バージョン12.0以降でのECEとPCCEの統合

内容

はじめに

このドキュメントでは、エンタープライズチャットおよび電子メール(ECE)をPackaged Contact Center Enterprise(PCCE)バージョン12.0以降に統合する手順について説明します

前提条件

要件

次の項目に関する知識があることが推奨されます。

- エンタープライズチャットおよび電子メール(ECE)12.x
- Packaged Contact Center Enterprise(PCCE)12.x

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

PCCEバージョン12.0では、Single Pane of Glass(SPOG)と呼ばれる新しい管理インターフェイスが導入されました。コンタクトセンターおよび関連アプリケーションのほぼすべての管理は、このインターフェイスで実行されます。ECEとPCCEの両方を適切に統合するには、この統合に固有のいくつかの手順を実行する必要があります。このドキュメントでは、このプロセスについて説明します。

用語

このドキュメントでは、次の用語を使用しています。

- エンタープライズチャットおよび電子メール(ECE):ECEは、電子メールおよびチャットの要求を、音声コールと同じ方法でコンタクトセンターエージェントにルーティングできる製品です。
- Single Pane of Glass(SPOG):SPOGは、PCCE管理がバージョン12.0以降で実行される方法です。SPOGは、12.0より前のバージョンで使用されていたCCE管理ツールの完全なリライトです。
- 認証局(CA)：公開キーインフラストラクチャ(PKI)モデルに従ってデジタル証明書を発行するエンティティ。

  発生する可能性のあるCAには2つのタイプがあります。

  - パブリックCA：パブリックCAは、ほとんどのブラウザとオペレーティングシステムにルート証明書と中間証明書が含まれているCAです。一般的なパブリックCAには、Identrust、DigiCert、GoDaddy、GlobalSignなどがあります。
  - プライベートCA – プライベートCAは、企業内に存在するCAです。一部のプライベートCAはパブリックCAによって署名されますが、ほとんどの場合、これらのCAはスタンドアロンCAであり、発行される証明書はその組織内のコンピューターによってのみ信頼されます。

2つのCAタイプのどちらにも、2つのタイプのCAサーバがあります。

  - ルートCAサーバ：ルートCAサーバはそれ自体の証明書に署名します。標準の多層PKI展開では、ルートCAはオフラインでアクセスできません。このモデルのルートCAは、中間CAと呼ばれる別のCAサーバに証明書を発行するだけです。一部の企業では、単層CAのみを使用することを選択しています。このモデルでは、ルートCAは、別のCAサーバ以外のエンティティが使用する証明書を発行します。
  - 中間CAサーバ：中間CAサーバまたは発行側CAサーバは、別のCAサーバ以外のエンティティが使用する証明書を発行します。
- Microsoft管理コンソール(MMC):Microsoft Windowsに付属するアプリケーションで、さまざまなスナップインをロードできます。スナップインを使用して、サーバー管理用にカスタマイズされたコンソールを構築できます。Windowsには多くの異なるスナップインが含まれています。例の短いリストには、証明書、デバイスマネージャ、ディスク管理、イベントビューア、サービスなどがあります。
- ネットワークロードバランサ(NLB)：複数の物理リソースを共通の物理名でエンドユーザに提供するデバイスまたはアプリケーションです。NLBは、Webアプリケーションおよびサービスで非常に一般的です。NLBはさまざまな方法で実装できます。ECEとともに使用する場合、NLBは、ユーザセッションがcookie-insertまたは同等の方法を使用して同じ物理バックエンドWebサーバに戻るように設定する必要があります。これは、cookie-insertを使用するスティッキセッションと呼ばれます。スティッキセッションとは、すべてのインタラクションでユーザのセッションを同じ物理バックエンドサーバに返すロードバランサの機能を指します。
  - Secure Sockets Layer(SSL)パススルー：SSLパススルーは、エンドユーザデバイスと、ユーザのセッションが割り当てられた物理Webサーバとの間にSSLセッションが存在する方式です。HTTPセッションは常に物理的に暗号化されるため、SSLパススルーはcookie-insertを許可しません。ほとんどのNLBは、セッション設定のserverhelloおよびclienthello部分を監視し、一意の値をテーブルに保存するstickテーブルを使用して、SSLパススルーによるスティッキセッションをサポートしています。これらの値に一致する次の要求がNLBに提示されると、stickテーブルを使用して同じバックエンドサーバにセッションを返すことができます。
  - SSLオフロード：NLBがSSLオフロード用に設定されている場合、特定のエンドユーザセッションに対して2つのSSLセッションまたはトンネルが存在します。1つ目は、エンドユーザデバイスと、Webサイト用にNLBで設定された仮想IP(VIP)の間にあります。2つ目は、NLBのバックエンドIPと、ユーザのセッションが割り当てられている物理Webサーバの間のアドレスです。SSLオフロードは、追加のHTTP cookieを挿入してセッション検査を実行できるNLBでHTTPストリームが完全に復号化される一方で、cookie-insertをサポートします。SSLオフロードは、WebアプリケーションがSSLを必要とせず、代わりにセキュリティのために実行される場合によく使用されます。
    ECEの現在のバージョンでは、非SSLセッションでのアプリケーションへのアクセスはサポートされていません。

前提条件の手順

2つのシステムの統合を開始する前に、いくつかの前提条件を完了する必要があります。

- 最小PCCEパッチレベル

- バージョン12.0(1) - ES37
- バージョン12.5(1)：基本機能の現在の最小要件なし

- 最小ECEパッチレベル

  ECEでは、最新のEngineering Special(ES)を実行することをお勧めします。

  - バージョン12.0(1) - ES3 + ES3_ET1a
  - バージョン12.5(1)：基本機能の現在の最小要件なし

- 設定項目

  ECE_Email、ECE_Chat、およびECE_Outbound Media Routing Domains(MRD)を正しいアプリケーションインスタンスに関連付けていることを確認します。

  - PCCE 2000エージェント導入モデルでは、アプリケーションインスタンスはマルチチャネルであり、PCCEの導入時に事前設定されます。
  - PCCE 4000/12000 Agentの導入モデルでは、アプリケーションインスタンスは任意の名前にすることができ、統合を実行するユーザによって作成される必要があります。ベストプラクティスは、{site}_{peripheral_set}_{application_instance}という形式を使用することです。
    サイト名をMain、ペリフェラルをPS1、アプリケーションインスタンスをMultichannelに設定してPCCEをインストールした場合、アプリケーションインスタンス名はMain_PS1_Multichannelになります。

注：アプリケーションインスタンス名は大文字と小文字が区別されます。ECE Webサーバをインベントリに追加するときに、名前が正しく入力されていることを確認します。

統合手順

このドキュメントのすべての手順の詳細は、ECEとPCCEの両方のドキュメントで説明されていますが、リストに表示されたり、すべて同じドキュメントに表示されたりすることはありません。詳細については、このドキュメントの最後にあるリンクを参照してください。

