Répertoire d'entreprise questions non trouvées de « hôte »

TAC

ID de document : 118699

Mis à jour : Janv. 26, 2015

Contribué par Gagarin Sathiyanarayanan, ingénieur TAC Cisco.

PDF de téléchargement
Copie
Commentaires

Produits connexes

- Cisco Unified Communications Manager (CallManager)

Contenu

Introduction
Les informations importantes
Fonctionner le scénario
L'URL de service de téléphonie est placé à la « application : Cisco/CorporateDirectory » et le HTTP d'utilisations de téléphone
Dépannez
D'autres scénarios quand la question non trouvée de « hôte » se produit
Cisco relatif prennent en charge des discussions de la Communauté

Introduction

Ce document décrit comment dépanner les questions non trouvées de « hôte » dans le répertoire d'entreprise. Les informations importantes concernant ce document sont :

- Le répertoire d'entreprise est Cisco-a fourni le service de téléphonie d'IP par défaut qui installe automatiquement avec Cisco Unified Communications Manager (CUCM).
- La table de « TelecasterService » enregistre les paramètres pour tous les services de téléphonie qui provisioned sur le système.
- Au téléphone quand vous sélectionnez l'option « répertoire d'entreprise », le téléphone envoie une demande de HTTP ou HTTPS à un des serveurs CUCM et est retourné un objet XML comme réponse de HTTPS.

Les informations importantes

- Clarifiez si la question se produit quand vous accédez aux « répertoires » ou le « répertoire d'entreprise ».
- Quel est le champ « URL de service » réglé à sous le service de répertoire d'entreprise ? Si l'URL est placé à la « application : Cisco/CorporateDirectory » puis, basé sur la version de firmware du téléphone, le téléphone fait une demande de HTTP ou HTTPS.Les téléphones qui utilisent la version 9.3.3 et ultérieures de micrologiciels par défaut font une demande HTTPS.
- Quand l'URL de service est placé à la « application : Cisco/CorporateDirectory », le téléphone envoie la demande de HTTPS au serveur qui est premier dans elle est groupe du CallManager (cm).
- Identifiez la topologie du réseau entre le téléphone et le serveur auxquels la demande de HTTPS est envoyée.
- Prêtez l'attention aux Pare-feu, les optimiseurs BLÊMES, et ainsi de suite dans le chemin qui peut relâcher/trafic http de panier.

Fonctionner le scénario

Dans ce scénario, l'URL de service de téléphonie est placé à la « application : Cisco/CorporateDirectory » et les utilisations HTTPS de téléphone.

Cet exemple affiche le fichier de configuration du téléphone avec l'URL correct.

```
<phoneService  type="1" category="0">
<name>Corporate Directory</name>
<url>Application:Cisco/CorporateDirectory</url>
<vendor></vendor>
<version></version>
</phoneService>
```

Du téléphone la console se connecte vous pourra vérifier ces étapes.

1. Le téléphone utilise l'URL HTTPS.`7949 NOT 11:04:14.765155  CVM-appLaunchRequest: [thread=AWT-EventQueue-0] [class=cip.app.G4ApplicationManager] Creating application module - Corporate Directory 7950 ERR 11:04:14.825312 CVM-XsiAppData&colon;:getCdUrl: [thread=appmgr MQThread] [class=cip.app.ar] Using HTTPS URL`
2. Le certificat de Web de Tomcat présenté au téléphone du serveur de répertoires ne sera pas disponible au téléphone. Par conséquent les tentatives de téléphone d'authentifier le certificat par l'intermédiaire du service de vérification de confiance (TV).`7989 ERR 11:04:15.038637  SECD: -HTTPS cert not in CTL, <10.106.111.100:8443> 7990 NOT 11:04:15.038714 SECD: -TVS service available, will attempt via TVS`
3. Les aspects de téléphone dans le theTVS cachent d'abord et sinon le fondent contacte le serveur TV.`7995 NOT 11:04:15.039286  SECD: -TVS Certificate Authentication request 7996 NOT 11:04:15.039394 SECD: -No matching entry found at cache`
4. Puisque la connexion au theTVS est également sécurisée, une authentification de certificat est terminée et ce message est imprimé s'il est réussi.`8096 NOT 11:04:15.173585  SECD: -Successfully obtained a TLS connection to the TVS server`

