

# Cisco Unified Contact Center Enterprise 再スキルアップ ツールの便利なトレース設定

## 目次

[はじめに](#)

[Q.](#)

[A.](#)

## 概要

このドキュメントでは、バージョン 11.x よりも前の Unified Contact Center Enterprise ( UCCE ) バージョンの UCCE リスキル ツールの便利なトレース設定について説明します。これは、以下の質問に関する情報をどこで見つけるか示す場合に役立ちます。

**Q.**

1. リスキルはいつ行われましたか？
2. 誰 (たとえば、どのスーパーバイザ アカウント) がリスキルを行いましたか？
3. スーパーバイザは何を行いましたか？つまり、どのスキル グループがどのエージェントに対して追加/削除されましたか？
4. どこでどの PC が特定のスーパーバイザにより使用されましたか？

**A.**

これらの情報を収集するには、次のトレースを有効にする必要があります。

### 1. CMSNode

Windows の [Start] メニューから regedit を開始し、HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Distributor\EMS\CurrentVersion\Library\Processes\cms\EMSTraceMask に移動し、値を [off] に設定します。

ログを収集するには、Windows のコマンドラインを使用し、`cdlog <instance> dis` ( dis はディストリビュータを表します ) および `run dumplog cms /last /of cms.log` と入力します。

### 2. リスキル アプリケーション

`\icm\tomcat\webapps\uiroot\WEB-`

`INF\properties\common\apiserver\logManager\APIServer.properties` に移動し、

`verbosity=LOCAL_DUMP` ( ファイルの下部近辺 ) に変更してロギングを有効にします。デフォルトのロギングは `verbosity=VERBOSITY_NONE` ( オフ ) です。

変更前

```
APIServer.TraceFilter.localTraceFilter.className=com.cisco.ics.util.log.trace.WLTraceMessageFilter
```

```
  APIServer.TraceFilter.localTraceFilter.verbosity=VERBOSITY_NONE
```

```
  『
```

```
  APIServer.TraceFilter.localTraceFilter.className=com.cisco.ics.util.log.trace.WLTraceMessageFilter
```

```
  APIServer.TraceFilter.localTraceFilter.verbosity=LOCAL_DUMP
```

問題が再発生した場合、C:\icm\tomcat\webapps\uiroot\WEB-INF\logs\? からログを収集します。

### 3. Apache Tomcat

ステップ 1：ファイル C:\icm\tomcat\conf\server.xml を別のフォルダにバックアップします。

ステップ 2：Windows サービスから Apache Tomcat サービスを停止します。

ステップ 3：強調表示されている部分を追加して、ファイル \icm\tomcat\conf\server.xml を変更します。

```
<Host name="localhost" appBase="webapps"
unpackWARs="true" autoDeploy="true"
xmlValidation="false" xmlNamespaceAware="false">
```

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log." suffix=".txt" pattern="common" resolveHosts="false"
</Host>
```

ステップ 4：Tomcat サービスを開始します。

\icm\tomcat\logs\ で localhost\_access\_log.2014-02-14.txt で始まるファイルを収集します。

ここで、最初に提示した質問に戻ります。

#### 質問 1 リスキルはいつ行われましたか？

CMSNode ログまたはリスキル アプリケーション ログでアクティビティを確認します。

ログの例を次に示します。

-----CMSNode ログ-----

```
11:26:44:208 dis-cms Trace: [2014/06/16 12:26:44] [ProcessID=5236, ThreadID=5524] 8 DIAG-TRACE (42071) Process: Transporter - PREM Received - [BLOCK-START][REM-START]"2014-6-16-11-26-44""300000""192.168.250.63:87999af:14506964d71:-8000""192.168.250.63:-59aa96ef:146a1f65ce4:-7ff4""6""4""0""""IPCCAdmin""2""175""0""1584""[REM-END][STATUS-START]"2014-6-16-11-26-44""0""0""0""0""0""0""0""0""0""0""0""0""0""0""[STATUS-END][VECTOR-START][TABLE-START]"Skill_Group_Member"[COLUMN-START]"SkillGroupSkillTargetID""AgentSkillTargetID"[COLUMN-END][ROW-START]"1""2""0""5004""5001"[ROW-END][TABLE-END][VECTOR-END][BLOCK-END] CMSSVR.DLL E:\Jenkins\workspace\SHARED_ICM\icm\AW\Cms\CmsSvr\cmssvr.cpp Line #523
```

CMS ログで IPCCAdmin を検索します。リスキル ツールである IPCCAdmin アプリケーションが 11:26:44 にアクティビティを実行したことが分かります。リスキル アプリケーション ログでも、同じタイムスタンプの同じアクティビティを確認できます。ipccAdmin.reskill.saveAgent を検索します。

-----リスキル アプリケーションのログ-----

