在12.0版及更高版本中将ECE与PCCE集成

目录

简介

本文档介绍在版本12.0及更高版本中将企业聊天和电子邮件(ECE)与Packaged Contact Center Enterprise(PCCE)集成的步骤

先决条件

要求

Cisco 建议您了解以下主题：

- 企业聊天和电子邮件(ECE)12.x

- 套装联络中心企业版(PCCE)12.x

使用的组件

本文档中的信息基于以下软件版本：

- ECE 12.5(1)
- PCCE 12.5(1)

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。

背景信息

PCCE 12.0版引入了称为单一管理平台(SPOG)的新管理界面。 现在，几乎所有联系中心和相关应用的管理都在此界面中执行。要正确集成ECE和PCCE，您必须完成此集成独有的几个步骤。本文档将指导您完成此过程。

术语

在本文档中，使用这些术语。

- 企业聊天和电子邮件(ECE)- ECE是允许以与语音呼叫相同的方式将电子邮件和聊天请求路由到联系中心座席的产品。
- 单一管理平台(SPOG)- SPOG是PCCE管理在12.0版及更高版本中执行的方式。SPOG是对CCE管理工具的完全重写，该工具在12.0之前的版本中使用。
- 证书颁发机构(CA) — 根据公钥基础设施(PKI)模型颁发数字证书的实体。 您可能会遇到两种类型的CA。公共CA — 公共CA是大多数浏览器和操作系统都包含其根证书和中间证书的CA。一些常见公共CA包括IdenTrust、DigiCert、GoDaddy和GlobalSign。专用CA — 专用CA是公司内部存在的专用CA。某些专用CA由公共CA签名，但通常这些CA是独立CA，并且它们颁发的证书仅受该组织中的计算机信任。在这两种CA类型中，有两种类型的CA服务器。根CA服务器 — 根CA服务器签署自己的证书。在标准的多层PKI部署中，根CA处于脱机状态且无法访问。此模型中的根CA也仅向另一个CA服务器（称为中间CA）颁发证书。有些公司选择仅使用单层CA。在此模型中，根CA颁发证书，以供其他CA服务器以外的实体使用。中间CA服务器 — 中间或颁发CA服务器颁发证书，以供其他CA服务器以外的实体使用。
- Microsoft管理控制台(MMC)- Microsoft Windows附带的允许加载各种管理单元的应用程序。您可以使用管理单元构建用于服务器管理的自定义控制台。Windows中包含许多不同的管理单元。示例的简单列表包括证书、设备管理器、磁盘管理、事件查看器和服务。
- 网络负载均衡器(NLB) — 向具有公用物理名称的最终用户显示多个物理资源的设备或应用。NLB在Web应用和服务中非常常见。NLB可以通过多种方式实施。当与ECE配合使用时，NLB的配置必须确保用户会话通过使用cookie插入或等效方法返回到同一物理后端Web服务器。这称为带cookie插入的粘滞会话。粘滞会话只是指负载均衡器将用户会话返回到所有交互的同一物理后端服务器的能力。 安全套接字层(SSL)直通 — SSL直通是一种方法，其中最终用户设备与分配了用户会话的物理Web服务器之间存在SSL会话。SSL直通不允许Cookie插入，因为HTTP会话始终以物理方式加密。大多数NLB通过使用单条表支持使用SSL直通的粘滞会话，该单条表监控会话设置的serverhello和clienthello部分并将唯一值存储在表中。当向NLB显示与这些值匹配的下一个请求时，可以使用单条表将会话返回到同一后端服务器。SSL卸载 —

当为SSL卸载配置NLB时，存在两个SSL会话或隧道，适用于任何给定的最终用户会话。第一个是在最终用户设备和在NLB上为网站配置的虚拟IP(VIP)之间。第二个是NLB的后端IP与分配用户会话的物理Web服务器之间。SSL卸载支持cookie插入，因为HTTP流在NLB上完全解密，在NLB上可以插入其他HTTP Cookie并可以执行会话检查。当Web应用不需要SSL，而是为了安全起见时，通常使用SSL卸载。当前版本的ECE不支持在非SSL会话中访问应用。

必备步骤

在开始集成两个系统之前，必须完成几个先决条件。

- 最低PCCE补丁级别 版本12.0(1)- ES37版本12.5(1) — 基本功能当前无最低要求
  Webex体验管理(WXM)分析器功能需要ES7
- 最低ECE补丁级别 建议ECE运行最新的工程特别计划(ES)。版本12.0(1)- ES3 + ES3_ET1a版本12.5(1) — 基本功能当前无最低要求
  WXM分析器功能需要ES1
- 配置项 确保将ECE_Email、ECE_Chat和ECE_Outbound媒体路由域(MRD)与正确的应用实例关联。对于PCCE 2000代理部署模式，应用实例为MultiChannel。对于PCCE 4000/12000代理部署模型，应用实例的形式为{site}_{peripheral_set}_{application_instance}。
  如果安装的PCCE的站点名称为Main，外围设备设置为PS1，应用实例设置为Multichannel，则应用实例名称为Main_PS1_Multichannel。**注意：**应用实例名称区分大小写。确保在将ECE Web服务器添加到资产时正确键入名称。

集成步骤

本文档中所有步骤的详细信息都包含在ECE和PCCE的文档中，但它们不显示在列表中，也不都在同一文档中。有关详细信息，请参阅本文档末尾包含的链接。

步骤1.配置SSL证书

必须生成ECE Web服务器要使用的证书。您可以使用自签名证书，但通常使用CA签名证书更容易。自签名证书的安全性不低于CA签名证书，最初创建证书的步骤更少，但当需要替换证书时，必须记住将新证书上传到所有PCCE管理数据服务器上的Java密钥库。如果使用CA签名的证书，则只需上传根证书（如果存在）和中间证书到密钥库。

