg#\logfiles\dumplog ctisvr /bt <HH:MM> /et <HH:MM> /ms /o
!-- This CTI server example places output in a default ctisvr.txt file

c:\ icm\<customer_name>\ctios\logfiles\dumplog ctios /bt <HH:MM> /et <HH:MM> /ms /o
!-- This CTIOS server example places output in a default ctios.txt file
```

Suivi d'enable sur des serveurs CVP

SIP

Cette procédure décrit comment activer le suivi sur des serveurs CVP avec le Logiciel de téléphones IP Cisco SIP :

1. Sur les serveurs d'appel, allez à l'outil de diag CVP (http://localhost(CallServer):8000/cvp/diag) afin d'obtenir la pile de Protocole SIP (Session

Initiation Protocol).

2. Ajoutez com.dynamicsoft.Dslibs.DsUAlibs avec mettent au point.

3. **Positionnement de** clic.

4. Clic **DEBUG/41**.

H323

Cette procédure décrit comment activer le suivi sur des serveurs CVP avec une passerelle de h323 :

1. Sur les serveurs d'appel, procédure de connexion à VBAdmin.

2. Activez ces suivis pour le navigateur de Voix CVP :

```
setcalltrace on
setinterfacetrace on
```

Tirez les logs CVP des serveurs d'appel

Collectez le fichier CVP *.log et les fichiers d'Error.log pendant la période de la période de test. Ces fichiers sont dans le répertoire de C:\Cisco\CVP\logs sur les deux serveurs CVP.

Ce sont les emplacements des fichiers journal pour CVP unifié, où CVP_HOME est le répertoire dans lequel le logiciel unifié CVP est installé.

Type de logs	Emplacement
Serveur d'appel et/ou journaux du serveur d'enregistrement	**CVP_HOME \ logs **
Logs de console d'exécutions	**CVP_HOME \ logs \ OAMP **
Journaux du serveur de la Voix XML (VXML)	**CVP_HOME \ logs \ VXML **
Logs d'agent de Protocole SNMP (Simple Network Management Protocol)	**CVP_HOME \ logs \ SNMP **
Logs unifiés de gestionnaire de ressources CVP	**CVP_HOME \ logs \ ORM **

Un emplacement d'exemple est C:\Cisco\CVP.

Journaux du serveur VXML

Pour des applications XML faites sur commande de Voix telles qu'une application déployée d'Audium, vous pouvez activer un enregistreur de débogage.

Ajoutez cette ligne à la section de **<loggers>** (la dernière section) du fichier de configuration settings.xml dans C:\Cisco\CVP\VXMLServer\applications\APP _NAME \ données \ application \ répertoire :

```
<logger_instance name="MyDebugLogger"
class="com.audium.logger.application.debug.ApplicationDebugLogger"/>
```

Au délai d'exécution, cet enregistreur sort un log détaillé de VoiceXML au \ à Cisco \ CVP \ VXMLServer \ applications \ répertoire APP_NAME \ MyDebuggerLogger.

Remarque: Vous pouvez changer le nom de l'enregistreur dans le fichier de configuration settings.xml de MyDebugLogger à n'importe quel nom que vous choisissez.

Suivi lié au numéroteur sortant et collecte de log

Cette procédure décrit comment augmenter le processus de badialer ouvre une session le numéroteur sortant (qui est habituellement trouvé à une PAGE).

1. Assurez EMSDisplaytoScreen = 0.

2. Employez l'éditeur de registre afin d'éditer HKEY_LOCAL_MACHINE \ LOGICIEL \ Cisco Systems, Inc. \ missile aux performances améliorées \ <instance> \ numéroteur \ SME \ CurrentVersion \ bibliothèque \ processus \ baDialer.

3. Positionnement :

   - EMSTraceMask = 0xff
   - EMSUserData = FF FF (quatre f en mode binaire)

4. Employez l'éditeur de registre afin d'éditer HKEY_LOCAL_MACHINE \ LOGICIEL \ Cisco Systems, Inc. \ missile aux performances améliorées \ <instance> \ numéroteur.

5. Placez DebugDumpAllEvents = 1.

Tirez les logs

Exécutez l'utilitaire Dumplog à partir du répertoire de /icm/ <instance>/dialer/logfiles :

