Intégrer ECE avec PCCE dans les versions 12.0 et ultérieures

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Terminologie
- Étapes prérequises
- Étapes d'intégration
  - Étape 1. Configurer les certificats SSL
    - Étape 1.1. Générer un certificat
    - Étape 1.2. Lier le certificat au site Web
  - Étape 2. Configurer l'administrateur de partition SSO
    - Étape 2.1. Obtenir un certificat Active Directory (AD) et créer un magasin de clés.
    - Étape 2.2. Configurez ECE avec les informations d'accès LDAP (Lightweight Directory Access Protocol) AD.
  - Étape 3. Valider le fichier de configuration
  - Étape 4. Ajouter ECE à l'inventaire PCCE
    - Étape 4.1. Télécharger le certificat du serveur Web ECE dans le magasin de clés Java
    - Étape 4.2. Ajouter le serveur de données ECE à l'inventaire
    - Étape 4.3. Ajouter le serveur Web ECE à l'inventaire
  - Étape 5. Intégrer ECE et PCCE
  - Étape 6. Valider l'intégration ECE
- Dépannage
  - Noms et emplacements des fichiers sur la CEE
  - Noms et emplacements des fichiers sur PCCE
  - Configuration du niveau de suivi
  - Collecte des fichiers journaux
- Informations connexes

Introduction

Ce document décrit les étapes d'intégration de la messagerie instantanée d'entreprise (ECE) avec Packaged Contact Center Enterprise (PCCE) dans les versions 12.0 et ultérieures

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Chat et e-mail d'entreprise (ECE) 12.x
- Packaged Contact Center Enterprise (PCCE) 12.x

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- CEE 12.5 1)
- PCCE 12.5(1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

PCCE version 12.0 a introduit une nouvelle interface de gestion appelée SPOG (Single Pane of Glass). La quasi-totalité de la gestion du centre de contacts et des applications associées est désormais effectuée dans cette interface. Afin d'intégrer correctement à la fois ECE et PCCE, vous devez effectuer plusieurs étapes qui sont uniques à cette intégration. Ce document vous guide tout au long de ce processus.

Terminologie

Dans le présent document, ces termes sont utilisés.

- Enterprise Chat and Email (ECE) : ECE est un produit qui permet d'acheminer les e-mails et les demandes de discussion vers les agents du centre de contact de la même manière que les appels vocaux.
- Single Pane of Glass (SPOG) - SPOG est la façon dont l'administration de PCCE est effectuée dans la version 12.0 et ultérieure. SPOG est une réécriture complète de l'outil d'administration CCE qui était utilisé dans les versions antérieures à 12.0.
- Autorité de certification (CA) : entité qui émet des certificats numériques conformément à un modèle d'infrastructure à clé publique (PKI).

  Il existe deux types d'autorités de certification que vous pouvez rencontrer.

  - Autorité de certification publique : une autorité de certification publique est une autorité dont les certificats racine et intermédiaires sont inclus dans la plupart des navigateurs et systèmes d'exploitation. Parmi les autorités de certification publiques courantes, citons IdenTrust, DigiCert, GoDaddy et GlobalSign.
  - Autorité de certification privée : une autorité de certification privée est une autorité de certification qui existe au sein d'une société. Certaines autorités de certification privées sont signées par des autorités de certification publiques, mais il s’agit le plus souvent

d’autorités de certification autonomes et les certificats qu’elles émettent ne sont approuvés que par les ordinateurs de cette organisation.

Dans l'un ou l'autre des deux types d'autorité de certification, il existe deux types de serveurs d'autorité de certification.