如果您的部署中有多个Web服务器，则必须查看这些准则。配置网络负载均衡器所需的具体步骤不在本文档的讨论范围之内。如果需要，请与负载均衡器供应商联系以获得帮助。

虽然不需要负载均衡器，但可以大大简化实施

访问每台Web服务器上的ECE应用程序必须使用SSL，而不管使用哪种负载均衡器方法

负载均衡器可配置为SSL直通或SSL卸载

如果选择SSL直通，则必须执行以下操作：您必须从一台服务器执行所有证书操作

正确配置证书后，您必须导出证书并确保私钥包含到个人信息交换(PFX)文件

您必须将PFX文件复制到部署中的所有其他Web服务器，然后将证书导入IIS

如果选择SSL卸载，则每台Web服务器可能配置有各自的SSL证书

注意：如果您有多个Web服务器，并在Web服务器上选择SSL通过，或者如果您希望在所有服务器上都有通用证书，则必须选择一个Web服务器以执行第1步，然后将证书导入到所有其他Web服务器。
如果选择SSL卸载，则必须在所有Web服务器上执行这些步骤。您还必须生成要在负载均衡器上使用的证书。

步骤1.1.生成证书

如果已创建或获取证书，则可以跳过此部分，否则请选择两个选项之一。

选项1.使用自签名证书

1. 导航到IIS管理。
2. 在左侧的“连接”树中选择服务器名称。
3. 在中心窗格中找到**Server Certificates**，然后双击将其打开。
4. 从右**侧的“操作”(Actions)窗格中**选择“创建自签名证书……”(Create Self-Signed Certificate...)。
5. 在“创**建自签名证书**”窗口中，选择并在“指定证**书的友好名称：**包装盒.此名称是证书在下一主要步骤的选择过程中的显示方式。此名称不需要与证书的公用名称匹配，也不会影响证书对最终用户的显示方式。
6. 确保在**为新**证书选择**证书存储区中选择了个人：**下拉框。
7. 选择**OK**以创建证书。
8. 继续执行下一个主要步骤，将证**书绑定到网站**。

选项2.使用CA签名的证书

CA签名的证书要求您生成证书签名请求(CSR)。 CSR是文本文件，随后将其发送到CA，在CA上签名，然后返回签名证书以及所需的CA证书，CSR将得到履行。您可以选择通过IIS管理或通过Microsoft管理控制台(MMC)执行此操作。 IIS管理方法更简单，无需特殊知识，但仅允许您配置证书的“主题”属性中包含的字段并更改位长度。MMC需要额外的步骤，并且您对有效CSR中所需的所有字段都有全面的了解。强烈建议您仅在具有中等至专家证书创建和管理经验时使用MMC。如果您的部署需要通过多个完全限定名称访问ECE，或者如果您需要更改证书的任何部分（主题和位长度除外），则必须使用MMC方法。

1. 通过IIS管理 使用以下步骤通过IIS管理器生成证书签名请求(CSR)。导航到IIS管理。在左侧的“连接”树中选择服务器名称。在中心窗格中找到**Server Certificates**，然后双击将其打开。从右**侧的“操作”(Actions)窗**格中选择“创建证书请求……”。系统将显示**“请求证**书”向导。在“可**分辨名称属**性”页上，在系统的表单中输入值。必须输入所有字段。选择**Next**继续。在“加密服**务提供程序属性**”页上，保留“加密服务提供程序：”**的默认选择**。更改位**长度：**降至最低值2048**年**。选择**Next**继续。在“文**件名**”(File Name)页面上，选择要保存CSR文件的位置。将文件提供给CA。收到签名证书后，将其复制到Web服务器并继续下一步。在IIS Manager中的同一位置，在“操作”窗**格中选择“完**成证书**请求**”。系统将显示向导。在“指**定证书颁发机构响**应”(Specify Certificate Authority Response)页面上，选择CA提供的证书。在“友好名称”**框中指**定名称。此名称是证书在下一主要步骤的选择过程中的显示方式。确保为新**证书选择证书存储区：**下拉列表设置为“个**人”**。选择**OK** 以完成证书上传。继续执行下一个主要步骤，将证**书绑定到网站**。
2. 通过Microsoft管理控制台(MMC) 使用以下步骤通过MMC生成CSR。此方法允许您自定义

CSR的每个方面。右键单击“开始”按钮，然后选择“运行”。在运行框中键入mmc，然后选择OK。将证书管理单元添加到MMC窗口。 选择文件，然后选择添加/删除管理单元……。系统将显示“添加或删除管理单元”框。在左侧的列表中，找到证书，然后选择添加>。系统将显示Certificates管理单元框。选择选项“计算机帐户”，然后选择“下一步”>。确保本地计算机：（此控制台打开的计算机）在“选择计算机”页面上选择，然后选择完成。选择确定以关闭添加或删除管理单元框。生成CSR 在左窗格中，依次展开Certificates(Local Computer)和Personal，然后选择Certificates文件夹。右键单击“证书”文件夹，然后导航到“所有任务”>“高级操作”>选择“创建自定义请求……”。。系统将显示“证书注册”向导。在简介屏幕上选择“下一步”。在“选择证书注册策略”页上，选择“继续但不注册策略”(列在“自定义请求”下面)，然后选择“下一步”。在“自定义请求”(Custom request)页面上，确保选择的模板是(No template)CNG密钥，并且请求格式适合您的CA。PKCS #10与Microsoft CA配合使用。选择Next以继续下一页。在“证书信息”页上，选择“详细信息”旁边的下拉列表，然后选择属性按钮。系统将显示“证书属性”窗体。为“证书属性”表单提供所有选项已超出本文档的范围。有关详细信息，请参阅Microsoft文档。以下是有关此表单的一些注释和提示。 确保填充主题名称中的所有必需值：部分:选项卡确保为“公用名”提供的值也在“备用名”中：部分设置类型：要DNS，请将URL键入Value:，然后选择“添加”>按钮如果希望使用多个URL访问ECE，请在此字段中提供每个备用名称，并在每个URL后面选择Add >确保将“私钥”选项卡上的密钥大小设置为大于1024的值。如果计划导出证书以在多个Web服务器上使用（通常在HA安装中执行），请确保选择“使私钥可导出”。如果不执行此操作，将导致以后无法导出证书输入的值和所做的选择不会验证。您必须确保提供所有必需信息，否则CA可能无法完成CSR选择所有选择后，OK返回向导。选择Next以继续下一页。在“要将脱机请求保存到何处？”上页面，在您可以访问的位置中选择文件名。对于大多数CA，应选择Base 64作为格式。将文件提供给您的CA。当他们签名并将证书返回给您后，将证书复制到Web服务器并继续执行最后的步骤。在MMC的证书管理管理单元中，导航到证书（本地计算机）> 个人，右键单击证书，然后选择所有任务>导入……。系统将显示证书导入向导。在介绍性屏幕上选择“下一步”。在“要导入的文件”屏幕上，选择已由CA签名的证书，然后选择“下一步”。确保选择“Place all certificates in the following store”。确保在证书存储中选择“Personal”：，然后选择“下一步”。查看最终屏幕，然后选择“完成”以完成导入。现在可以关闭MMC控制台。如果系统提示您保存控制台设置，则可以选择否。这不会影响证书导入。继续执行下一个主要步骤，将证书绑定到网站。