ステップ 1：SSL証明書の設定

ECE Webサーバで使用する証明書を生成する必要があります。自己署名証明書を使用することもできますが、多くの場合、CA署名付き証明書を使用する方が簡単です。自己署名証明書は、CA署名付き証明書と比べて安全性が高く、最初に証明書を作成する手順も少なくなりますが、証明書を置き換える必要がある場合は、すべてのPCCE Administration Data ServerのJavaキーストアに新しい証明書をアップロードすることを忘れないでください。CA署名付き証明書を使用する場合は、ルート証明書と、中間証明書（存在する場合）をキーストアにアップロードするだけです。

導入環境に複数のWebサーバがある場合は、これらのガイドラインを確認する必要があります。ネットワークロードバランサの設定に必要な特定の手順については、このドキュメントでは扱い

ません。必要に応じて、ロードバランサのベンダーに問い合わせてください。

- 必須ではありませんが、ロードバランサによって実装が大幅に簡素化されます
- 各Webサーバ上のECEアプリケーションへのアクセスには、使用するロードバランサ方式に関係なく、SSLを使用する必要があります
- ロードバランサは、SSLパススルーまたはSSLオフロードとして設定できます
- SSLパススルーが選択されている場合：
  - 1つのサーバからすべての証明書操作を実行する必要があります
  - 証明書が正しく設定されたら、証明書をエクスポートし、秘密キーがPersonal Information Exchange(PFX)ファイルに含まれていることを確認する必要があります
  - PFXファイルを展開内の他のすべてのWebサーバにコピーしてから、証明書をIISにインポートする必要があります
- SSLオフロードを選択すると、各Webサーバに個別のSSL証明書を設定できます

注：複数のWebサーバがあり、WebサーバでSSLパススルーを選択するか、すべてのサーバで共通の証明書を使用する場合は、手順1を実行するWebサーバを1つ選択し、証明書を他のすべてのWebサーバにインポートする必要があります。
SSLオフロードを選択する場合は、すべてのWebサーバで次の手順を実行する必要があります。ロードバランサで使用する証明書も生成する必要があります。

ステップ 1.1：証明書の生成

すでに証明書を作成または取得している場合は、このセクションをスキップできます。それ以外の場合は、2つのオプションのいずれかを選択します。

オプション 1自己署名証明書の使用

1. IIS Administrationに移動します。
2. 左側の[接続]ツリーでサーバ名を選択します。
3. 中央のペインでServer Certificatesを探し、ダブルクリックして開きます。
4. 右側のActionsペインで、Create Self-Signed Certificate...を選択します。
5. Create Self-Signed Certificateウィンドウで、を選択し、Specify a friendly name for the certificate:ボックスに名前を入力します。この名前は、次の主要な手順の選択プロセスで証明書がどのように表示されるかを示します。この名前は、証明書の共通名と一致している必要はなく、エンドユーザに対する証明書の表示に影響を与えません。
6. Select a certificate store for the new certificate:ドロップダウンボックスでPersonalが選択されていることを確認します。
7. OKを選択して証明書を作成します。
8. 次の主な手順「証明書のWebサイトへのバインド」に進みます。

オプション 2CA署名付き証明書の使用

CA署名付き証明書では、証明書署名要求(CSR)を生成する必要があります。CSRはテキストファイルであり、CAに送信されて署名が行われ、署名付き証明書と必要なCA証明書が返され、

CSRが履行されます。この操作は、IIS管理またはMicrosoft管理コンソール(MMC)を使用して実行できます。IISの管理方法は、特別な知識を必要としないはるかに簡単ですが、証明書のSubject属性に含まれるフィールドを設定してビット長を変更することしかできません。MMCを使用するには追加の手順が必要で、有効なCSRに必要なすべてのフィールドに関する十分な知識があること。証明書の作成と管理に関する中程度から専門的な経験がある場合にのみ、MMCを使用することを強くお勧めします。展開でECEに複数の完全修飾名でアクセスする必要がある場合、または証明書のサブジェクトとビット長以外の部分を変更する必要がある場合は、MMCメソッドを使用する必要があります。

1. IIS管理を使用する

   IISマネージャを使用して証明書署名要求(CSR)を生成するには、次の手順を使用します。

   1. IIS Administrationに移動します。
   2. 左側の[接続]ツリーでサーバ名を選択します。
   3. 中央のペインでServer Certificatesを探し、ダブルクリックして開きます。
   4. 右側のActionsペインで、Create Certificate Request...を選択します。Request Certificateウィザードが表示されます。
   5. 識別名のプロパティページで、システムのフォームに値を入力します。すべてのフィールドを入力する必要があります。Nextを選択して続行します。
   6. Cryptographic Service Provider Propertiesページで、Cryptographic service provider:のデフォルトの選択をそのままにします。Bit length:ドロップダウンを2048以上に変更します。Nextを選択して続行します。
   7. File Nameページで、CSRファイルを保存する場所を選択します。
   8. ファイルをCAに提供します。署名付き証明書を受け取ったら、それをWebサーバにコピーし、次の手順に進みます。
   9. IISマネージャの同じ場所で、ActionsペインのComplete Certificate Requestを選択します。ウィザードが表示されます。
   10. Specify Certificate Authority Responseページで、CAから提供された証明書を選択します。Friendly nameボックスに名前を入力します。この名前は、次の主要な手順の選択プロセスで証明書がどのように表示されるかを示します。Select a certificate store for the new certificate:ドロップダウンがPersonalに設定されていることを確認します。
   11. OKを選択して、証明書のアップロードを完了します。
   12. 次の主な手順「証明書のWebサイトへのバインド」に進みます。

2. Microsoft管理コンソール(MMC)経由

   MMCを使用してCSRを生成するには、次の手順を使用します。この方法を使用すると、CSRのすべての側面をカスタマイズできます。

   1. [スタート]ボタンを右クリックし、 [ファイル名を指定して実行]を選択します。
   2. Runボックスにmmcと入力し、OKを選択します。
   3. 証明書スナップインをMMCウィンドウに追加します。
      1. File、Add/Remove Snap-in...の順に選択します。Add or Remove Snap-insボックスが表示されます。
      2. 左側のリストでCertificatesを見つけて、Add >を選択します。Certificatesスナップインボックスが表示されます。

3. オプションComputer accountを選択し、Next >を選択します。
4. Select Computerページで Local computer: (The computer this console is on)が選択されていることを確認してから、Finishを選択します。
5. OKを選択して、Add or Remove Snap-insボックスを閉じます。

