协作边缘TC根据终端配置示例

目录

简介

本文描述什么要求为了配置和排除故障网真编码(TC) -基于终端注册通过莫比尔和远程访问解决方案。

先决条件

要求

Cisco 建议您了解以下主题：

- 莫比尔和远程访问解决方案
- 视频通信服务器(VCS)证书
- Expressway X8.1.1或以上
- Cisco Unified Communications管理器(CUCM)版本9.1.2或以上
- 基于TC的终端

使用的组件

本文档中的信息基于以下软件和硬件版本：

- VCS X8.1.1或以上
- CUCM版本9.1(2)SU1或以上和IM &在线状态9.1(1)或以上
- TC 7.1或以上固件**(推荐的TC7.2)**
- VCS控制& Expressway/Expressway核心&边缘
- CUCM
- TC终端

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

这些配置步骤假设，管理员将配置安全设备已注册的基于TC的终端。安全注册不是需求，然而整体莫比尔和远程访问解决方案指南有印象是，因为有显示在CUCM的安全设备配置文件从配置的屏幕画面。

创建在CUCM的安全电话配置文件在FQDN格式(可选)

1. 在CUCM，请选择**系统> Security >电话安全配置文件**。
2. 单击新增。
3. 选择基于TC的终端类型并且配置这些参数： 名称- **Secure-EX90.tbtp.local (要求的FQDN格式)**设备安全性模式-**已加密**传输类型- **TLS**SIP电话波尔特- **5061**

保证团星安全模式是(1) -混合(可选)

1. 在CUCM，请选择**System > Enterprise Parameters**。
2. 移下来对**安全参数>团星安全模式> 1。**

如果值不是1 CUCM未获取。如果这是实际情形，管理员需要查看这两个文档之一为了获取CUCM。

CUCM 9.1(2)安全指南

CUCM 10安全指南

创建在CUCM的配置文件基于TC的终端的

1. 在CUCM，请选择**Device > Phone**。
2. 单击新增。
3. 选择基于TC的终端类型并且配置这些参数： MAC地址-从基于TC的设备的MAC地址需要的担任主角的字段(*)所有者-用户所有者用户ID -用设备关联的所有者设备安全性配置文件-以前已配置的配置文件(Secure-EX90.tbtp.local)SIP配置文件-英文虎报SIP配置文件或以前创建的任何自定义配置文件

添加安全配置文件名称到ExpresswayC/VCS C证书的SAN (可选)

1. 在ExpresswayC/VCS C，请选择**维护> Security证书>Server证书**。
2. 单击**生成CSR**。
3. 填写证书签名请求(CSR)字段并且保证“Unified CM电话安全配置文件名称”有列出的确切的电话安全配置文件在完全合格的域名(FQDN)格式。例如， Secure-EX90.tbtp.local。**注意**：Unified CM电话安全配置文件名称是列出的在附属的替代名称(SAN)字段的上一步。
4. 发送CSR对将签字的一内部或第三方Certificate Authority (CA)。
5. 选择**维护> Security证书>Server证书**为了上传证书到ExpresswayC/VCS C。

添加UC域到ExpresswayE/VCS E证书

1. 在ExpresswayE/VCS E，请选择**维护> Security证书>Server证书**。
2. 单击**生成CSR**。
3. 填写CSR字段并且保证“统一域”包含域基于TC的终端将做协作边缘的CM注册(collab边缘)请求，在域名服务器(DNS)或服务名称(SRV)格式。
4. 发送CSR对将签字的内部或第三方CA。
5. 选择**维护> Security证书>Server证书**为了上传证书到ExpresswayE/VCS E。

安装适当的委托CA证书对基于TC的终端

1. 在基于TC的终端，请选择**Configuration>安全**。
2. 选择**CA**选项卡并且为签署您的ExpresswayE/VCS E证书的CA证书浏览。
3. 单击**添加得认证机关**。**注意**：一旦证书成功地添加您看到在证书列表列出了。**注意**：TC 7.2包含一被事先装配的CA列表。如果签署ExpresswayE证书的CA在此列表内包含，在此部分列出的步骤没有要求。**注意**：被事先装配的CA页包含方便“配置当前设置”把您带直接地对在下一部分的步骤注释的必需的配置2的按钮。

设置边缘供应的基于TC的终端

1. 在基于TC的终端，请选择**Configuration>网络**并且保证这些字段适当地填写在DNS部分下：
   域名服务器地址
2. 在基于TC的终端，请选择**设置的Configuration>**并且保证这些字段适当地被填装在：
   LoginName -如对CUCM定义模式-**边缘**密码-如对CUCM定义
   外部管理器地址-您的ExpresswayE/VCS E主机名域-域您的collab边缘记录存在的地方