步骤1.2.将证书绑定到网站

警告：您必须确保主机名字段留空，并且“编辑站点绑定”框中未选择“需要服务器名称指示”选项。如果配置了其中任一项，SPOG在尝试与ECE通信时会失败

1. 如果您以前没有打开Internet信息服务(IIS)管理器。
2. 在左侧的“连接”窗格中，导航至“站点”，然后选择“默认网站”。 如果选择使用“默认网站”以外的网站名称，请确保选择正确的网站名称。
3. 从右侧的“操作”窗格中选择“绑定……”。系统将显示“站点绑定”框。 如果没有Type、https和Port的行，请完成以下操作。否则，请继续执行下一个主要步骤。 选择“添加……”按钮，将显示“添加站点绑定”框。在类型中选择https:下拉菜单。确保IP地址：下拉菜单显示“All Unassigned”和“Port:字段为443。确保保留主机名：字段为空，且未选择“需要服务器名称指示”选项。在SSL证书中：下拉菜单中，选择与之前创建的证书名称对应的证书名称。 如果您不确定要选择哪个证书，请使用Select...按钮查看和搜索服务器上存在的证书使用“查看……”按钮查看所选证书并验证详细信息是否正确选择OK以保存选择。选择在“类型”列中显示https的行，然后选择“编辑……”按钮。系统将显示“编辑站点绑定”框。 确保IP地址：下拉菜单显示“All Unassigned”和“Port:字段为443。确保主机名：字段留空，并且未选择“需要服务器名称指示

”选项。在SSL证**书中：**下拉菜单中，选择与之前创建的证书名称对应的证书名称。 如果您不确定要选择哪个证书，请使**用Select...**按钮查看和搜索服务器上存在的证书使用“**查看……**”按钮查看所选证书并验证详细信息是否正确选择**OK**以保存选择。选择**关闭**以返回IIS管理器。
4. 现在可以关闭IIS管理器。

步骤2.配置分区管理员SSO

分区管理员SSO配置允许ECE为在SPOG中打开ECE小工具的任何管理员自动创建分区级别用户帐户。

注意：即使您不计划启用代理或管理引擎SSO，也必须配置分区管理员SSO。

步骤2.1.获取Active Directory(AD)证书并创建密钥库。

要解决Microsoft最近宣布的安全更改，需要执行此步骤。

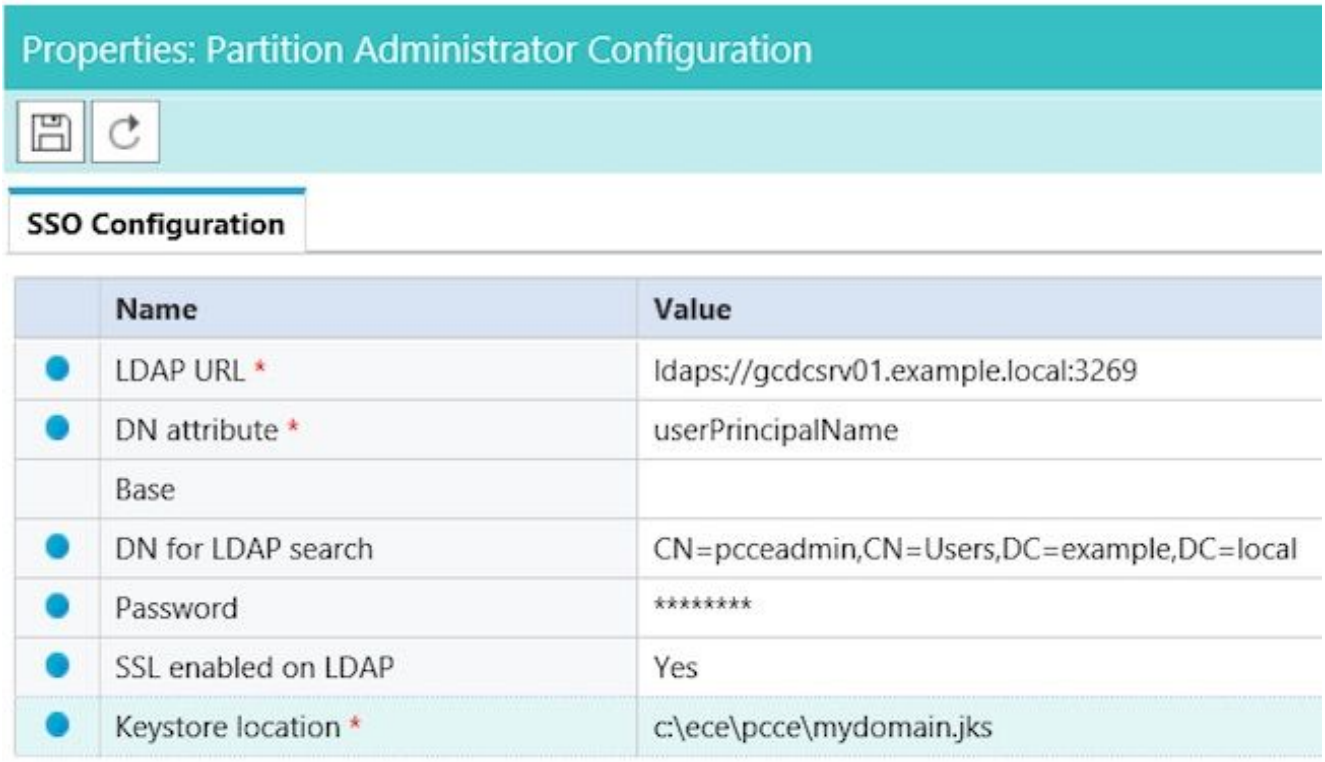
有关详情，请参阅https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows。