5. Le téléphone envoie maintenant une demande d'authentifier le certificat.
```
8159 NOT 11:04:15.219065  SECD: -Successfully sent the certificate Authentication
request to TVS server, bytes written : 962
8160 NOT 11:04:15.219141 SECD: -Done sending Certificate Validation request
8161 NOT 11:04:15.219218 SECD: -Authenticate Certificate : request sent to
TVS server - waiting for response
```
6. La réponse "0" des TV signifie que l'authentification était réussie.
```
8172 NOT 11:04:15.220060 SECD: -Authentication Response received, status : 0
```
7. Ce message est affiché et alors vous verrez la réponse.
```
8185 NOT 11:04:15.221043  SECD: -Authenticated the HTTPS conn via TVS

8198 NOT 11:04:15.296173 CVM-[truncated] Received
HTTP/1.1 200 OK^M
X-Frame-Options: SAMEORIGIN^M
Set-Cookie: JSESSIONID=660646D3655BB00734D3895606BCE76F;
Path=/ccmcip/; Secure; HttpOnly^M
Content-Type: text/xml;charset=utf-8^M
Content-Length: 966^M
Date: Tue, 30 Sep 2014 11:04:15 GMT^M
Server: ^M
^M
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><CiscoIPPhoneInput>
<Title>Directory Search</Title><Prompt>Enter search criteria</Prompt><SoftKeyItem>
<Name>Search</Name><Position>1</Position><URL>SoftKey:Submit</URL></SoftKeyItem>
<SoftKeyItem><Name>&lt;&lt;</Name><Position>2</Position><URL>SoftKey:&lt;&lt;</URL>
</SoftKeyItem><SoftKeyItem><Name>Cancel</Name><Position>3</Position>
<URL>SoftKey:Cancel</URL></SoftKeyItem>
<URL>https://10.106.111.100:8443/ccmcip/xmldirectorylist.jsp</URL>
<InputItem><DisplayName>First Name</DisplayName>
<QueryStringParam>f</QueryStringParam><InputFlags>A</InputFlags>
<DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Last Name</DisplayName><QueryStringParam>l</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
```
<DisplayName>La procédure d'authentification de certificat est semblable à ce qui est discuté dans le service de vérification de confiance de contacts de téléphone pour le certificat inconnu.Des captures de paquet (PCAPs) collectées à l'extrémité de téléphone, vous devriez pouvoir vérifier la transmission TV avec l'utilisation de ce filtre - "tcp.port==2445".

Dans les logs simultanés TV :

1. Les suivis d'examen en vue de la main de Transport Layer Security (TLS) secouent.
2. Ensuite, passez en revue le vidage hexadécimal entrant.
```
04:04:15.270 |   debug ipAddrStr (Phone) 10.106.111.121
04:04:15.270 |<--debug
04:04:15.270 |-->debug
04:04:15.270 | debug 2:UNKNOWN:Incoming Phone Msg:
.
.
04:04:15.270 | debug
HEX_DUMP: Len = 960:

04:04:15.270 |<--debug
04:04:15.270 |-->debug
04:04:15.270 | debug 57 01 01 00 00 00 03 ea
.
<<o/p omitted >>
.
04:04:15.271 | debug MsgType : TVS_MSG_CERT_VERIFICATION_REQ
```
3. Les TV récupère les détails d'émetteur.
```
04:04:15.272 |-->CDefaultCertificateReader::GetIssuerName
04:04:15.272 | CDefaultCertificateReader::GetIssuerName got issuer name
```

```
04:04:15.272 |<--CDefaultCertificateReader::GetIssuerName
04:04:15.272 |-->debug
04:04:15.272 | debug tvsGetIssuerNameFromX509 - issuerName :
CN=cucm10;OU=TAC;O=Cisco;L=Blore;ST=KN;C=IN and Length: 43
04:04:15.272 |<--debug
```