  - Serveur AC racine : le serveur AC racine signe son propre certificat. Dans le déploiement PKI multiniveau standard, l'autorité de certification racine est hors ligne et inaccessible. L'autorité de certification racine de ce modèle émet également uniquement des certificats à un autre serveur d'autorité de certification connu sous le nom d'autorité de certification intermédiaire. Certaines entreprises choisissent de n'utiliser qu'une autorité de certification de niveau unique. Dans ce modèle, l'autorité de certification racine émet des certificats destinés à être utilisés par une entité autre qu'un autre serveur d'autorité de certification.
  - Serveur AC intermédiaire : le serveur AC intermédiaire ou émetteur émet des certificats destinés à être utilisés par une entité autre qu'un autre serveur AC.
- Microsoft Management Console (MMC) : application incluse dans Microsoft Windows qui permet de charger divers composants logiciels enfichables. Vous pouvez utiliser les composants logiciels enfichables pour créer une console personnalisée pour l'administration du serveur. De nombreux composants logiciels enfichables différents sont inclus dans Windows. Les certificats, le Gestionnaire de périphériques, la Gestion des disques, l'Observateur d'événements et les Services sont quelques exemples de ces fonctionnalités.
- Équilibreur de charge réseau (NLB) : périphérique ou application qui présente plusieurs ressources physiques aux utilisateurs finaux sous un nom physique commun. Les NLB sont très courants avec les applications et les services Web. Les NLB peuvent être implémentés de plusieurs manières. Lorsqu'il est utilisé avec ECE, l'équilibrage de la charge réseau doit être configuré de manière à garantir que les sessions utilisateur retournent au même serveur Web principal physique à l'aide d'une insertion de cookie ou d'une méthode équivalente. C'est ce qu'on appelle une session rémanente avec cookie-insert. La session rémanente fait simplement référence à la capacité d'un équilibreur de charge à renvoyer la session d'un utilisateur au même serveur principal physique pour toutes les interactions.
  - Passthrough SSL (Secure Sockets Layer) : le passthrough SSL est une méthode dans laquelle la session SSL existe entre le périphérique de l'utilisateur final et le serveur Web physique auquel la session de l'utilisateur a été attribuée. Le passthrough SSL n'autorise pas l'insertion de cookies car la session HTTP est physiquement chiffrée à tout moment. La plupart des NLB prennent en charge les sessions rémanentes avec le Passthrough SSL en utilisant des tables de contrôle qui surveillent les parties serverhello et clienthello de la configuration de session et stockent les valeurs uniques dans une table. Lorsque la requête suivante qui correspond à ces valeurs est présentée à l’équilibrage de la charge réseau, la table stick peut être utilisée pour renvoyer la session au même serveur principal.
  - Déchargement SSL : lorsqu'un NLB est configuré pour le déchargement SSL, il existe deux sessions ou tunnels SSL pour une session d'utilisateur final donnée. La première se situe entre le périphérique de l'utilisateur final et l'adresse IP virtuelle (VIP) configurée sur l'équilibrage de la charge réseau du site Web. La seconde se situe entre l’adresse IP back-end de l’équilibrage de la charge réseau et le serveur Web physique

auquel la session de l’utilisateur est attribuée. Le déchargement SSL ne prend pas en charge l'insertion de cookies car le flux HTTP est entièrement déchiffré tandis que sur l'équilibrage de charge réseau, où des cookies HTTP supplémentaires peuvent être insérés et une inspection de session peut être effectuée. Le déchargement SSL est souvent utilisé lorsque l'application Web ne requiert pas SSL, mais est effectuée pour des raisons de sécurité. Les versions actuelles d'ECE ne prennent pas en charge l'accès à l'application dans une session non SSL.

Étapes prérequises

Plusieurs conditions préalables doivent être remplies avant de commencer à intégrer les deux systèmes.

- Niveau de correctif PCCE minimum
  - Version 12.0(1) - ES37
  - Version 12.5(1) - Pas de minimum actuel pour la fonctionnalité de base
- Niveau de raccordement CEE minimal

  Il est recommandé que la CEE exécute la dernière offre spéciale d'ingénierie (ES) disponible.

  - Version 12.0(1) - ES3 + ES3_ET1a
  - Version 12.5(1) - Pas de minimum actuel pour la fonctionnalité de base
- Éléments de configuration

  Veillez à associer les domaines de routage de support ECE_Email, ECE_Chat et ECE_Outbound Media Routing (MRD) à l'instance d'application appropriée.