```
dumplog badialer /bt hh:mm:ss /et hh:mm:ss /o
```

Sur l'importation

Cette procédure décrit comment augmenter le log de processus de baimport.

1. Employez l'éditeur de registre afin d'éditer HKEY_LOCAL_MACHINE \ LOGICIEL \ Cisco Systems, Inc. \ missile aux performances améliorées \ <instance> \ LoggerA \ SME \ CurrentVersion \ bibliothèque \ processus \ baImport.

2. Positionnement :

   - EMSTraceMask = 0xff
   - EMSUserData = FF FF (quatre f en mode binaire)

3. Exécutez l'utilitaire Dumplog à partir du répertoire de /icm/ <instance>/la/logfiles :

   ```
   dumplog baimport /bt hh:mm:ss /et hh:mm:ss /o
   ```

Sur le Campaignmanager

Cette procédure décrit comment augmenter le log de processus de campaignmanager.

1. Employez l'éditeur de registre afin d'éditer HKEY_LOCAL_MACHINE \ LOGICIEL \ Cisco Systems, Inc. \ missile aux performances améliorées \ <instance> \ LoggerA \ SME \ CurrentVersion \ bibliothèque \ processus \ CampaignManager.

2. Positionnement :

   - EMSTraceMask = 0xff
   - EMSUserData = FF FF (quatre f en mode binaire)

3. Exécutez l'utilitaire Dumplog à partir du répertoire de /icm/ <instance>/la/logfiles :

   ```
   dumplog campaignmanager /bt hh:mm:ss /et hh:mm:ss /o
   ```

ÀLa PAGE du gestionnaire de transmissions d'Avaya (ACD), employez l'utilitaire **opctest** afin d'augmenter le suivant pour le CallManager et l'Avaya.

```
C:\opctest /cust <instance> /node <pgname>
opctest: type debug /agent /closedcalls /cstacer /routing
opctest: q !-- Quits
```

Cette procédure décrit comment augmenter le suivi pour le processus de ctisvr.

1. Employez l'éditeur de registre afin d'éditer HKEY_LOCAL_MACHINE \ LOGICIEL \ Cisco Systems, Inc.\ICM\icm\CG1A\EMS\CurrentVersion\Library\Processes\ctisvr.

2. Placez EMSTraceMask = f8. Vous pouvez laisser la valeur à f0 si vous voulez.

Processus de routeur de logins de routeur d'enable

Cette procédure décrit comment activer des journaux du routeur :

1. Sur le routeur, naviguez vers le **Start > Run**, et écrivez le **rtrtrace**.

2. Introduisez le nom de client.

3. Cliquez sur **Connect**.

4. Sélectionnez ces options :

   agentchangesrouterequestsscriptselectsnetworkvrutracingtranslationroutecallqueuingcalltype realtime

5. Cliquez sur **Apply**.

6. Quittez l'utilitaire.

Pour la version 8.5 opctest, utilisez le Portico diagnostique de cadre à la place.

```
debug level 3 component "icm:Router A" subcomponent icm:rtr
```

Tirez les journaux du routeur

Employez l'utilitaire Dumplog afin de tirer des journaux du routeur de l'un ou l'autre de routeur pour le délai prévu des tests. Référez-vous à comment utiliser l'utilitaire Dumplog pour des détails supplémentaires.

C'est un exemple d'une demande de log des logins 10/21/2011 entre 09:00:00 et 09:30:00 (dans le format horaire de 24 heures). Cette sortie va au C de fichier : /router_output.txt :

```
C:\Documents and Settings\ICMAdministrator>cdlog u7x ra
C:\icm\u7x\ra\logfiles>dumplog rtr /bd 10/21/2011 /bt 09:00:00 /ed 10/21/2011
/et 09:30:00 /ms /of C:/router_output.txt
```

Soumettez le fichier de sortie (C : /router_output.txt) à Cisco pour dépanner si nécessaire.

La passerelle trace (le SIP)

Ces commandes activent le suivi sur des serveurs CVP avec le SIP :