验证

使用本部分可确认配置能否正常运行。

基于TC的终端

1. 在Web GUI中，请导航给“霍姆”。正在寻找‘SIP代理部分“注册”状态的1"。代理地址是您的ExpresswayE/VCS E。
2. 从CLI，回车**xstatus //prov**。如果注册您应该看到供应状态“已配置”。 **xstatus //prov**

```
*s Network 1 IPv4 DHCP ProvisioningDomain: ""
*s Network 1 IPv4 DHCP ProvisioningServer: ""
*s Provisioning CUCM CAPF LSC: Installed
*s Provisioning CUCM CAPF Mode: IgnoreAuth
*s Provisioning CUCM CAPF OperationResult: NotSet
*s Provisioning CUCM CAPF OperationState: NonPending
*s Provisioning CUCM CAPF ServerName: ""
*s Provisioning CUCM CAPF ServerPort: 0
*s Provisioning CUCM CTL State: Installed
*s Provisioning CUCM ExtensionMobility Enabled: False
*s Provisioning CUCM ExtensionMobility LastLoggedInUserId: ""
*s Provisioning CUCM ExtensionMobility LoggedIn: False
*s Provisioning CUCM ITL State: Installed
*s Provisioning CUCM ProvisionSecurity: Signed
*s Provisioning CUCM TVS Proxy 1 IPv6Address: ""
*s Provisioning CUCM TVS Proxy 1 Port: 2445
*s Provisioning CUCM TVS Proxy 1 Priority: 0
*s Provisioning CUCM TVS Proxy 1 Server: "xx.xx.97.131"
*s Provisioning CUCM UserId: "pstojano"
*s Provisioning NextRetry: ""
*s Provisioning Reason: ""
*s Provisioning Server: "xx.xx.97.131"
*s Provisioning Software Current CompletedAt: ""
*s Provisioning Software Current URL: ""
*s Provisioning Software Current VersionId: ""
*s Provisioning Software UpgradeStatus LastChange: "2014-06-30T19:08:40Z"
*s Provisioning Software UpgradeStatus Message: ""
*s Provisioning Software UpgradeStatus Phase: None
*s Provisioning Software UpgradeStatus SecondsUntilUpgrade: 0
*s Provisioning Software UpgradeStatus SessionId: ""
*s Provisioning Software UpgradeStatus Status: None
*s Provisioning Software UpgradeStatus URL: ""
*s Provisioning Software UpgradeStatus VersionId: ""
*s Provisioning Status: Provisioned
** end
```

CUCM

在CUCM，请选择**Device > Phone**。请通过列表移动或过滤根据您的终端的列表。您应该看到“注册与%CUCM_IP%”消息。在此右边的IP地址应该是代理注册的您的ExpresswayC/VCS C。

ExpresswayC

1. 在ExpresswayC/VCS C，请选择**状态>统一通信>视图供应会话。**
2. 由您基于TC的终端的IP地址过滤。一已配置会话的示例显示此处：

故障排除

本部分提供的信息可用于对配置进行故障排除。

注册问题可以由包括DNS，证书问题，配置的许多要素导致，等等。此部分包括全面列表什么您典型地会看到，如果如何遇到一给的问题和对修正它。如果遇到问题的外部什么已经描述了，请感到自由包括它。

工具

最初，请注意工具在您的处理。

TC终端

Web GUI

- all.log
- 启动延长的记录日志(请包括完整的信息包捕获)

CLI

这些命令是最有利为了排除故障在实时：

- 日志ctx HttpClient调试9
- 日志ctx PROV调试9
- 日志输出在<--通过控制台显示记录日志

有效方式再现问题将再按乒乓键从“边缘的”供应模式对Off然后回到“边缘”在Web GUI内。您能也输入**xConfiguration供应模式：**in命令CLI。

高速公路

- 诊断记录
- Tcpdump

CUCM

- SDI/SDL跟踪

问题1 ：Collab边缘记录不可视并且/或者主机名不可解决

正如你看到的get_edge_config发生故障由于名字解析。

TC终端日志

```
15716.23 HttpClient   HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Couldn't resolve host name'

15716.23 PROV ProvisionRequest failed: 4 (Couldn't resolve host name)
15716.23 PROV I: notify_http_done: Received 0 (Couldn't resolve host name) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
```