4. Les TV vérifie le certificat.
```
04:04:15.272 |   debug tvsGetSerialNumberFromX509 - serialNumber :
6F969D5B784D0448980F7557A90A6344 and Length: 16
04:04:15.272 | debug CertificateDBCache::getCertificateInformation -
Looking up the certificate cache using Unique MAP ID :
6F969D5B784D0448980F7557A90A6344CN=cucm10;OU=TAC;O=Cisco;L=Blore;ST=KN;C=IN
04:04:15.272 | debug CertificateDBCache::getCertificateInformation -
Certificate compare return =0
04:04:15.272 | debug CertificateDBCache::getCertificateInformation -
Certificate found and equal
```

5. Les TV envoie la réponse au téléphone.
```
04:04:15.272 |   debug 2:UNKNOWN:Sending
CERT_VERIF_RES msg
04:04:15.272 | debug MsgType : TVS_MSG_CERT_VERIFICATION_RES
```

L'URL de service de téléphonie est placé à la « application : Cisco/CorporateDirectory » et le HTTP d'utilisations de téléphone

> Remarque: Au lieu de l'utilisation d'une version de firmware plus tôt de téléphone, le service et l'URL sécurisé de service ont été codé en dur à l'URL HTTP. Cependant, la même séquence d'opérations est vue en micrologiciel de téléphone qui se sert du HTTP par défaut.

Le fichier de configuration du téléphone a l'URL correct.

```
<phoneService  type="1" category="0">
<name>Corporate Directory</name>
<url>Application:Cisco/CorporateDirectory</url>
<vendor></vendor>
<version></version>
</phoneService>
```

Du téléphone la console se connecte vous pourra vérifier ces étapes.

```
7250 NOT 11:44:49.981390  CVM-appLaunchRequest: [thread=AWT-EventQueue-0]
[class=cip.app.G4ApplicationManager] Creating application module -
Corporate Directory/-838075552
7254 NOT 11:44:50.061552 CVM-_HTTPMakeRequest1: Processing Non-HTTPS URL
7256 NOT 11:44:50.061812 CVM-_HTTPMakeRequest1() theHostname: 10.106.111.100:8080


7265 NOT 11:44:50.233788 CVM-[truncated] Received
HTTP/1.1 200 OK^M
X-Frame-Options: SAMEORIGIN^M
Set-Cookie: JSESSIONID=85078CC96EE59CA822CD607DDAB28C91;
Path=/ccmcip/; HttpOnly^M
Content-Type: text/xml;charset=utf-8^M
Content-Length: 965^M
Date: Tue, 30 Sep 2014 11:44:50 GMT^M
Server: ^M
^M
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><CiscoIPPhoneInput>
<Title>Directory Search</Title><Prompt>Enter search criteria</Prompt><SoftKeyItem>
<Name>Search</Name><Position>1</Position><URL>SoftKey:Submit</URL></SoftKeyItem>
<SoftKeyItem><Name>&lt;&lt;</Name><Position>2</Position><URL>SoftKey:&lt;&lt;</URL>
</SoftKeyItem><SoftKeyItem><Name>Cancel</Name><Position>3</Position>
```

```
<URL>SoftKey:Cancel</URL></SoftKeyItem>
<URL>http://10.106.111.100:8080/ccmcip/xmldirectorylist.jsp</URL><InputItem>
<DisplayName>First Name</DisplayName><QueryStringParam>f</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Last Name</DisplayName><QueryStringParam>l</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Number</D
```

Du paquet vous capture verra une requête HTTP GET et une RÉPONSE réussie. C'est le PCAP de CUCM :