4. CSRの生成
   1. 左側のペインで、Certificates (Local Computer)、Personalの順に展開し、Certificatesフォルダを選択します。
   2. Certificatesフォルダを右クリックし、All Tasks > Advanced Operationsの順に移動して、Create Custom Request...を選択します。Certificate Enrollmentウィザードが表示されます。
   3. 概要画面でNextを選択します。
   4. Select Certificate Enrollment Policyページで、Custom Requestの下にリストされているProceed without enrollment policyを選択し、Nextを選択します。
   5. Custom requestページで、選択したTemplateが(No template) CNG keyであり、Request formatがCAに適していることを確認します。PKCS #10はMicrosoft CAで動作します。Nextを選択して、次のページに進みます。
   6. Certificate Informationページで、Detailsという単語の横にあるドロップダウンを選択し、Propertiesボタンを選択します。Certificate Propertiesフォームが表示されます。
   7. Certificate Propertiesフォームのすべてのオプションについては、このドキュメントの範囲外です。詳細については、Microsoftのドキュメントを参照してください。このフォームに関する注意事項とヒントを次に示します。
      - Subject:タブのSubject name:セクションに、必要な値がすべて入力されていることを確認します
      - Common nameに指定した値が、Alternative name:セクションにも指定されていることを確認します
      - Type:をDNSに設定し、Value:ボックスにURLを入力してから、Add >ボタンを選択します
      - 複数のURLを使用してECEにアクセスする場合は、この同じフィールドに各代替名を入力し、それぞれの後でAdd >を選択します
      - Private Keyタブの Key sizeを1024より大きい値に設定していることを確認します。
      - HAのインストールで行われることが多い複数のWebサーバで使用するために証明書をエクスポートする場合は、Make private key exportableを選択していることを確認します。これを行わないと、後で証明書をエクスポートできなくなります
      - 入力した値と選択した内容は検証されません。必要な情報をすべて入力しないと、CAはCSRを完了できません
   8. すべての選択が完了したら、OKをクリックしてウィザードに戻ります。Nextを選択して、次のページに進みます。
   9. Where do you want to save the offline request?ページで、アクセスできる場所のファイル名を選択します。ほとんどのCAでは、形式としてBase 64を選択する必要があります。
   10. ファイルをCAに提供します。署名して証明書を返したら、証明書をWebサーバにコピーし、最後の手順に進みます。
   11. MMCの証明書管理スナップインで、Certificates (Local Computer) > Personalの

順に移動し、Certificatesを右クリックして、All Tasks > Import...の順に選択します。Certificate Import Wizardが表示されます。
12. 初期画面でNextを選択します。
13. File to import画面で、CAによって署名された証明書を選択し、Nextを選択します。
14. Place all certificates in the following storeを選択したことを確認します。
15. Certificate store:ボックスでPersonalが選択されていることを確認し、Nextを選択します。
16. 最後の画面を確認し、Finishを選択してインポートを完了します。
17. MMCコンソールを閉じます。コンソール設定の保存を求めるプロンプトが表示されたら、Noを選択します。これは、証明書のインポートには影響しません。
18. 次の主な手順「証明書のWebサイトへのバインド」に進みます。

ステップ 1.2：Webサイトへの証明書のバインド

⚠ 注意: 「ホスト名」フィールドを空白のままにし、「サイトバインドの編集」ボックスで「サーバー名の表示を必須にする」オプションを選択していないことを確認してください。これらのいずれかが設定されている場合、SPOGはECEとの通信を試みると失敗します。

---

1. インターネットインフォメーションサービス(IIS)マネージャーを開いていない場合は、開きます。
2. 左側のConnectionsペインでSitesに移動し、Default Web Siteを選択します。

   [既定のWebサイト]以外のサイト名を使用する場合は、正しいサイト名を選択してください。

3. 右側のActionsペインからBindings...を選択します。Site Bindingsボックスが表示されます。
   1. Type、https、Port、443の行がない場合は、次の手順を実行します。それ以外の場合は、次の主要な手順に進みます。
      1. Add...ボタンを選択すると、Add Site Bindingボックスが表示されます。
      2. Type:ドロップダウンでhttpsを選択します。
      3. IP address:ドロップダウンにAll Unassignedと表示され、Port:フィールドが443であることを確認します。
      4. Host name:フィールドを空白のままにして、Require Server Name Indicationオプションを選択解除してください。
      5. SSL certificate:ドロップダウンで、前に作成した証明書名に対応する証明書名を選択します。
         - 選択する証明書がわからない場合は、「Select...」ボタンを使用して、サーバにある証明書を表示および検索します
         - View...ボタンを使用して、選択した証明書を表示し、詳細が正しいことを確認します
      6. OKを選択して選択内容を保存します。
   2. Type列でhttpsを示す行を選択し、Edit...ボタンを選択します。Edit Site Bindingボックスが表示されます。
      1. IP address:ドロップダウンにAll Unassignedと表示され、Port:フィールドが443であることを確認します。

2. Host name:フィールドが空白のままになっており、Require Server Name Indicationオプションが選択されていないことを確認します。
3. SSL certificate:ドロップダウンで、前に作成した証明書名に対応する証明書名を選択します。
    - 選択する証明書がわからない場合は、「Select...」ボタンを使用して、サーバにある証明書を表示および検索します
    - View...ボタンを使用して、選択した証明書を表示し、詳細が正しいことを確認します
4. OKを選択して選択内容を保存します。

3. Closeを選択して、IIS Managerに戻ります。
4. IISマネージャを閉じます。

ステップ 2：パーティション管理者SSOの設定

パーティション管理者SSO設定を使用すると、ECEは、SPOGでECEガジェットを開く任意の管理者のパーティションレベルのユーザアカウントを自動的に作成できます。

注：エージェントまたはスーパーバイザSSOを有効にする予定がない場合でも、パーティション管理者SSOを設定する必要があります。

ステップ 2.1：Active Directory(AD)証明書を取得し、キーストアを作成します。

この手順は、Microsoftが発表した最近のセキュリティの変更に対処するために必要になる場合があります。更新が適用されず、ドメインに変更が加えられていない場合、この操作はスキップできます。

詳細については、Microsoft KB4520412の詳細を参照してください。

1. Partition Administrator Configurationフォームで指定したADサーバから、Base 64形式のSSL証明書を取得します。1つの方法が示されています。
    1. ワークステーションを使用して、OpenSSLからWindows用OpenSSLのコピーをダウンロードし、インストールします。Light工ディションで十分です。
    2. OpenSSLコマンドプロンプトを起動します。
    3. 次のコマンドを実行します。サーバー名を、使用しているグローバルカタログドメインコントローラーの完全修飾名で置き換えます。
       openssl s_client -connect gcdcsrv01.example.local:3269
    4. 出力で、Server証明書の行を探します。

```
C:openssl s_client -connect 14.10.162.6:3269
CONNECTED(00000003)
depth=1 DC = com, DC = massivedynamic, CN = MassiveDynamic Enterprise CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:
   i:/DC=com/DC=massivedynamic/CN=MassiveDynamic Enterprise CA
 1 s:/DC=com/DC=massivedynamic/CN=MassiveDynamic Enterprise CA
   i:/C=US/OU=pki.uclabservices.com/O=Cisco Systems Inc/CN=UCLAB Services Root
```

```
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIH1DCCBbygAwIBAgITJwAAAAbAAn/HKFuWCQAAAAAABjANBgkqhkiG9w0BAQsF
ADBcMRMwEQYKCZImiZPyLGQBGRYDY29tMR4wHAYKCZImiZPyLGQBGRYObWFzc2l2
ZWR5bmFtaWMxJTAjBgNVBAMTHE1hc3NpdmVEeW5hbWljIEVudGVycHJpc2UgQ0Ew
HhcNMjAwNDE1MDAxNDM0WhcNMjEwNDE1MDAxNDM0WjAAMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxFajhqjrWqQHfqTXg+SXP5pzvNVrTHIigrAam8D0
```