1. 从AD服务器（在分区管理员配置表单中提供）获取Base 64格式的SSL证书。
2. 将证书文件复制到其中一个应用程序服务器。
3. 打开到复制证书的应用程序服务器的RDP会话。
4. 按如下所述创建新的Java密钥库。 在应用服务器上打开命令提示符。更改为ECE Java开发套件(JDK)bin目录。运行此命令。根据需要替换值。
   keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c:\ece\pcce\mydomain.jks -storepass MyP@ssword
5. 将密钥库复制到环境中所有其他应用程序服务器上的相同路径。

步骤2.2.使用AD轻量级目录访问协议(LDAP)访问信息配置ECE。

1. 从装有Internet Explorer 11的工**作站或计**算机，导航至业务分区URL。 **提示：**业务分区也称为分区1。对于大多数安装，可以通过类似于https://ece.example.com/default的URL访问业务分区。
2. 以**pa**身份登录并为系统提供密码。
3. 成功登录后，在初始控制台上选择**Administration**链接。
4. 按如下方**式导航**到SSO Configuration文件**夹，Administration > Partition:default > Security > SSO and Provisioning**。
5. 在右侧顶部窗格中，选择分区管**理配置**条目。
6. 在右侧底部窗格中，输入轻量目录访问协议(LDAP)和AD的值。 **LDAP URL** — 最佳做法是使用全局目录(GC)域控制器的名称。
   如果不使用GC，则ApplicationServer日志中可能会出现错误，如下所示。
   LDAP身份验证中出现异常<@>
   javax.naming.PartialResultException:未处理的继续参考；剩余名称'DC=example，DC=com'
   非安全全局编录端口为3268安全全局编录端口为3269**DN属性** — 此属性必须为userPrincipalName。**Base** — 如果使用GC，则不需要此选项，否则，必须提供基本正确的LDAP格式。**DN for LDAP search** — 除非域允许匿名绑定，否则必须提供用户的可分辨名称，以便能够绑定到LDAP并搜索目录树。

提示 — 为用户找到正确值的最简单方法是使用Active Directory用户和计算机工具。 在“视**图**”**菜**单中启**用高**级功能。导航至用户对象，然后右键单击并选择“**属性**”。选择“**属性**”选项卡。选择“筛**选器**”按钮，然后**选择“仅显示带值的属性**”。在列表**中查**找distinquisedName，然后双击以查看值。突出显示显示的值，然后将其复制并粘贴到文本编辑器。将文本文件中的值复制并粘贴到LDAP**搜索的DN**字段。
值应类似于， CN=pcceadmin， CN=Users， DC=example， DC=local**密码** — 除非域允许匿名绑定，否则必须为用户指定的密码提供密码。**在LDAP上启用SSL** — 对于大多数客户，应将此字段视为必填项。**密钥库位置** — 这应该是从AD导入SSL证书的密钥库的位置。在示例中，这是c:\ece\pcce\mydomain.jks，如图所示：



7. 选择软盘图标以保存更改。

步骤3.验证配置文件

对于所有12.0安装，必须完成本节。对于12.0以外的任何版本，您可能可以跳过此部分。
对于可能需要此步骤的所有版本，还有两个其他方案。第一种是在高可用性设置中安装ECE时。第二种情况更常见，即Web服务器的主机名与您用于访问ECE的名称不匹配。例如，如果在主机名为UCSVRECEWEB.example.com的服务器上安装ECE Web服务器，但用户访问URL为chat.example.com的ECE网页，则必须完成此部分。如果服务器的主机名和您使用访问ECE的URL相同，并且您安装了12.5版或更高版本，则可以跳过此步骤并完成该部分。

将{ECE_HOME}替换为您安装ECE的物理位置。例如，如果您已在C:\Cisco安装**ECE**，则在每个位置将{ECE_HOME}**替换为**C:\Cisco。

提示：使用文本编辑器（如Notepad++），而不是记事本或写字板，因为这些编辑器无法正确解释行尾。

1. 打开与部署中所有ECE Web服务器的远程桌面会话。
2. 导航到此路径**{ECE_HOME}\eService\templates\finesse\gadget\spog**。
3. 找到**spog_config.jsfile**并在安全位置创建备份副本。