  - Pour le modèle de déploiement de l'agent PCCE 2000, l'instance d'application est multicanal et est préconfigurée lors du déploiement de PCCE.
  - Pour le modèle de déploiement d'agent PCCE 4000/12000, l'instance d'application peut être n'importe quel nom et doit être créée par la personne qui effectue l'intégration. La meilleure pratique consiste à utiliser la forme {site}_{peripheral_set}_{application_instance}.
    Si vous avez installé PCCE avec le nom de site Main, le périphérique défini sur PS1 et l'instance d'application Multichannel, le nom de l'instance d'application est Main_PS1_Multichannel.

Remarque : le nom de l'instance d'application est sensible à la casse. Veillez à taper le nom correctement lorsque vous ajoutez le serveur Web ECE à l'inventaire.

Étapes d'intégration

Les détails de toutes les étapes du présent document sont tous traités dans la documentation de la CEE et du PCCE, mais ils ne figurent pas dans une liste et ne figurent pas tous dans le même document. Pour plus d'informations, reportez-vous aux liens fournis à la fin de ce document.

Étape 1. Configurer les certificats SSL

Vous devez générer un certificat à utiliser par le serveur Web de la CEE. Vous pouvez utiliser un certificat auto-signé, mais il est souvent plus facile d'utiliser un certificat signé par une autorité de certification. Les certificats auto-signés ne sont pas moins sécurisés que les certificats signés par une autorité de certification. Il y a moins d'étapes à suivre pour créer le certificat, mais lorsque le certificat doit être remplacé, n'oubliez pas de télécharger le nouveau certificat vers les magasins de clés Java sur tous les serveurs de données d'administration PCCE. Si vous utilisez un certificat signé par une autorité de certification, il vous suffit de télécharger les certificats racine et, le cas échéant, les certificats intermédiaires vers les magasins de clés.

Si votre déploiement comporte plusieurs serveurs Web, vous devez consulter ces instructions. Les étapes spécifiques requises pour configurer un équilibreur de charge réseau sortent du cadre de ce document. Contactez le fournisseur de votre équilibreur de charge pour obtenir de l'aide si nécessaire.

- Bien qu'il ne soit pas nécessaire, un équilibreur de charge simplifie grandement la mise en oeuvre
- L'accès à l'application ECE sur chaque serveur Web doit utiliser SSL quelle que soit la méthode d'équilibrage de charge utilisée
- L'équilibreur de charge peut être configuré en tant que passthrough SSL ou déchargement SSL
- Si vous choisissez SSL passthrough :
    - Vous devez effectuer toutes les opérations de certificat à partir d'un serveur
    - Une fois le certificat correctement configuré, vous devez l'exporter et vous assurer que la clé privée est incluse dans un fichier PFX (Personal Information Exchange)
    - Vous devez copier le fichier PFX sur tous les autres serveurs Web du déploiement, puis importer le certificat dans IIS
- Si vous choisissez le déchargement SSL, chaque serveur Web peut être configuré avec son propre certificat SSL

Remarque : si vous disposez de plusieurs serveurs Web et que vous choisissez SSL passthrough sur votre serveur Web, ou si vous souhaitez avoir un certificat commun sur tous les serveurs, vous devez choisir un serveur Web pour effectuer l'étape 1, puis importer le certificat sur tous les autres serveurs Web.
Si vous choisissez le déchargement SSL, vous devez effectuer ces étapes sur tous les serveurs Web. Vous devez également générer un certificat à utiliser sur votre équilibreur de charge.

Étape 1.1. Générer un certificat

Vous pouvez ignorer cette section si vous avez déjà créé ou obtenu un certificat, sinon choisissez l'une des deux options.

Option 1. Utiliser un certificat auto-signé

1. Accédez à IIS Administration.
2. Sélectionnez le nom du serveur dans l'arborescence Connexions située à gauche.
3. Recherchez Server Certificates dans le volet central et double-cliquez pour l'ouvrir.
4. Sélectionnez Créer un certificat auto-signé... dans le volet Actions sur la droite.
5. Dans la fenêtre Créer un certificat auto-signé, choisissez et entrez un nom dans la zone Spécifier un nom convivial pour le certificat :. Ce nom indique comment le certificat apparaît dans le processus de sélection à l'étape principale suivante. Ce nom ne doit pas nécessairement correspondre au nom commun du certificat et n'affecte pas la façon dont le certificat apparaît à l'utilisateur final.
6. Assurez-vous que Personal est sélectionné dans la liste déroulante Select a certificate store for the new certificate:.
7. Sélectionnez OK pour créer le certificat.
8. Passez à l'étape majeure suivante, Lier le certificat au site Web.