5. 「-----BEGIN CERTIFICATE-----」の先頭から「-----END CERTIFICATE-----」までの出力をコピーします。BEGIN CERTIFICATE行とEND CERTIFICATE行が含まれていることを確認します。
6. コピーした情報を新しいテキストファイルに貼り付け、crt拡張子を付けてコンピュータに保存します。

2. 証明書ファイルをアプリケーションサーバのいずれかにコピーします。
3. 証明書をコピーしたアプリケーションサーバへのRDPセッションを開きます。
4. 新しいJavaキーストアを作成します。
    1. アプリケーションサーバでコマンドプロンプトを開きます。
    2. ECE Java Development Kit (JDK) binディレクトリに移動します。
    3. 次のコマンドを実行します。必要に応じて値を置き換えます。
       keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c:\ece\pcce\mydomain.jks -storepass MyP@ssword
5. 12.6よりも前のバージョンでは、環境内の他のすべてのアプリケーションサーバ上の同じパスにキーストアをコピーします。バージョン12.6では、ECEを設定するワークステーションからアクセス可能な場所にキーストアをコピーします。

ステップ 2.2：AD Lightweight Directory Access Protocol(LDAP)アクセス情報を使用してECEを設定します。

1. Internet Explorer 11がインストールされているワークステーションまたはコンピュータから、ビジネスパーティションURLに移動します。

ヒント：ビジネスパーティションは、パーティション1とも呼ばれます。ほとんどのインストールでは、https://ece.example.com/defaultのようなURLを使用してBusinessパーティションにアクセスできます。

---

2. paとしてログインし、システムのパスワードを入力します。
3. ログインに成功したら、最初のコンソールでAdministrationリンクを選択します。
4. SSO Configurationフォルダに移動し、Administration > Partition: default > Security > SSO and Provisioningの順に選択します。
5. 右側の上部ペインで、Partition Administration Configurationエントリを選択します。
6. 右側の下部ペインで、Lightweight Directory Access Protocol(LDAP)とADの値を入力します。
    1. LDAP URL：ベストプラクティスとして、グローバルカタログ(GC)ドメインコントローラの名前を使用します。
       GCを使用しない場合、ApplicationServerのログに次のようなエラーが記録されます。
       LDAP認証の例外<@>

javax.naming.PartialResultException：未処理の継続参照；残りの名前 'DC=example,DC=com'

- 非セキュアなグローバルカタログポートは3268
- セキュアグローバルカタログポートは3269です。

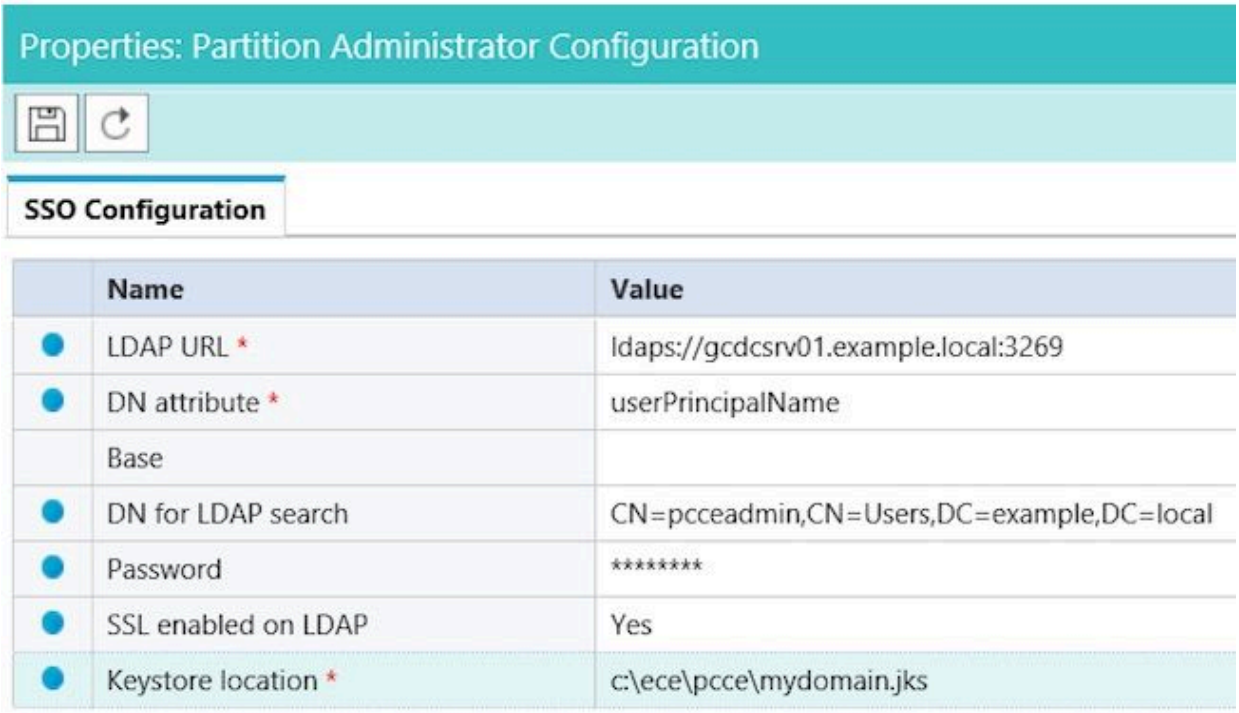
2. DN属性:userPrincipalNameである必要があります。
3. Base:GCを使用する場合は必須ではありません。それ以外の場合は、ベースとなる適切なLDAP形式を指定する必要があります。
4. LDAP検索のDN：ドメインで匿名バインドが許可されていない場合、LDAPにバインドしてディレクトリツリーを検索する機能を持つユーザの識別名を指定する必要があります。

ヒント：ユーザの正しい値を見つける最も簡単な方法は、Active Directory Users and Computersツールを使用することです。次の手順は、この値を見つける方法を示しています。

---

1. ViewメニューからAdvanced Featuresオプションを選択します。
2. ユーザオブジェクトに移動し、右クリックしてPropertiesを選択します。
3. Attributesタブを選択します。
4. Filterボタンを選択してから、Only show attributes with valuesを選択します。
5. リストでdistinquishedNameを検索し、ダブルクリックして値を表示します。
6. 表示された値をハイライト表示し、コピーしてテキストエディタに貼り付けます。
7. テキストファイルの値をコピーして、DN for LDAP検索フィールドに貼り付けます。
   値は、CN=pcceadmin, CN=Users, DC=example, DC=localのようにする必要があります。

5. Password：指定したユーザのパスワードを指定します。
6. LDAPでのSSLの有効化：このフィールドは、ほとんどのお客様で必須と見なすことができます。
7. キーストアの場所:ADからSSL証明書をインポートしたキーストアの場所である必要があります。図に示すように、この例ではc:\ece\pcce\mydomain.jksです。