修正

1. 如果collab边缘记录是存在并且返回正确主机名，请验证。
2. 如果在客户端配置的DNS服务器信息正确，请验证。

问题2 ：CA在基于TC的终端的委托CA列表内不是存在

TC终端日志

```
15975.85 HttpClient     Trying xx.xx.105.108...
15975.85 HttpClient Adding handle: conn: 0x48390808
15975.85 HttpClient Adding handle: send: 0
15975.86 HttpClient Adding handle: recv: 0
15975.86 HttpClient Curl_addHandleToPipeline: length: 1
15975.86 HttpClient - Conn 64 (0x48396560) send_pipe: 0, recv_pipe: 0
15975.87 HttpClient - Conn 65 (0x4835a948) send_pipe: 0, recv_pipe: 0
15975.87 HttpClient - Conn 67 (0x48390808) send_pipe: 1, recv_pipe: 0
15975.87 HttpClient Connected to RTP-TBTP-EXPRWY-E.tbtp.local (xx.xx.105.108)
port 8443 (#67)
15975.87 HttpClient successfully set certificate verify locations:
15975.87 HttpClient CAfile: none
CApath: /config/certs/edge_ca_list
15975.88 HttpClient Configuring ssl context with special Edge certificate verifier
15975.88 HttpClient SSLv3, TLS handshake, Client hello (1):
15975.88 HttpClient SSLv3, TLS handshake, Server hello (2):
15975.89 HttpClient SSLv3, TLS handshake, CERT (11):
15975.89 HttpClient SSLv3, TLS alert, Server hello (2):
15975.89 HttpClient SSL certificate problem: self signed certificate in
certificate chain
15975.89 HttpClient Closing connection 67
15975.90 HttpClient HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Peer certificate cannot be authenticated with given CA certificates'

15975.90 PROV ProvisionRequest failed: 4 (Peer certificate cannot be
authenticated with given CA certificates)
15975.90 PROV I: notify_http_done: Received 0 (Peer certificate cannot be
authenticated with given CA certificates) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
15975.90 PROV EDGEProvisionUser: start retry timer for 15 seconds
```

修正

1. 如果第三方CA是列出的在终端的**安全> CA**选项卡下请验证。
2. 如果CA是列出的，请验证正确。

问题3 ：ExpresswayE没有在SAN内列出的UC域

TC终端日志

```
82850.02 CertificateVerification ERROR: [verify_edge_domain_in_san]: Edge TLS
verification failed: Edge domain 'tbtp.local' and corresponding SRVName
'_collab-edge._tls.tbtp.local' not found in certificate SAN list
82850.02 HttpClient SSLv3, TLS alert, Server hello (2):
82850.02 HttpClient SSL certificate problem: application verification failure
82850.02 HttpClient Closing connection 113
82850.02 HttpClient HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Peer certificate cannot be authenticated with given CA certificates'
```

ExpresswayE SAN

X509v3 Subject Alternative Name:
DNS:RTP-TBTP-EXPRWY-E.tbtp.local, SRV:_collab-edge._tls.tbtppppp.local

修正

1. 再生ExpresswayE CSR为了包括UC域。
2. 很可能，在TC终端“ExternalManager域”参数没有设置对什么UC域是。如果这是实际情形您必须匹配它。

问题4 ：在TC和密码供应的用户名设置配置文件不正确

TC终端日志

```
83716.67 HttpClient     Server auth using Basic with user 'pstojano'
83716.67 HttpClient GET /dGJ0cC5jb20/get_edge_config/ HTTP/1.1
Authorization: xxxxxx
Host: RTP-TBTP-EXPRWY-E.tbtp.local:8443
Cookie: JSESSIONIDSSO=34AFA4A6DEE1DDCE8B1D2694082A6D0A
Content-Type: application/x-www-form-urlencoded
Accept: text/xml
User-Agent: Cisco/TC
Accept-Charset: ISO-8859-1,utf-8
83716.89 HttpClient HTTP/1.1 401 Unauthorized
83716.89 HttpClient Authentication problem. Ignoring this.
83716.90 HttpClient WWW-Authenticate: Basic realm="Cisco-Edge"
83716.90 HttpClient Server CE_C ECS is not blacklisted
83716.90 HttpClient Server: CE_C ECS
83716.90 HttpClient Date: Thu, 25 Sep 2014 17:42:51 GMT
83716.90 HttpClient Age: 0
83716.90 HttpClient Transfer-Encoding: chunked
83716.91 HttpClient Connection: keep-alive
83716.91 HttpClient
83716.91 HttpClient 0
83716.91 HttpClient Connection #116 to host RTP-TBTP-EXPRWY-E.tbtp.local
left intact
83716.91 HttpClient HTTPClientCurl received HTTP error 401

83716.91 PROV ProvisionRequest failed: 5 (HTTP code=401)
83716.91 PROV I: notify_http_done: Received 401 (HTTP code=401) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
```