Option 2. Utiliser un certificat signé par une autorité de certification

Les certificats signés par une autorité de certification nécessitent la génération d'une demande de signature de certificat (CSR). Le CSR est un fichier texte qui est ensuite envoyé à l'autorité de certification où il est signé, puis le certificat signé ainsi que les certificats d'autorité de certification requis sont renvoyés et le CSR est exécuté. Vous pouvez choisir d'effectuer cette opération via l'administration IIS ou via la console MMC (Microsoft Management Console). La méthode d'administration IIS est beaucoup plus facile sans connaissances particulières requises, mais vous permet seulement de configurer les champs qui sont inclus dans l'attribut Subject du certificat et de modifier la longueur en bits. MMC exige des étapes supplémentaires et que vous possédiez une connaissance approfondie de tous les champs requis dans un CSR valide. Il est fortement recommandé d'utiliser MMC uniquement si vous disposez d'une expérience modérée à spécialisée en création et gestion de certificats. Si votre déploiement nécessite que l'ECE soit accessible par plusieurs noms complets ou si vous devez modifier une partie du certificat, à l'exception du sujet et de la longueur de bit, vous devez utiliser la méthode MMC.

1. Via l'administration IIS

   Suivez ces étapes pour générer une demande de signature de certificat (CSR) via le Gestionnaire des services Internet (IIS).

   1. Accédez à IIS Administration.
   2. Sélectionnez le nom du serveur dans l'arborescence Connexions située à gauche.
   3. Recherchez Server Certificates dans le volet central et double-cliquez pour l'ouvrir.
   4. Sélectionnez Créer une demande de certificat... dans le volet Actions sur la droite. L'Assistant Demande de certificat apparaît.
   5. Sur la page Propriétés de Nom unique, entrez les valeurs du formulaire correspondant à votre système. Tous les champs doivent être renseignés. Sélectionnez Next pour continuer.

6. Sur la page Propriétés du fournisseur de services de chiffrement, conservez la sélection par défaut du fournisseur de services de chiffrement :. Modifiez la liste déroulante Longueur de bit : à un minimum de 2048. Sélectionnez Next pour continuer.
7. Dans la page Nom de fichier, sélectionnez un emplacement où vous souhaitez enregistrer le fichier CSR.
8. Fournissez le fichier à l'autorité de certification. Lorsque vous avez reçu le certificat signé, copiez-le sur le serveur Web et passez à l'étape suivante.
9. Au même emplacement dans le Gestionnaire des services Internet, sélectionnez Terminer la demande de certificat dans le volet Actions. L'assistant apparaît.
10. Sur la page Spécifier la réponse de l'autorité de certification, sélectionnez le certificat fourni par votre autorité de certification. Donnez un nom dans la zone Nom convivial. Ce nom indique comment le certificat apparaît dans le processus de sélection à l'étape principale suivante. Assurez-vous que la liste déroulante Sélectionner un magasin de certificats pour le nouveau certificat : est définie sur Personnel.
11. Sélectionnez OK pour terminer le téléchargement du certificat.
12. Passez à l'étape majeure suivante, Lier le certificat au site Web.

2. Via Microsoft Management Console (MMC)

   Suivez ces étapes pour générer un CSR via MMC. Cette méthode vous permet de personnaliser chaque aspect de la CSR.