Dépannez

Avant que vous dépanniez, recueillez les détails de la question répertoriée plus tôt :

Logs à collecter, s'il y a lieu

- Captures simultanées de paquet du téléphone IP et du serveur CUCM (le serveur qui est premier dans lui est groupe cm à où la demande de HTTPS serait envoyée).
- Logs de console de téléphone IP.
- Logs de Cisco TV (détaillés).Quand vous placez les TV se connecte à détaillé, le service doit être redémarré pour que les modifications de niveau de suivi aient lieu. Voir l'ID de bogue Cisco CSCuq22327 pour que l'amélioration annonce qu'une reprise de service est exigée quand des niveaux de log sont changés.

Terminez-vous ces étapes afin d'isoler la question :

Étape 1

Créez un service de test avec ces détails :

```
Service Name : <Any Name>
Service URL : http://<CUCM_IP_Address>:8080/ccmcip/xmldirectoryinput.jsp
Secure-Service URL : http://<CUCM_IP_Address>:8080/ccmcip/xmldirectoryinput.jsp
Service Category : XML Service
Service Type : Directories
Enable : CHECK
Enterprise Subscription : DO NOT CHECK
```

Maintenant, abonnez-vous ce service à un des téléphones affectés :

1. Allez à la page de configuration de périphérique.
2. Choisi **abonnez-vous/désabonnez-vous les services** sous des liens connexes.
3. Abonnez-vous le service de test que vous avez créé.
4. Sauvegardez, appliquez la configuration, et remettez à l'état initial le téléphone. Ce que vous avez fait est, indépendamment de la version FW du téléphone qui détermine si utiliser le HTTP ou URL HTTPS, le forcent pour utiliser l'URL HTTP.Accédez au service de « répertoire d'entreprise » au téléphone.Si cela ne fonctionne pas, alors collecter les logs mentionnés ci-dessus et les comparer au scénario fonctionnant mentionné sous « fonctionner le scénario » et identifier où la déviation est.Si cela fonctionne, alors vous avez au moins confirmé cela du point de vue de service de téléphonie IP CUCM là n'êtes aucune question.Àce stade la question pourrait être le plus probablement avec les téléphones qui utilisent l'URL HTTPS.Maintenant, sélectionnez un téléphone qui ne fonctionne pas et poursuit à l'étape suivante.

Quand cela fonctionne avec cette modification, vous devez décider s'il est CORRECT de laisser la configuration avec la demande/réponse de répertoire d'entreprise qui fonctionne au-dessus du HTTP au lieu de HTTPS. La transmission HTTPS ne fonctionne pas en raison d'une des raisons a discuté ensuite.

Étape 2

Collectez les logs mentionnés précédemment et comparez-les au scénario fonctionnant mentionné sous « fonctionner le scénario » et identifiez où la déviation est.

Il pourrait être l'une de ces questions :

1. Le téléphone ne peut pas contacter le serveur TV. Dans le PCAPS, vérifiez la transmission sur le port 2445.Assurez-vous qu'aucun des périphériques de réseau dans le bloc de chemin ce port.
2. Le téléphone contacte le serveur TV, mais la prise de contact de TLS échoue.Ces lignes seront imprimées dans les logs de console de téléphone :
```
5007: NOT 10:25:10.060663 SECD:
clpSetupSsl: Trying to connect to IPV4,
IP: 192.168.136.6, Port : 2445
5008: NOT 10:25:10.062376 SECD: clpSetupSsl: TCP connect() waiting,
<192.168.136.6> c:14 s:15 port: 2445
5009: NOT 10:25:10.063483 SECD: clpSetupSsl: TCP connected,
<192.168.136.6> c:14 s:15
5010: NOT 10:25:10.064376 SECD: clpSetupSsl: start SSL/TLS handshake,
<192.168.136.6> c:14 s:15
5011: ERR 10:25:10.068387 SECD: EROR:clpState: SSL3 alert
read:fatal:handshake failure:<192.168.136.6>
5012: ERR 10:25:10.069449 SECD: EROR:clpState: SSL_connect:failed in SSLv3
read server hello A:<192.168.136.6>
5013: ERR 10:25:10.075656 SECD: EROR:clpSetupSsl: ** SSL handshake failed,
<192.168.136.6> c:14 s:15
5014: ERR 10:25:10.076664 SECD: EROR:clpSetupSsl: SSL/TLS handshake failed,
<192.168.136.6> c:14 s:15
5015: ERR 10:25:10.077808 SECD: EROR:clpSetupSsl: SSL/TLS setup failed,
<192.168.136.6> c:14 s:15
5016: ERR 10:25:10.078771 SECD: EROR:clpSndStatus: SSL CLNT ERR,
srvr<192.168.136.6>
```
Voir le pour en savoir plus de l'ID de bogue Cisco CSCua65618.