```
#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
```

> Remarque: N'importe quelle modification sur un logiciel gw de Cisco IOS® de production pourrait entraîner une panne.

C'est une plate-forme très robuste qui peut manipuler suggéré met au point au volume d'appels fourni sans question. Cependant, Cisco recommande que vous :

- Envoyez tous les logs à un serveur de Syslog au lieu de au tampon de journalisation :

  ```
  logging <syslog server ip>
  logging trap debugs
  ```
- Appliquez les commandes de débogage un par un, et vérifiez l'utilisation du processeur après chacun :

  ```
  show proc cpu hist
  ```

  > Remarque: Si la CPU obtient l'utilisation du processeur jusqu'à 70-80%, le risque d'une incidence en fonction du mérite de service est considérablement augmenté. Ainsi, n'activez pas supplémentaire met au point si le gw frappe 60%.

Activez ces derniers met au point :

```
debug isdn q931
debug voip ccapi inout
```

```
debug ccsip mess
debug http client all
debug voip application vxml all
debug vtsp all
debug voip application all
```
Après que vous fassiez l'appel et simuliez la question, arrêtez l'élimination des imperfections :

```
#undebug all
```
Collectez cette sortie :

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

Suivi de TRANCHANT

Ces commandes activent le suivi de SIP sur le Cisco Unified SIP Proxy (TRANCHANT) :