   1. Cliquez avec le bouton droit sur le bouton Démarrer et sélectionnez Exécuter.
   2. Tapez mmc dans la zone Exécuter et sélectionnez OK.
   3. Ajoutez le composant logiciel enfichable Certificat à la fenêtre MMC.
      1. Sélectionnez Fichier, puis Ajouter/Supprimer un composant logiciel enfichable... La boîte Ajouter ou supprimer des composants logiciels enfichables s'affiche.
      2. Dans la liste de gauche, localisez Certificates et sélectionnez Add >. La zone du composant logiciel enfichable Certificats s'affiche.
      3. Sélectionnez l'option Compte d'ordinateur, puis Suivant >.
      4. Assurez-vous que Ordinateur local : (l'ordinateur sur lequel se trouve cette console) est sélectionné dans la page Sélectionner un ordinateur, puis sélectionnez Terminer.
      5. Cliquez sur OK pour fermer la zone Ajouter ou supprimer des composants logiciels enfichables.
   4. Générer le CSR
      1. Dans le volet gauche, développez Certificates (Local Computer), puis Personal et sélectionnez le dossier Certificates.
      2. Cliquez avec le bouton droit sur le dossier Certificates et naviguez jusqu'à All Tasks > Advanced Operations > puis sélectionnez Create Custom Request.... L'Assistant Inscription de certificat apparaît.
      3. Sélectionnez Next sur l'écran d'introduction.
      4. Sur la page Sélectionner une stratégie d'inscription de certificat, sélectionnez Continuer sans stratégie d'inscription, répertorié sous Demande personnalisée, puis sélectionnez Suivant.
      5. Sur la page Demande personnalisée, vérifiez que le modèle sélectionné est (Pas de modèle) clé CNG et que le format de la demande est adapté à votre autorité

de certification. PKCS # 10 fonctionne avec l'autorité de certification Microsoft. Sélectionnez Next pour passer à la page suivante.

6. Sur la page Certificate Information, sélectionnez la liste déroulante en regard du mot Details, puis sélectionnez le bouton Properties. Le formulaire Propriétés du certificat s'affiche.
7. Ce document n'a pas pour objectif de fournir toutes les options du formulaire Propriétés de certificat. Pour plus d'informations, consultez la documentation Microsoft. Voici quelques notes et conseils sur ce formulaire.
    - Veillez à renseigner toutes les valeurs requises dans la section Nom de l'objet : de l'onglet Objet
    - Assurez-vous que la valeur fournie pour Nom commun est également fournie dans la section Autre nom :
    - Définissez Type : sur DNS, tapez l'URL dans la zone Value :, puis sélectionnez le bouton Add >
    - Si vous souhaitez utiliser plusieurs URL pour accéder à ECE, indiquez chaque autre nom dans ce même champ et sélectionnez Add > after each
    - Assurez-vous de définir la taille de clé sur l'onglet Clé privée à une valeur supérieure à 1024.
    - Si vous prévoyez d'exporter le certificat pour l'utiliser sur plusieurs serveurs Web, comme c'est souvent le cas dans une installation haute disponibilité, assurez-vous que vous sélectionnez Make private key exportable. Si vous ne le faites pas, vous ne pourrez pas exporter le certificat ultérieurement
    - Les valeurs que vous saisissez et les sélections que vous effectuez ne sont pas validées. Vous devez vous assurer de fournir toutes les informations requises, sinon l'autorité de certification ne pourra pas remplir le CSR
8. Une fois que vous avez effectué toutes les sélections, sélectionnez OK pour revenir à l'Assistant. Sélectionnez Next pour passer à la page suivante.
9. Sur la page Où voulez-vous enregistrer la demande hors connexion ?, sélectionnez un nom de fichier dans un emplacement auquel vous pouvez accéder. Pour la plupart des autorités de certification, vous devez sélectionner Base 64 comme format.
10. Fournissez le fichier à votre AC. Une fois le certificat signé et renvoyé, copiez-le sur le serveur Web et suivez les dernières étapes.
11. Dans le composant logiciel enfichable Gestion des certificats pour MMC, accédez à Certificats (Ordinateur local) > Personnel, cliquez avec le bouton droit sur Certificats, puis choisissez Toutes les tâches > Importer.... L'Assistant Importation de certificat apparaît.
12. Sélectionnez Suivant sur l'écran d'introduction.
13. Dans l'écran Fichier à importer, sélectionnez le certificat qui a été signé par votre autorité de certification, puis sélectionnez Suivant.
14. Assurez-vous de sélectionner Placer tous les certificats dans le magasin suivant.
15. Assurez-vous que Personal est sélectionné dans la zone Certificate store:, puis sélectionnez Next.
16. Vérifiez l'écran final, puis sélectionnez Terminer pour terminer l'importation.
17. Fermez la console MMC. Si vous êtes invité à enregistrer les paramètres de la console, sélectionnez No. Cela n'affecte pas l'importation du certificat.