3. Le téléphone contacte les serveurs TV et la prise de contact de TLS est réussie, mais les TV ne peut pas vérifier le signataire du certificat qui le téléphone demandé d'authentifier.Des extraits des logs TV sont répertoriés ici :Le téléphone entre en contact avec les TV.

```
05:54:47.779 |   debug 7:UNKNOWN:Got a new ph conn 10.106.111.121 on 10, Total Acc = 6..
.
.
05:54:47.835 | debug MsgType : TVS_MSG_CERT_VERIFICATION_REQ
```
Les TV obtient le nom d'émetteur.
```
05:54:47.836 |-->CDefaultCertificateReader::GetIssuerName
05:54:47.836 | CDefaultCertificateReader::GetIssuerName got issuer name
05:54:47.836 |<--CDefaultCertificateReader::GetIssuerName
05:54:47.836 |-->debug
05:54:47.836 | debug tvsGetIssuerNameFromX509 - issuerName :
CN=cucmpub9;OU=TAC;O=Cisco;L=Bangalore;ST=KN;C=IN and Length: 49
```
Il des consultations le certificat, mais ne peut pas le trouver.
```
05:54:47.836 |   debug
CertificateCTLCache::getCertificateInformation
- Looking up the certificate cache using Unique MAP ID :
62E09123B09A61D20E77BE5BF5A82CD4CN=cucmpub9;OU=TAC;O=Cisco;L=Bangalore;ST=KN;C=IN
```

```
05:54:47.836 |<--debug
05:54:47.836 |-->debug
05:54:47.836 | debug ERROR:CertificateCTLCache::getCertificateInformation
- Cannot find the certificate in the cache
05:54:47.836 |<--debug
05:54:47.836 |-->debug
05:54:47.836 | debug getCertificateInformation(cert) : certificate not found
```

4. Le trafic HTTPS est bloqué/abandonné quelque part dans le réseau.Obtenez PCAPs simultané du téléphone et du serveur CUCM afin de vérifier la transmission.

D'autres scénarios quand la question non trouvée de « hôte » se produit

1. Le serveur CUCM est défini par l'adresse Internet avec des questions dans la résolution de noms.
2. La liste de serveur TV est vide au téléphone quand elle télécharge le fichier xmldefault.cnf.xml. (Dans la version 8.6.2 le fichier de configuration par défaut n'aura pas l'entrée TV dans lui dû à l'ID de bogue Cisco CSCti64589.)
3. Le téléphone ne peut pas utiliser l'entrée TV dans le fichier de configuration parce qu'il a téléchargé le fichier xmldefault.cnf.xml. Voir l'ID de bogue Cisco CSCuq33297 - Phoneto analysent les informations TV à partir du fichier de configuration par défaut.
4. Le répertoire d'entreprise ne fonctionne pas après une mise à jour CUCM parce que les mises à jour du firmware de téléphone à une version ultérieure qui change par la suite le comportement de l'utilisation de HTTPS par défaut.

Cisco relatif prennent en charge des discussions de la Communauté

Mis à jour : Janv. 26, 2015
ID de document : 118699