7. フロッピーディスクのアイコンを選択して変更を保存します。

ステップ 3：構成ファイルの検証

このセクションは、12.0のすべてのインストールに必須です。12.0以外のバージョンでは、このセクションを省略できます。
この手順を必要とするすべてのバージョンには、さらに2つのシナリオがあります。1つ目は、ECEがハイアベイラビリティ設定にインストールされている場合です。2つ目は、Webサーバのホスト名がECEへのアクセスに使用する名前と一致しない場合です。たとえば、ホスト名がUCSVRECEWEB.example.comのサーバにECE Webサーバをインストールしたにもかかわらず、ユーザがURLがchat.example.comのECE Webページにアクセスする場合、このセクションを完了する必要があります。サーバのホスト名とECEにアクセスするURLが同じで、バージョン12.5以降をインストールしている場合は、この手順を省略してセクションを完了できます。

{ECE_HOME}は、ECEをインストールした物理的な場所に置き換えてください。たとえば、ECEをC:\Ciscoにインストールしている場合は、それぞれの場所で{ECE_HOME}をC:\Ciscoに置き換えます。

ヒント：メモ帳やワードパッドでは行末が正しく解釈されないため、メモ帳++などのテキストエディタを使用してください。

1. 展開のすべてのECE Webサーバに対してリモートデスクトップセッションを開きます。
2. このパス{ECE_HOME}\eService\templates\finesse\gadget\spogに移動します。
3. spog_config.jsfileを見つけ、安全な場所にバックアップコピーを作成します。
4. 現在のspog_config.jsfileをテキストエディタで開きます。
5. これら2つの回線を見つけ、展開に合わせて更新します。
   web_server_protocolはhttpsである必要があります。必要に応じて更新してください。
   web_server_nameを更新して、ECEへのアクセスに使用するために割り当てた完全修

飾名と一致させます。例：ece.example.com
    - var web_server_protocol = "https";
    - var web_server_name = "ece.example.com";
6. 変更を保存します。
7. 展開内の他のすべてのWebサーバに対して、この手順を繰り返します。

ステップ 4：ECEをPCCEインベントリに追加

12.0の時点で、PCCEには2000エージェント（2Kエージェント）、4000エージェント（4Kエージェント）、および12000エージェント（12Kエージェント）という3つの異なる展開オプションがあります。これら3つの導入オプションは、2Kエージェントと4K/12Kエージェントの2つのグループに分けることができます。SPOGでの見え方にはいくつかの根本的な違いがあるため、このように分離されています。この段落の後に、2つの方法を非常に高いレベルで比較します。このドキュメントでは、コンポーネントをインベントリに追加するための具体的な手順については説明しません。このプロセスの詳細については、このドキュメントの最後にあるリンクを参照してください。このセクションでは、ECEをPCCEに追加する際に検証する必要がある特定の詳細について説明します。また、このドキュメントでは、PCCEのインストールが完了していること、およびこのソリューションの他の側面にアクセスして設定できることを前提としています。

- 2Kエージェントの導入
    - PCCEコンポーネントの初期設定は、CCE Administrationによって完全に実行され、自動化されています
    - 新しいコンポーネントは、IPまたはホスト名、必要なクレデンシャル、またはコンポーネント固有の設定などの詳細を入力するポップアップボックスを介してインベントリページに追加されます
- 4Kおよび12Kエージェントの導入
    - 初期設定の多くは、UCCEで使用される手順と同じです
    - コンポーネントは、CCE Administrationからダウンロードしたカンマ区切り値(CSV)ファイルを介して追加され、特定のインストールごとに入力された後、アップロードされます
    - 初期導入では、最初のCSVファイルに含める特定のコンポーネントが必要です
    - システムの初期設定時に追加されなかったコンポーネントは、必要な情報を含むCSVファイルで追加されます

ステップ 4.1：ECE Webサーバ証明書のJavaキーストアへのアップロード

1. 自己署名証明書が使用されている場合
    1. プライマリのサイドA管理データサーバ(ADS)へのリモートデスクトップ接続を開きます。
    2. Internet Explorer 11を管理者として開き、ECEビジネスパーティションに移動します。
    3. URLバーの右側にある南京錠のアイコンを選択し、View Certificatesを選択します。
    4. Certificateボックスで、Detailsタブを選択します。
    5. タブの下部にあるCopy to File...を選択します。
    6. Certificate Export Wizardで、Export File Formatページが表示されるまでNextを選択します。Base-64 encoded X.509 (.CER) formatを選択していることを確認します。

7. 証明書をADSサーバ上のc:\Temp\certificatesなどの場所に保存して、エクスポートを完了します。
8. 証明書を他のすべてのADSサーバにコピーします。
9. 管理コマンドプロンプトを開きます。
10. Javaホームディレクトリに移動し、次にbinディレクトリに移動します。Javaホームディレクトリは、次のコマンドでアクセスできます。cd %JAVA_HOME%\bin
11. 現在のcacertsファイルをバックアップします。cacertsファイルを%JAVA_HOME%\lib\securityから別の場所にコピーします。
12. このコマンドを実行して、以前に保存した証明書をインポートします。キーストアのパスワードが「changeit」でない場合は、インストールに合わせてコマンドを更新します。
    keytool -keystore ../lib/security/cacerts -storepass changeit -import -alias <ECEサーバーのFQDN> -file <証明書を保存した場所>
13. ADSサーバを再起動します。
14. 他のADSサーバーで手順8 ~ 12を繰り返します。

2. CA署名付き証明書が使用されている場合
    1. DER/PEM形式のルートおよび中間証明書を取得し、すべてのADSサーバのC:\Temp\certificatesなどの場所にコピーします。

    > 注:CA管理者に連絡して、これらの証明書を取得してください。

    2. プライマリのサイドA ADSへのリモートデスクトップ接続を開きます。
    3. 管理コマンドプロンプトを開きます。
    4. Javaホームディレクトリに移動し、次にbinディレクトリに移動します。Javaホームディレクトリは、次のコマンドでアクセスできます。cd %JAVA_HOME%\bin
    5. 現在のcacertsファイルをバックアップします。cacertsファイルを%JAVA_HOME%\lib\securityから別の場所にコピーします。
    6. このコマンドを実行して、以前に保存した証明書をインポートします。キーストアのパスワードが「changeit」でない場合は、インストールに合わせてコマンドを更新します。
       keytool -keystore ../lib/security/cacerts -storepass changeit -trustcacerts -import -alias <CAルートの名前> -file <ルート証明書を保存した場所>
    7. ステップ6を繰り返し、中間証明書が存在する場合はインポートします。
    8. ADSサーバを再起動します。
    9. 他のすべてのADSサーバーで手順2 ~ 12を繰り返します。