4. 在文本编辑器中打开当前spog_config.jsfile。
5. 找到这两行并更新它们以匹配部署。
   web_server_protocol必须是https，如果需要，请更新。
   更新web_server_name以匹配您分配用于访问ECE的完全限定名称。示例：ece.example.com var web_server_protocol = "https";var web_server_name = "ece.example.com";
6. 保存更改。
7. 在部署中的所有其他Web服务器上重复此步骤。

步骤4.将ECE添加到PCCE资产

自12.0起，PCCE有3个不同的部署选项，2000个代理（2K代理）、4000个代理（4K代理）和12000个代理（12K代理）。 这三个部署选项可分为两组，即2K代理和4K/12K代理。由于在SPOG中看法存在几个根本差异，因此它们以这种方式分开。下面对这两种方法进行了非常高级别的比较。本文档未提供将组件添加到库存的具体步骤。有关此流程的具体详细信息，请参阅本文档末尾的链接。本节介绍在将ECE添加到PCCE时必须验证的具体详细信息。本文档还假设PCCE安装已完成，并且您能够访问和配置解决方案的其他方面。

- 2000代理部署 PCCE组件的初始配置完全通过CCE管理完成，并实现自动化新组件通过弹出框添加到“资产”页面，在该弹出框中输入详细信息，如IP或主机名以及任何必要的凭证或组件特定配置
- 4K和12K代理部署 许多初始配置都反映了用于UCCE的步骤组件通过从CCE管理下载的逗号分隔值(CSV)文件添加，根据特定安装进行填充，然后上传初始部署需要将某些特定组件包含在第一个CSV文件中最初设置系统时未添加的组件通过包含所需信息的CSV文件添加

步骤4.1.将ECE Web服务器证书上传到Java密钥库

1. 如果使用自签名证书 打开与主A端管理数据服务器(ADS)的远程桌面连接。以管理员身份打开Internet Explorer 11并导航至ECE业务分区。选择URL栏右侧的挂锁图标，然后选择“查看证书”。在“证书”框中，选择“详细信息”选项卡。选择选项卡底部附近的“复制到文件……”。在证书导出向导中，选择下一步，直到到“导出文件格式”页。确保选择Base-64编码的X.509(.CER)格式。将证书保存到ADS服务器上的c:\Temp\certificates等位置，以完成导出。将证书复制到所有其他ADS服务器。打开管理命令提示符。更改到Java主目录，然后更改到bin目录。Java主目录的访问方式如下。cd %JAVA_HOME%\bin备份当前cacerts文件。将cacerts文件从%JAVA_HOME%\lib\security复制到其他位置。运行此命令以导入之前保存的证书。如果密钥库密码不是“changeit”，请更新命令以匹配安装。
   keytool -keystore ../lib/security/cacerts -storepass changeit -import -alias <ECE服务器的FQDN> -file <您保存证书的位置>重新启动ADS服务器。在其他ADS服务器上重复步骤8-12。
2. 如果使用CA签名的证书 以DER/PEM格式获取根证书和中间证书，并将其复制到所有ADS服务器上的C:\Temp\certificates等位置。 注意：请联系CA管理员获取这些证书。 打开与主A侧ADS的远程桌面连接。打开管理命令提示符。更改到Java主目录，然后更改到bin目录。Java主目录的访问方式如下。cd %JAVA_HOME%\bin备份当前cacerts文件。将cacerts文件从%JAVA_HOME%\lib\security复制到其他位置。运行此命令以导入之前保存的证书。如果密钥库密码不是“changeit”，请更新命令以匹配安装。
   keytool -keystore ../lib/security/cacerts -storepass changeit -trustcacerts -import -alias <CA根名称> -file <您保存根证书的位置>重复步骤6.并导入中间证书（如果存在）。重新启动ADS服务器。在所有其他ADS服务器上重复步骤2-12。

步骤4.2.将ECE数据服务器添加到资产

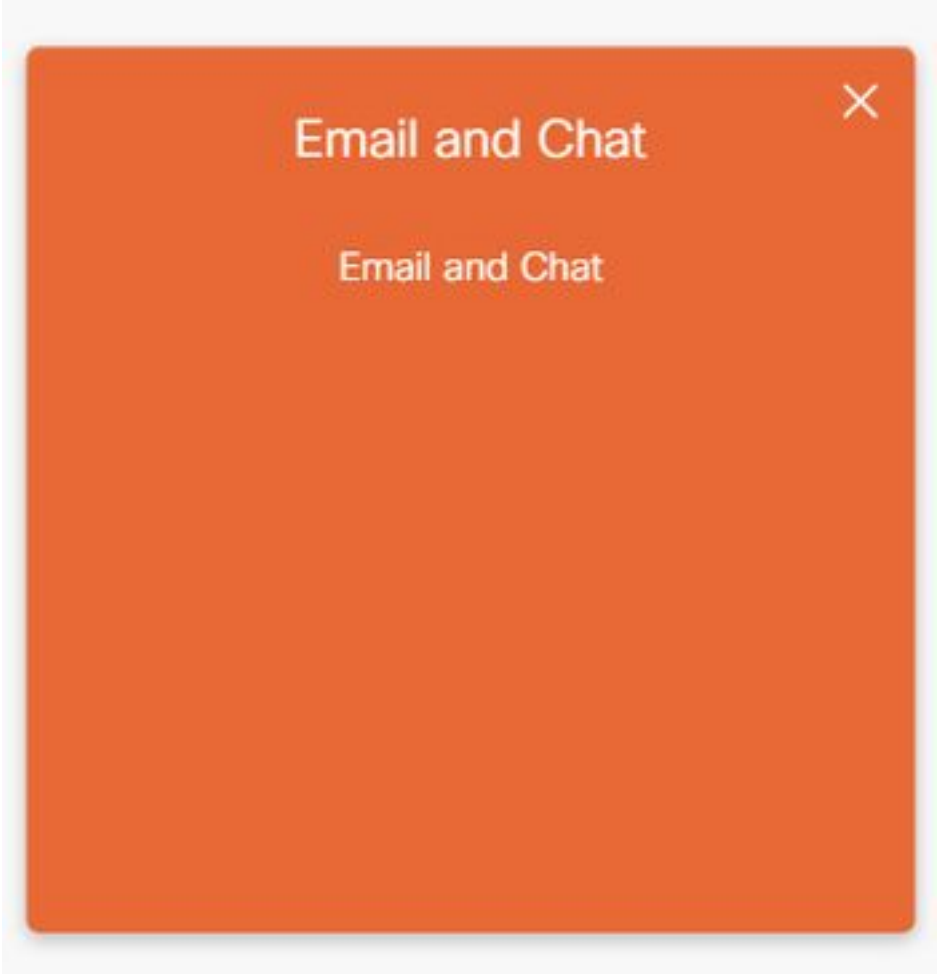
- 虽然数据服务器必须存在于系统清单中，但PCCE ADS和数据服务器之间没有直接通信
- 在1500代理部署中部署ECE时，数据服务器即是服务服务器
- 在HA配置中安装ECE时，应添加两个服务服务器