```
(cusp)> config
(cusp-config)> sip logging
(cusp)> trace enable
(cusp)> trace level debug component sip-wire
```
Souvenez-vous pour tourner se fermer une session une fois que vous êtes fait.

Cette procédure décrit comment collecter les logs :

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

2. Ajoutez cette configuration à la demande de TRANCHANT :

   ```
   username <userid> create
   username <userid> password <password>
   username <userid> group pfs-privusers
   ```
3. FTP à l'adresse IP de TRANCHANT. Utilisez le nom d'utilisateur (test) et le mot de passe comme défini dans l'étape précédente.

4. Répertoires de modification à /cusp/log/trace.

5. Obtenez le log_<filename>.

Utilisation de CLI pour la découverte

Dans la version 8 et ultérieures UCCE, vous pouvez employer l'interface de ligne de commande unifiée de système (CLI) afin de collecter des suivis. Comparé aux utilitaires Dumplog, le CLI est très un rapide et une méthode efficace pour obtenir un jeu complet de logs d'un serveur tel qu'une PAGE ou un Rogger.

Cette procédure décrit comment commencer l'analyse de problème et comment déterminer quel suivi à activer. Les logs de rassemblements d'exemple de ces serveurs :

- ROUTER-A/ROUTER-B
- LOGGER-A/LOGGER-B

- PGXA/PGXB
- Tous les serveurs d'appel CVP
- Tous les serveurs CVP VXML/Media (si présent)

1. Sur chaque système dans la liste, ouvrez le système unifié CLI sur chaque serveur, et exécutez cette commande :

   `show tech-support absdatetime mm-dd-yyyy:hh:mm mm-dd-yyyy:hh:mm redirect dir c:\temp`Remplacez la première millimètre-*densité double-yyyy : hh : millimètre de* chaîne avec une date et une heure qui est approximativement 15 minutes avant l'événement.

   Remplacez la deuxième millimètre-*densité double-yyyy : hh : millimètre de* chaîne avec une date et une heure qui est approximativement 15 minutes après que l'événement est résolu. Si l'événement se produit toujours, recueillez au moins 15 minutes.Ceci produit un fichier nommé clioutputX.zip, où X est le prochain nombre dans l'ordre.

2. Exportez les valeurs virgule-séparées par logins de l'application Windows/Sécurité/système de chaque système (CSV) formatent, et sauvegardent à C:\Temp le répertoire.

3. Ajoutez les logs de Windows CSV au zip de l'étape 1, et renommez le fichier zip dans ce format :

   <SERVERNAME>-SystCLILogs-EvntOn-YYYYMMDD_HHMMSS.zip

4. Sur n'importe quel PG agent, collectez les logins le répertoire C:\Program Files\Cisco\Desktop\logs chaque fois que la panne est vue. Zippez les logs dans un fichier avec un nom dans ce format :

   <SERVERNAME>-CADLogs-EvntOn-YYYYMMDD_HHMMSS.zip

   Si vous utilisez l'édition de CAD-navigateur (CAD-BE) ou tous les Produits de Web CAD, recueillez les logs à partir du répertoire de C:\Program Files\Cisco\Desktop\Tomcat\logs, et ajoutez-les au même fichier zip.

   Si vous exécutez sur Windows l'un des 2008 Produits x64, le répertoire de log est sous C:\Program classe (x86)\Cisco\Desktop\…

5. Reliez ces fichiers à la demande de service, ou téléchargez les fichiers au FTP s'ils sont trop grands pour envoyer ou se relier.

Recueillez ces informations complémentaires si possible :

- Le temps de début et d'arrêt d'événement.
- Plusieurs échantillons de l'ANI/DNIS/AgentID impliqué en cas. Au minimum, Cisco a besoin au moins d'un de ces derniers afin de voir l'événement.
- Le RouteCallDetail (RCD) et TerminationCallDetail (TCD) pour le délai prévu entourant l'événement. La requête RCD a lieu :
  CHOISI * De Route_Call_Detail OÙ DbDateTime > « YYYY-MM-DD HH : Millimètre : SS.MMM » et DbDateTime < « YYYY-MM-DD HH : Millimètre : SS.MMM »La requête TCD a

lieu :
CHOISI * Du Termination_Call_Detail OÙ DbDateTime > « YYYY-MM-DD HH : Millimètre : SS.MMM » et DbDateTime < « YYYY-MM-DD HH : Millimètre : SS.MMM »

Exemple CLI

> Remarque: On t'avertit que ces actions pourraient affecter le système, ainsi vous pouvez vouloir effectuer ce travail pendant outre des heures ou pendant un temps lent.

Il y a deux outils : un outil diagnostique de cadre et l'outil du système CLI. Chacun des deux sont des icônes sur l'appareil de bureau ou sous le répertoire de programmes sur chaque serveur.

Cette procédure décrit comment utiliser le système unifié CLI pour la découverte.

1. Cliquez sur l'icône unifiée du système CLI, puis la procédure de connexion avec le domaine et le nom d'utilisateur. (Dans cet exemple, l'administrateur de domaine a ouvert une session avant, ainsi le CLI connaît déjà le domaine (JecodyEntLab) et le nom d'utilisateur (Jcody).

2. Entrez le mot de passe.

3. Écrivez le nom d'exemple ; dans cet exemple, c'est v802. Regardez à la PAGE un des services ; le nom d'exemple est la première partie du nom de service.

4. Un moyen simple de trouver le nom d'exemple est de regarder les services qui exécutent sur le serveur.

5. Une fois que vous voyez le message d'accueil, sélectionnez cette commande :

   `show tech-support absdatetime mm-dd-yyyy:hh:mm mm-dd-yyyy:hh:mm redirect dir c:\temp`
   Remplacez la première millimètre-*densité double-yyyy : hh : millimètre de* chaîne avec une date et une heure qui est approximativement 15 minutes avant l'événement.

   Remplacez la deuxième millimètre-*densité double-yyyy : hh : millimètre de* chaîne avec une date et une heure qui est approximativement 15 minutes après que l'événement est résolu.

   Si l'événement se produit toujours, recueillez au moins 15 minutes.

   Ceci produit un fichier nommé clioutputX.zip, où X *est le* prochain nombre dans l'ordre.

6. Une fois que le processus se termine, recherchez le fichier clioutputX.zip dans le répertoire :

   Remarque: Ce fichier est en général très grand parce qu'il contient tous les fichiers liés UCCE pour tous les services sur ce serveur.
7. Si vous avez besoin de seulement un log, vous pouvez le trouver plus facile d'utiliser l'utilitaire Dumplog plus ancien ou d'utiliser le portique diagnostique de cadre :