ExpresswayC/VCS C

```
2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C edgeconfigprovisioning
UTCTime="2014-09-25 17:46:20,92" Module="network.http.edgeconfigprovisioning"
Level="DEBUG" Action="Received"
Request-url="https://xx.xx.97.131:8443/cucm-uds/user/pstojano/devices"
HTTPMSG:
|HTTP/1.1 401 Unauthorized
Expires: Wed, 31 Dec 1969 19:00:00 EST
Server:
Cache-Control: private
Date: Thu, 25 Sep 2014 17:46:20 GMT
Content-Type: text/html;charset=utf-8
WWW-Authenticate: Basic realm="Cisco Web Services Realm"

2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C UTCTime="2014-09-25 17:46:20,92"
Module="developer.edgeconfigprovisioning.server" Level="DEBUG"
CodeLocation="edgeprotocol(1018)" Detail="Failed to authenticate user against server"
Username="pstojano" Server="('https', 'xx.xx.97.131', 8443)"
```

```
Reason="<twisted.python.failure.Failure <type 'exceptions.Exception'>>
"2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C edgeconfigprovisioning:
Level="INFO" Detail="Failed to authenticate user against server" Username="pstojano"
Server="('https', 'xx.xx.97.131', 8443)" Reason="<twisted.python.failure.Failure
<type 'exceptions.Exception'>>" UTCTime="2014-09-25 17:46:20,92"
```

修正

1. 验证用户名/密码被输入在TC终端的供应页下有效。
2. 验证凭证CUCM数据库。 版本10 -请使用Self关心门户版本9 -请使用CM用户选项

两个门户的URL是相同的：https://%CUCM%/ucmuser/

如果提交与一个不足的权利错误，请保证这些角色分配到用户：

- Standard CTI Enabled
- 标准的CCM最终用户

问题5 ：基于TC的终端注册被拒绝

CUCM跟踪

```
08080021.043 |16:31:15.937 |AppInfo  |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate, Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local,
Expected=SEP00506006EAFE. Will check SAN the next
08080021.044 |16:31:15.937 |AppInfo |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate Error , did not find matching SAN either,
Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local, Expected=Secure-EX90.tbtp.local
08080021.045 |16:31:15.937 |AppInfo |ConnectionFailure - Unified CM failed to open
a TLS connection for the indicated device Device Name:SEP00506006EAFE
IP Address:xx.xx.97.108 IPV6Address: Device type:584 Reason code:2 App ID:Cisco
CallManager Cluster ID:StandAloneCluster Node ID:RTP-TBTP-CUCM9 08080021.046
|16:31:15.938 |AlarmErr |AlarmClass: CallManager, AlarmName: ConnectionFailure,
AlarmSeverity: Error, AlarmMessage: , AlarmDescription: Unified CM failed to open
a TLS connection for the indicated device, AlarmParameters:
DeviceName:SEP00506006EAFE, IPAddress:xx.xx.97.108, IPV6Address:,
DeviceType:584, Reason:2, AppID:Cisco CallManager, ClusterID:StandAloneCluster,
NodeID:RTP-TBTP-CUCM9,
```

TC终端

实际ExpresswayC/VCS C

```
08080021.043 |16:31:15.937 |AppInfo  |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate, Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local,
Expected=SEP00506006EAFE. Will check SAN the next
08080021.044 |16:31:15.937 |AppInfo |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate Error , did not find matching SAN either,
Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local, Expected=Secure-EX90.tbtp.local
08080021.045 |16:31:15.937 |AppInfo |ConnectionFailure - Unified CM failed to open
a TLS connection for the indicated device Device Name:SEP00506006EAFE
IP Address:xx.xx.97.108 IPV6Address: Device type:584 Reason code:2 App ID:Cisco
CallManager Cluster ID:StandAloneCluster Node ID:RTP-TBTP-CUCM9 08080021.046
|16:31:15.938 |AlarmErr |AlarmClass: CallManager, AlarmName: ConnectionFailure,
AlarmSeverity: Error, AlarmMessage: , AlarmDescription: Unified CM failed to open
a TLS connection for the indicated device, AlarmParameters:
DeviceName:SEP00506006EAFE, IPAddress:xx.xx.97.108, IPV6Address:,
DeviceType:584, Reason:2, AppID:Cisco CallManager, ClusterID:StandAloneCluster,
NodeID:RTP-TBTP-CUCM9,
```

在此特定日志示例中很清楚ExpresswayC/VCS C不包含在SAN的电话安全配置文件FQDN。(Secure-EX90.tbtp.local)。在传输层安全(TLS)握手， CUCM检查Expressway C/VCS C的服务器证

书。因为它没在SAN内找到它投掷粗体的错误并且报道预计了在FQDN格式的电话安全配置文件。

修正

1. 验证ExpresswayC/VCS C包含在FQDN格式的电话安全配置文件在SAN它内是服务器证书。
2. 验证设备在CUCM使用正确安全配置文件，如果在FQDN格式使用一安全配置文件。
3. 这能由Cisco Bug ID CSCuq86376也造成。如果这是案件检查ExpresswayC/VCS C SAN大小和电话安全配置文件的位置在SAN内的。

相关信息

- 莫比尔&远程访问指南
- VCS证书创建指南
- EX90/EX60入门指南
- CUCM 9.1管理员指南
- 技术支持和文档 - Cisco Systems