步骤4.3.将ECE Web服务器添加到资产

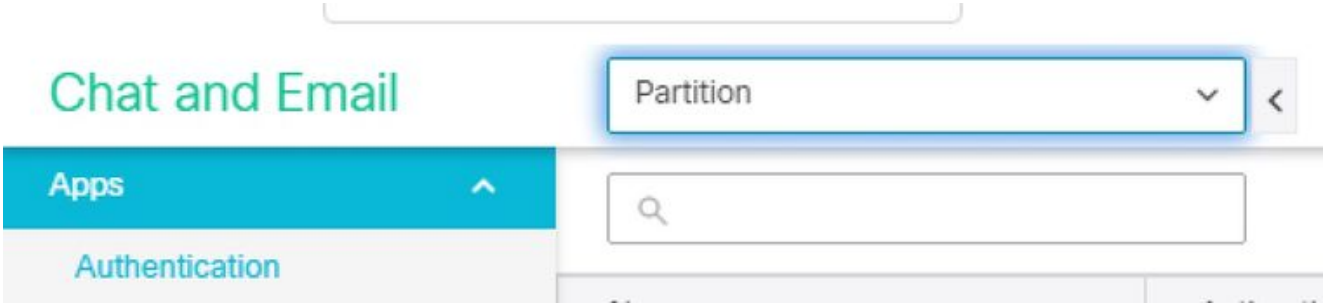
- 确保添加具有完全限定名称的Web服务器 此名称必须与ECE证书中的公用名称匹配，或者必须作为主题备用名称(SAN)之一列出不能仅使用主机名或IP地址
- ECE的用户名和密码应为个人登录凭证
- 确保应用实例正确 应用程序实例名称区分大小写对于2000代理PCCE部署，应用实例为MultiChannel对于4000/12000代理PCCE部署，应用实例包含作为名称一部分的站点和外围设备集
- 当ECE与多个Web服务器一起安装时（例如在1500代理部署或400代理HA部署中），您可以使用指向负载均衡器的URL或指向每个Web服务器的URL作为Web服务器的完全限定名称。
- 如果您有多个ECE部署，或者如果您选择在部署中添加多个单个Web服务器，则在SPOG中打开ECE小工具时，您会选择正确的Web服务器。

步骤5.将ECE与PCCE集成

1. 以管理员身份登录CCE管理。
2. 选择“**电子邮件和聊**天”卡，然**后选择“电**子邮件和聊天”链接，如图所示。



3. 在“设备名称”(Device Name)下拉列表中查看当前选定的服务器。如果在HA安装中添加了两个Web服务器，则可以选择任一Web服务器。如果以后将第二个ECE部署添加到系统，请确保在继续之前选择适当的服务器。
4. 在“聊天和电子邮件”**旁的下拉**列表中，**分区**或**全局**，如图所示。