ステップ 4.2：ECEデータサーバのインベントリへの追加

- データサーバはシステムインベントリに存在する必要がありますが、PCCE ADSとデータサーバ間の直接通信は行われません
- ECEが1500エージェントの導入で導入される場合、データサーバはサービスサーバです
- ECEがHA設定にインストールされている場合、サイドAサービスサーバのみを追加します

ステップ 4.3：ECE Webサーバのインベントリへの追加

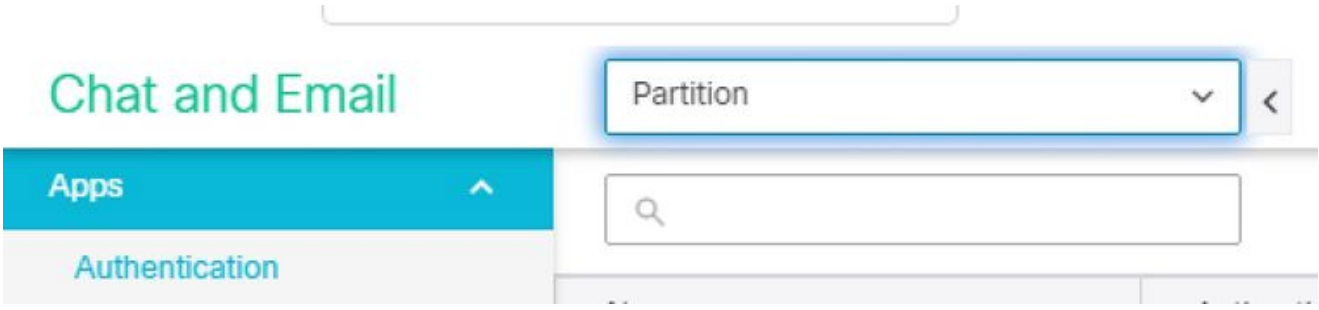
- Webサーバを完全修飾名で追加していることを確認します

    - この名前は、ECE証明書内の共通名と一致するか、サブジェクト代替名(SAN)の1つとしてリストされている必要があります
    - ホスト名またはIPアドレスだけを使用しないでください
- ECEのユーザ名とパスワードはpaログインクレデンシャルである必要があります
- アプリケーションインスタンスが正しいことを確認します
    - アプリケーションインスタンス名は大文字と小文字が区別されます
    - 2000エージェントPCCEの導入では、アプリケーションインスタンスはMultiChannelです
    - 4000/12000 Agent PCCE展開の場合、アプリケーションインスタンスには名前の一部としてサイトとペリフェラルセットが含まれます
- 1500エージェント環境や400エージェントHA環境など、複数のWebサーバーにECEがインストールされている場合は、ロードバランサを指すURLか、個々のWebサーバーを指すURLのいずれかをWebサーバーの完全修飾名として使用できます。ベストプラクティスは、ロードバランサを使用することです。
- 複数のECE展開がある場合、または複数のECEガジェットを含む展開にそれぞれのWebサーバを追加する場合、SPOGでECEガジェットを開いたときに正しいWebサーバを選択することがよくあります。

ステップ 5：ECEとPCCEの統合

1. 管理者としてCCE Administrationにログインします。
2. Email and Chatカードを選択し、次に図に示すようにEmail and Chatリンクを選択します。

3. Device Nameドロップダウンで現在選択されているサーバを確認します。両方のWebサーバをHAインストールに追加した場合は、いずれかのWebサーバを選択できます。システムに2つ目のECE導入を後で追加する場合は、適切なサーバを選択してから続行してください。
4. Chat and Emailの横にあるドロップダウンで、図に示すように、PartitionまたはGlobalを選択します。



5. トップメニューでIntegrationを選択し、図に示すようにUnified CCEの横にある矢印を選択して2番目のUnified CCEを選択します。

6. インストールのAWDB Detailsタブの値を入力し、Saveボタンを選択します。
7. Configurationタブを選択し、次のように入力します。
    1. Application Instanceの横にあるドロップダウンを選択し、ECE用に作成されたアプリケーションインスタンスを選択します。

> 注：これは、UQで始まるアプリケーションインスタンスであってはなりません。

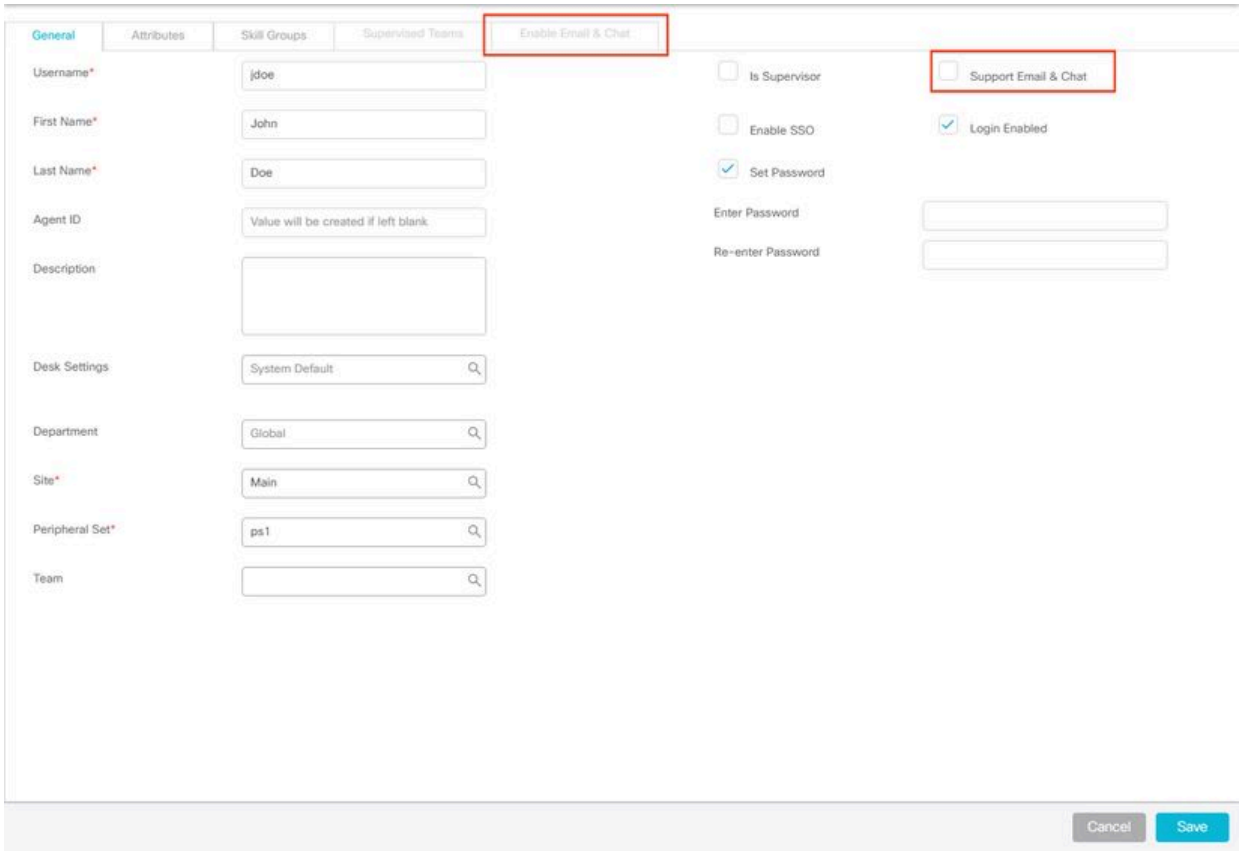
    2. 緑色の白いプラス記号の付いた円ボタンを選択し、Agent PGを選択します。
        1. Agent PG（複数の場合はAgent PG）を選択します。
        2. すべてのAgent PGを追加したら、Saveを選択します。