```
06/16/2014 11:26:44.195 TRACE LOCAL_DUMP "Servlet com.cisco.ics.inf.servlet.UIServlet"
com.cisco.ics.inf.servlet.UIServlet UIServlet.service "UIServlet_13 :
start=1402882004194SID=24tlnjkq30 SD = null req =
```

ipccAdmin.reskill.saveAgent" "" - HTTP Servlet Request for URL:

http://192.168.250.63/uiroot/uicommander

Parameters:

personChangeStamp = 1

lastName = One

agentChangeStamp = 4  
loginEnabled = true  
useDBListCachedParams = false  
create = false  
agentID = 1001  
agentTeamID = Team1  
description =  
skgIDList = 5004  
deskSetting = ADS\_Default  
SkillGroupsEditListInput = 5004  
firstName = agent1  
req = ipccAdmin.reskill.saveAgent  
key = 5001  
supervisorAgent = false  
loginName = agent1

### 質問 2 誰 (どのスーパーバイザ アカウント) がリスキルを行いましたか?

これは、リスキル アプリケーションのログでのみ確認できます。以下にサンプル ログの一部を示します。

```
06/16/2014 11:44:04.846 TRACE CLASS_DUMP "Command Dispatch"  
com.cisco.ics.inf.uiserver.APIServer APIServer.dispatchCommand "UIServlet_15 :  
start=1402883044845SID=24tlnjkq30 SD = default req = ipccAdmin.reskill.loginSupervisor" "" -  
Command dump: message: name = ipccAdmin.reskill.loginSupervisor  
<u>MsgProperties for ipccAdmin.reskill.loginSupervisor</u>  
<ul>  
<li>password (value suppressed)  
<li>name = supervisor1  
<li>req = ipccAdmin.reskill.loginSupervisor  
<li>svcDomain = default  
<li>loginByAgentID = false  
</ul>
```

ipccAdmin.reskill.loginSupervisor を検索します。supervisor1 がリスキルを行ったことがわかります。

### 質問 3 スーパーバイザは何を行いましたか? たとえば、どのスキル グループがどのエージェントに対して追加/削除されましたか?

この情報は CMS ログまたはリスキル アプリケーション ログから取得できます。以下にサンプル CMS ログの一部を示します。

```
11:26:44:208 dis-cms Trace: [2014/06/16 12:26:44] [ProcessID=5236, ThreadID=5524] 8 DIAG-  
TRACE (42071) Process: Transporter - PREM Received - [BLOCK-START][REM-START]"2014-6-  
16-11-26-44""300000""192.168.250.63:87999af:14506964d71:-8000""192.168.250.63:-  
59aa96ef:146a1f65ce4:-7ff4""6""4""0""IPCCAdmin""2""175""0""1584""[REM-END][STATUS-  
START]"2014-6-16-11-26-44""0""0""0""0""0""0""0""0""[STATUS-END][VECTOR-  
START][TABLE-START]"Skill_Group_Member"[COLUMN-  
START]"SkillGroupSkillTargetID""AgentSkillTargetID"[COLUMN-END]
```

```
[[ROW-START]]"-1""2""0""5004""5001"[ROW-END][TABLE-END][VECTOR-END][BLOCK-END]  
CMSSVR.DLL E:\Jenkins\workspace\SHARED_ICM\icm\AW\Cms\CmsSvr\cmssvr.cpp Line #523
```



Tomcat アクセス ログから、クライアントがアプリケーションにアクセスしたときの IP アドレスが分かります。次に、例を示します。

```
192.168.250.101- - [16/Jun/2014:11:44:02 +1000] "GET  
/uiroot/uicommander?req=ipccAdmin.reskill.logoutSupervisor HTTP/1.1" 200 3769
```

```
192.168.250.101- - [16/Jun/2014:11:44:04 +1000] "POST  
/uiroot/uicommander?svcDomain=default&req=ipccAdmin.reskill.loginSupervisor HTTP/1.1" 200  
3022
```

上記のメッセージから、IP アドレスが 192.168.250.101 のクライアント PC が、11:44 にリスキルアプリケーションからログアウトし、再ログインしたことが分かります。

まとめると、上記のデバッグがオンの場合、リスキル ツールが行ったアクティビティについてより詳しく知ることができます。