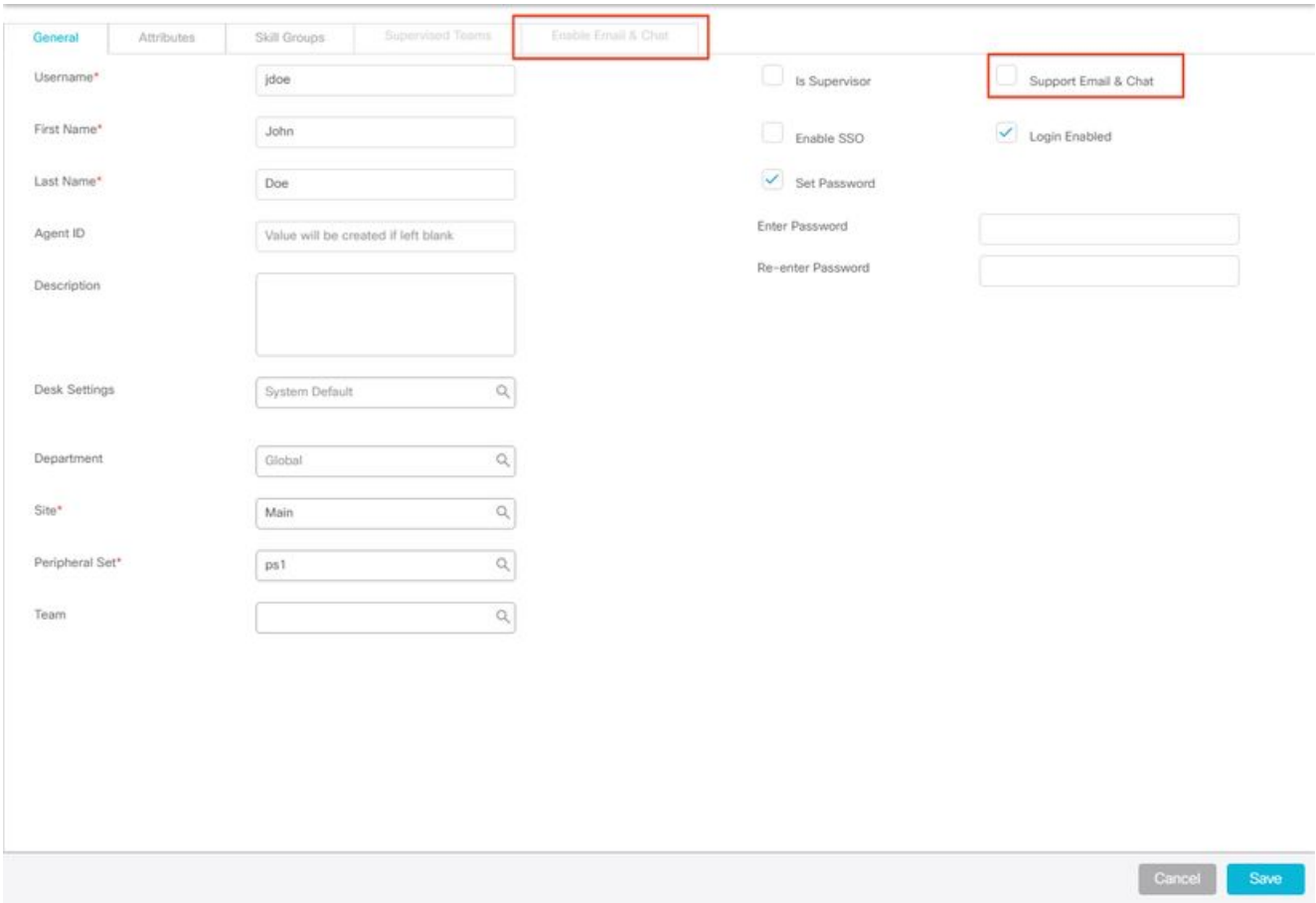


5. 在顶部菜单中，选择**Integration**，然后选择**Unified CCE**旁边的箭头，然后选择图**中所示的**第二个Unified CCE。

6. 在AWDB Details(AWDB详细**信息)选**项卡中为安装填充值，然后选择**Save(保**存)按钮。
7. 选择**Configuration**选项卡，然后按如下方式完成此操作。 选择Application Instance旁的下拉**菜单，**然后选择为ECE创建的Application Instance。 **注意：**这不能是以UQ开头的应用实例。选择带有白色加号按钮的绿色圆圈 选择Agent PG。 选择Agent PG(或Agent PG（如果有多个）。添加所**有代**理程序后，选择保存。 **警告：**选择“保存**”后**，系统将永久连接到PCCE，且无法撤消。如果本节中出错，则必须完全卸载ECE并删除所有数据库，然后安装ECE，就像新安装一样。

步骤6.验证ECE集成

1. 在CCE管理中，检查顶部状态栏中是否没有显示警报。 如果有警报，请选择**Alerts**一词并查看Inventory页面，以确保所有警报都不针对ECE服务器。
2. 在左**侧的导航**栏中选**择用户**，然后选择代理。
3. 从列表中选择一个代理并验证此操作。 现在，您应会在“常规”选项卡上看**到“支持电子邮件**和聊天**”的新**复选框。现在，您应该看到一个标有“启**用电子邮件和聊**天”的新选项卡，如图所示。



4. 为ECE启用测试代理。 选中“**支持电子邮件和聊**天”复选框，并注意，**现在可以**选择“启用电子邮件和聊天”选项卡。选择“启**用电子邮件和聊**天”选项卡，并在“屏幕名**称”字**段中提供值。选择**保存**以更新用户。您应收到成功消息。
5. 验证ECE是否已更新。 选择“**概述**”导航按钮，然后选**择“电子邮件**和聊天”卡和链接。在“聊天和电子邮件”**旁的下拉**菜单中，选择与座席的部门对应的名称。 **注意：**ECE的服务部门保留属于PCCE全球部门的所有对象。因此，部门名称Service是保留值。在顶部菜单中，选择“**用户管**理”，然**后在**“聊天和电子邮**件”下选择“用户”**。验证是否在列表中看到新座席。

故障排除

建议您下载多种工具，并将其保留在ECE服务器上。随着时间的推移，这些功能使解决方案的故障排除和维护更加容易。

- 文本编辑器，如Notepad++
- 存档工具，如7-Zip
- Windows程序的众多尾部之一
  以下是几个示例： 裸机 — https://www.baremetalsoft.com/baretail/Win32的尾部 — http://tailforwin32.sourceforge.net/

为了排除集成问题，您必须首先了解一些关键日志文件和每个日志文件的位置。

1. **ECE上的文件名和位置**

   ECE系统上有许多日志，这些日志在您尝试排除集成问题时最有帮助。

   服务器密钥：C =配置的服务器A =应用服务器S =服务服务器M =消息服务器大多数日志文件还有另外两个与它们关联的日志。eg_log_{服务器名称}_{PROCESS}.log — 主进程日志
   eg_log_dal_connpool_{SERVERNAME}_{PROCESS}.log — 连接池使用情况
   eg_log_query_timeout_{SERVERNAME}_{PROCESS}.log — 当查询因超时而失败时更新
2. **PCCE上的文件名和位置**