> 警告: Saveを選択すると、システムはPCCEに永続的に接続され、元に戻すことはできません。このセクションでエラーが発生した場合は、ECEを完全にアンインストールしてすべてのデータベースを削除してから、新規インストールの場合と同様にECEをインストールする必要があります。

手順 6：ECE統合の検証

1. CCE Administrationで、上部のステータスバーにアラートが表示されていないことを確認します。 アラートがある場合は、Alertsという語を選択してInventoryページを確認し、ECEサーバに対するアラートがないことを確認します。
2. 左側のナビゲーションバーでUsers、次にAgentsの順に選択します。

3. リストからエージェントを選択して確認します。
    1. Support Email & Chatの新しいチェックボックスがGeneralタブに表示されます。
    2. 次の図に示すように、「Enable Email & Chat」というラベルの付いた新しいタブが表示されます。



4. ECEのテストエージェントを有効にします。
    1. Support Email & Chatチェックボックスを選択し、Enable Email & Chatタブが選択できるようになったことを確認します。
    2. Enable Email & Chatタブを選択し、Screen Nameフィールドに値を入力します。
    3. Saveを選択して、ユーザを更新します。
    4. 成功メッセージが表示されます。
5. ECEが更新されていることを確認します。
    1. Overviewナビゲーションボタンを選択してから、Email and Chatカードとリンクを選択します。
    2. Chat and Emailの横にあるドロップダウンで、エージェントの部署に対応する名前を選択します。

注:ECEのサービス部門は、PCCEのグローバル部門に属するすべてのオブジェクトを保持します。したがって、部門名Serviceは予約済みの値です。

---

        1. トップメニューでUser Managementを選択し、Chat and Emailの下のメニューでUsersを選択します。
        2. 新しいエージェントがリストに表示されることを確認します。

トラブルシュート

複数のツールをダウンロードし、ECEサーバに保持することをお勧めします。これらの方法を使用すると、ソリューションのトラブルシューティングとメンテナンスが大幅に容易になります。

- メモ帳などのテキストエディタ++
- 7-Zipなどのアーカイブツール
- Windows用の多くのTailプログラムの1つ
  次に例をいくつか示します。
  - ベアテール
  - Win32のTail

統合に関する問題をトラブルシューティングするには、まず重要なログファイルとそれぞれの場所を把握しておく必要があります。

1. ECEのファイル名と場所

   ECEシステムには多くのログがあります。これらは、統合に関する問題をトラブルシューティングする際に最も役立つログです。

ログファイル	サーバ	命名規則	説明
アプリケーション サーバ	C/A	eg_log_{HOSTNAME}_ApplicationServer.log	Wildflyサーバからのログ
外部エージェントの割り当て	C/S	eg_log_{ホスト名}_EAAS-process.log	MR PGとのインタラクション
外部エージェントメッセージング	C/S	eg_log_{ホスト名}_EAMS-process.log	CTIサーバとのインタラクション
ルートログ	C/A/M/秒	egpl_root_{ホスト名}.log	プロセス間ログ、HazelCast、一般的なエラー
コンポーネントステータス	C/A/M/秒	例：log_{HOSTNAME}_component-status.log	プロセスの開始とファイルコピーの完了
プロセス起動ツール	C/A/M/秒	eg_log_{HOSTNAME}_ProcessLauncher.log	サービスおよびプロセスの開始に関する一般的なログ

分散サービスマネージャ	C/S	eg_log_{ホスト名}_DSMController.log	サービスサーバでのプロセスの開始と停止を示すログ

サーバキー：

- C =コロケートされたサーバ
- A =アプリケーションサーバ
- S =サービスサーバ
- M =メッセージングサーバ

ほとんどのログファイルには、他の2つのログも関連付けられています。

- eg_log_{SERVERNAME}_{PROCESS}.log：プライマリ・プロセス・ログ
- eg_log_dal_connpool_{SERVERNAME}_{PROCESS}.log – 接続プールの使用状況
- eg_log_query_timeout_{SERVERNAME}_{PROCESS}.log：タイムアウトが原因でクエリーが失敗すると更新される

2. PCCEのファイル名と場所

統合の問題に関するPCCEログはすべてサイドAのADSにあります。統合に関する問題をトラブルシューティングする際に最も重要となるログを次に示します。これらはそれぞれ、C:\icm\tomcat\logsにあります。

ログファイル	命名規則	説明
CCBU	CCBU.{YYYY}-{MM}-{DD}T{hh}-{mm}-{ss}.{msec}.startup.log	CCE Adminおよびすべての関連Webアプリケーションのプライマリログ
CCBUエラー	エラー。{YYYY}-{MM}-{DD}T{hh}-{mm}-{ss}.{msec}.startup.log	CCE管理者および関連するWebアプリケーションによって表示されるエラー
カタリナ	カタリナ。{YYYY}-{MM}-{DD}.log	Tomcatネイティブログ。証明書エラーが表示されます。
Tomcat stdout	tomcat9-stdout.{YYYY}-{MM}-{DD}.log	Tomcatからの標準的なOutログメッセージ
Tomcat stderr	tomcat9-stderr.{YYYY}-{MM}-{DD}.log	Tomcatからの標準エラーログメッセージ

これらのログのうち、最初の3つは最も頻繁に要求され、確認されています。

トレースレベルを設定し、必要なログを収集するには、次の手順を使用します。

3. トレースレベルの設定

このセクションはECEにのみ適用されます。PCCEから要求されるログは、シスコによってトレースレベルが設定されており、変更できません。

1. Internet Explorer 11がインストールされているワークステーションまたはコンピュータから、システムパーティションURLに移動します。

   ヒント：システムパーティションは、パーティション0とも呼ばれます。ほとんどのインストールでは、https://ece.example.com/systemのようなURLでシステムパーティションにアクセスできます。

2. saとしてログインし、システムのパスワードを入力します。
3. ログインに成功したら、最初のコンソールでSystemリンクを選択します。
4. Systemページで、System > Shared Resources > Logger > Processesの順に展開します。
5. 右上のペインで、トレースレベルを変更するプロセスを見つけて選択します。
   注：HAシステムおよび複数のApplication Serverを持つシステムでは、プロセスが複数回表示されます。データを確実にキャプチャするには、プロセスを含むすべてのサーバのトレースレベルを設定します。
6. 右下のペインで、Maximum trace levelのドロップダウンを選択し、適切な値を選択します。
   ECEには8つのトレースレベルが定義されています。このリストの4は、最も頻繁に使用されるものです。
   - 2 – エラー – プロセスの既定のトレースレベル
   - 4 - Info – 問題の解決に通常使用されるトレースレベル
   - 6 - Dbquery – セットアップの早い段階で問題を診断したり、より複雑な問題を診断したりするのに役立ちます。
   - 7 - Debug – 非常に詳細な出力。最も複雑な問題でのみ必要