   集成问题的PCCE日志都位于A侧ADS中。以下是排除集成问题时最重要的日志。每个都位于**C:\icm\tomcat\logs**。

   在这些日志中，前三个日志是请求和查看最频繁的日志。使用以下步骤设置跟踪级别并收集所需日志。
3. **跟踪级别配置**本节仅适用于ECE。PCCE所需的日志由思科设置跟踪级别，无法更改。 从装有Internet Explorer 11的工**作站或计**算机，导航至系统分区URL。 **提示：**系统分区也称为分区0。对于大多数安装，系统分区可以通过类似于https://ece.example.com/system的URL访问以**sa**身份登录并为系统提供密码。成功登录后，在初始控制台上选择**System**链接。在“系统”页中，展**开“**系统”**>“共**享资源”>“记**录器”>**“进程”。在右上角的窗格中，查找要更改跟踪级别的流程并选择它。
   注意：在HA系统和具有多个应用服务器的系统中，会列出多个进程。为确保捕获数据，请为包含该进程的所有服务器设置跟踪级别。在右下窗格中，选择“Maximum trace level（最大跟踪级别）”的下**拉列表，**然后选择适当的值。
   ECE中定义了8个跟踪级别。此列表中的4是最常使用的4。 2 — 错误 — 进程的默认跟踪级别4 — 信息 — 通常用于问题解决的跟踪级别6 - Dbquery — 通常有助于在设置早期诊断问题或更复杂的问题7 — 调试 — 非常详细的输出，仅在最复杂的问题中需要**注意：**不应将任何进程保持在6 - Dbquery的任意长度，并且通常仅在TAC指导下。大多数进程应保持跟踪级别，2 — 错误。如果选择级别7或8，则还必须选择最长持续时间。当达到最长持续时间时，跟踪级别将返回到最后一个级别集。

在系统设置后，将这四个进程更改为跟踪级别4。EAAS流程EAMS流程dx-processrx-process选择保存图标以设置新的跟踪级别。

4. **日志文件集合**

打开到服务器的远程桌面会话，该服务器需要进程记录。导航到日志文件位置。 ECE服务器日志的编写如下。默认情况下，日志是写入文件，最大大小为5MB当一个日志文件达到配置的最大值时，将以{LOGNAME}.log.{#}格式重命名。ECE保留之前的49个日志文件加上当前文件当前日志始终以.log结束，在日志既未存档也未压缩大多数日志具有通用结构日志文件使用<@>分隔各节日志始终以GMT+0000时间写入ECE日志根据特定安装位于不同位置。400代理部署 单面 服务器：配置的服务器地点：**{ECE_HOME}\eService_RT\logs**高可用性 服务器：两台同置服务器地点：**{ECE_HOME}\eService\logs**为分布式文件系统(DFS)共享创建的目录仅包含安装和升级日志。只有拥有分布式系统管理器(DSM)角色的服务器才会为属于服务角色的组件写入日志 DSM角色所有者可在Windows任务管理器的“进程”选项卡中找到。此服务器上有10-15个Java进程不在辅助服务器上。DSM下的组件包括EAAS、EAMS、检索器、调度器、工作流等。1500代理部署 位于承载角色的服务器上的日志地点：**{ECE_HOME}\eService\logs**除服务服务器外，所有服务器都为与组件关联的所有进程运行和写入日志在高可用性部署中，服务服务器在主用/备用配置中运行只有拥有分布式系统管理器(DSM)角色的服务器才能写入日志DSM角色所有者可以通过在Windows任务管理器中看到的进程数来识别。在主服务器上运行10-15个Java进程，在辅助服务器上只运行4个Java进程PCCE服务器 来自PCCE的所需日志位于**C:\icm\tomcat\logs**Tomcat日志不会回滚或存档日志在本地服务器时间写入收集发现问题后创建或修改的所有日志。
对日志和所发现的问题的完整说明不在本文档的范围之内。以下是一些常见问题、要审核的内容以及一些可能的解决方案。 证书相关问题 证书未导入 行为：当您尝试在SPOG中打开ECE小工具时，您会看到错误，“加载页面时出错。请与管理员联系。"检查：在PCCE上登录Catalina，查找类似以下错误
javax.net.ssl.SSLHandshakeException:sun.security.validator.ValidatorException:PKIX路径生成失败：sun.security.provider.certpath.SunCertPathBuilderException:找不到到请求目标的有效证书路径解决方案：确保已将ECE Web服务器证书或适当的CA证书导入ADS上的密钥库中证书不匹配 行为：当您尝试在SPOG中打开ECE小工具时，您会看到一个错误，表明证书的公用名称或使用者备用名称与配置的名称不匹配。检查：验证SSL证书解决方案：确保Subject中的Common Name字段或Subject Alternate Name中的DNS字段包含您在SPOG中输入的完全限定名称作为Web服务器名称。系统问题 服务未启动 行为：当您尝试在SPOG中打开ECE小工具时，您会看到错误，“https://{url}处的网页可能暂时关闭，或者它可能已永久移动到新地址。”检查：验证Windows服务 — 思科服务已在所有ECE服务器上启动（Web服务器除外）。查看应用服务器上的根日志以查找错误解决方案：在所有ECE服务上启动思科服务。配置问题 LDAP配置 行为：当您尝试在SPOG中打开ECE小工具时，您会看到错误，“加载页面时出错。请与管理员联系。"检查：将应用服务器的跟踪级别增加到级别7 — 调试，然后再次尝试登录并查看应用服务器日志。搜索LDAP一词。解决方案：验证分区管理员SSO的LDAP配置，确保其正确。

相关信息

这些是在开始任何ECE安装或集成之前必须仔细检查的重要文档。这不是ECE文档的综合列表。

> **警告：**大多数ECE文档有两个版本。请确保下载并使用适用于PCCE的版本。文档标题在版**本号后面有**Packaged Contact Center **Enterprise或(**用于PCCE**)或(用于UCCE和**PCCE)。

确保在安装、升级或集成之前，检查思科企业聊天和电子邮件文档的开始页面，查找任何更新。

https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html

- 12.0 企业聊天和电子邮件安装和配置指南企业聊天和电子邮件升级指南企业聊天和电子邮件管理员指南
- 12.5 企业聊天和电子邮件安装和配置指南企业聊天和电子邮件升级指南企业聊天和电子邮件管理员指南