   注：プロセスを6 - Dbquery以上で長時間放置しないでください。通常はTACのガイダンスがあるだけです。

   ほとんどのプロセスのトレースレベル、2-Errorを保持します。レベル7または8を選択する場合は、最大期間も選択する必要があります。最大継続時間に達すると、トレースレベルは最後に設定されたレベルに戻ります。
   システムの設定後、これら4つのプロセスをトレースレベル4に変更します。

   - EAASプロセス
   - EAMSプロセス
   - DXプロセス
   - rxプロセス
7. 保存アイコンを選択して、新しいトレースレベルを設定します。

4. ログファイルの収集

1. プロセスが必要なログを記録するサーバへのリモートデスクトップセッションを開きます。
2. ログファイルの場所に移動します。
    1. ECEサーバ

       ログは次のように書かれています。

       - デフォルトでは、ログは最大サイズが5 MBのファイルに書き込まれます
       - 1つのログファイルが設定された最大値に達すると、{LOGNAME}.log.{#}という形式で名前が変更されます
       - ECEは、以前の49個のログファイルと現在のファイルを保持します
       - 現在のログは常に.logで終わり、
       - ログはアーカイブも圧縮もされない
       - ほとんどのログには共通の構造があります
       - ログファイルでは、<@>を使用してセクションを区切ります
       - ログは常にGMT+0000時間で書き込まれる

       ECEログは、特定のインストールに基づいて異なる場所に配置されます。

        1. 400のエージェント導入
            1. 片面
                - サーバ：コロケートサーバ
                - 場所：{ECE_HOME}\eService_RT\logs
            2. high-availability
                - サーバ：両方のコロケーションサーバ
                - 場所：{ECE_HOME}\eService\logs
                - 分散ファイルシステム(DFS)共有のために作成されたディレクトリには、インストールとアップグレードのログだけが含まれます。
                - Distributed Systems Manager (DSM)ロールを所有するサーバーだけが、サービスロールの一部であるコンポーネントのログを書き込みます
                    - DSMロールの所有者は、Windowsタスクマネージャーの[プロセス]タブで確認できます。このサーバには、セカンダリサーバにはないJavaプロセスが10 ~ 15個あります。
                    - DSMの下のコンポーネントには、EAAS、EAMS、Retriever、Dispatcher、Workflowなどがあります。
        2. 1500エージェントの導入
            - ロールをホストするサーバ上のログ
            - 場所：{ECE_HOME}\eService\logs
            - サービスサーバを除くすべてのサーバが動作し、コンポーネントに関連付けられているすべてのプロセスのログを書き込みます
            - ハイアベイラビリティ展開では、サービスサーバはアクティブ/スタンバイ設定で動作します
            - Distributed Systems Manager(DSM)ロールを所有するサーバだけがロ

グを書き込みます
- DSMロールの所有者は、Windowsタスクマネージャーに表示されるプロセスの数で識別できます。プライマリサーバでは10 ~ 15のJavaプロセスが実行され、セカンダリサーバでは4つのJavaプロセスのみが実行されます

2. PCCEサーバ
   - PCCEからの必要なログは、C:\icm\tomcat\logsにあります。
   - Tomcatログはロールオーバーまたはアーカイブされません
   - ログはローカルサーバの時刻で書き込まれる
3. 問題が確認された後に作成または変更されたすべてのログを収集します。
   ログと発生する問題の詳細な説明は、このドキュメントの範囲外です。一般的な問題、確認事項、および考えられる解決策を次に示します。
   - 証明書に関連する問題
     - 証明書がインポートされていません
       - 動作： SPOGでECEガジェットを開こうとすると、「ページの読み込み中にエラーが発生しました。管理者に問い合わせてください。」
       - チェック：PCCEのCatalinaログで、次のような エラーが発生していないかどうかを確認します javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIXパスの構築に失敗しました： sun.security.provider.certpath.SunCertPathBuilderException：要求されたターゲットへの有効な認証パスが見つかりません
       - 解決策：ECE Webサーバ証明書または適切なCA証明書をADSのキーストアにインポートしたことを確認します
     - 証明書の不一致
       - 動作：SPOGでECEガジェットを開こうとすると、証明書の共通名またはサブジェクトの代替名が設定された名前と一致しないことを示すエラーが表示されます。
       - チェック：SSL証明書の検証
       - 解決方法： [件名]の[共通名]フィールド、または[サブジェクト代替名]のいずれかの[DNS]フィールドに、Webサーバー名としてSPOGに入力した完全修飾名が含まれていることを確認します。
   - システムに関する問題
     - サービスが開始されていません
       - 動作： SPOGでECEガジェットを開こうとすると、「https://{url}のWebページが一時的にダウンしているか、新しいアドレスに永続的に移動している可能性があります」というエラーが表示されます。
       - チェック：Webサーバを除くすべてのECEサーバでWindowsサービス – Ciscoサービスが開始されていることを確認します。Application Serverのルートログでエラーを確認します
       - 解決策：すべてのECEサービスでシスコサービスを開始します。
   - 設定の問題
     - LDAPの設定
       - 動作： SPOGでECEガジェットを開こうとすると、「ページの読み込み中にエラーが発生しました。管理者に問い合わせてください。」

- チェック：アプリケーション・サーバーのトレース・レベルをレベル7- Debugに上げ、ログインを再試行してアプリケーション・サーバー・ログを確認します。LDAPという単語を検索します。
- 解決策：パーティション管理者SSOのLDAP設定が正しいことを確認します。

関連情報

これらは、ECEのインストールまたは統合を開始する前に十分に確認する必要がある重要なドキュメントです。これはECEドキュメントの包括的なリストではありません。

⚠ 注意：ほとんどのECEドキュメントには2つのバージョンがあります。PCCE用のバージョンをダウンロードして使用していることを確認してください。ドキュメントのタイトルは、バージョン番号の後にPackaged Contact Center Enterprise(PCE)または（PCCE用）または（UCCEおよびPCCE用）のどちらかになります。

インストール、アップグレード、または統合の前に、Cisco Enterprise ChatおよびEメールのドキュメントのスタートページで更新がないかどうかを確認してください。

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

- 12.0
  - エンタープライズチャットおよび電子メールのインストールと設定ガイド
  - エンタープライズチャットおよびEメールアップグレードガイド
  - エンタープライズチャットおよびEメール管理者ガイド
- 12.5
  - エンタープライズチャットおよび電子メールのインストールと設定ガイド
  - エンタープライズチャットおよびEメールアップグレードガイド
  - エンタープライズチャットおよびEメール管理者ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。