18. Passez à l'étape majeure suivante, Lier le certificat au site Web.

Étape 1.2. Lier le certificat au site Web

⚠ Attention : vous devez vous assurer que le champ du nom d'hôte reste vide et que l'option Exiger l'indication du nom du serveur n'est pas sélectionnée dans la zone Modifier la liaison de site. Si l'un de ces paramètres est configuré, SPOG échoue lorsqu'il tente de communiquer avec ECE.

---

1. Ouvrez le Gestionnaire des services Internet (IIS) si vous ne l'avez pas déjà fait.
2. Dans le volet Connexions de gauche, accédez à Sites et sélectionnez Site Web par défaut.

   Assurez-vous de sélectionner le nom de site correct si vous choisissez d'utiliser un nom de site autre que Site Web par défaut.

3. Sélectionnez Liaisons... dans le volet Actions à droite. La zone Liaisons de sites s'affiche.
    1. S'il n'y a pas de ligne avec le Type, https et le Port, 443, complétez ce qui suit. Sinon, passez à l'étape principale suivante.
        1. Sélectionnez le bouton Ajouter..., la zone Ajouter une liaison de site apparaît.
        2. Sélectionnez https dans la liste déroulante Type :.
        3. Assurez-vous que la liste déroulante Adresse IP : affiche Toutes les adresses non attribuées et que le champ Port : est défini sur 443.
        4. Veillez à laisser le champ Nom d'hôte : vide et à désélectionner l'option Exiger l'indication du nom du serveur.
        5. Dans la liste déroulante Certificat SSL :, sélectionnez le nom du certificat qui correspond à celui que vous avez créé précédemment.
            - Si vous ne savez pas quel certificat choisir, utilisez le bouton Sélectionner... pour afficher et rechercher les certificats présents sur le serveur
            - Utilisez le bouton View... pour afficher le certificat choisi et vérifier que les détails sont corrects
        6. Cliquez sur OK pour enregistrer votre sélection.
    2. Sélectionnez la ligne qui affiche https dans la colonne Type, puis cliquez sur le bouton Modifier.... La zone Modifier la liaison de site s'affiche.
        1. Assurez-vous que la liste déroulante Adresse IP : affiche Toutes les adresses non attribuées et que le champ Port : est défini sur 443.
        2. Assurez-vous que le champ Nom d'hôte : a été laissé vide et que l'option Exiger l'indication du nom du serveur n'est pas sélectionnée.
        3. Dans la liste déroulante Certificat SSL :, sélectionnez le nom du certificat qui correspond à celui que vous avez créé précédemment.
            - Si vous ne savez pas quel certificat choisir, utilisez le bouton Sélectionner... pour afficher et rechercher les certificats présents sur le serveur
            - Utilisez le bouton View... pour afficher le certificat choisi et vérifier que les détails sont corrects
        4. Cliquez sur OK pour enregistrer votre sélection.
    3. Sélectionnez Fermer pour revenir au Gestionnaire des services Internet (IIS).
4. Fermez le Gestionnaire des services Internet.

Étape 2. Configurer l'administrateur de partition SSO

La configuration SSO de Partition Administrator permet à ECE de créer automatiquement un compte utilisateur au niveau de la partition pour tout administrateur qui ouvre le gadget ECE dans SPOG.

Remarque : vous devez configurer l'authentification unique de l'administrateur de partition même si vous ne prévoyez pas d'activer l'authentification unique de l'agent ou du superviseur.

Étape 2.1. Obtenir un certificat Active Directory (AD) et créer un magasin de clés.

Cette étape peut être nécessaire pour répondre aux récentes modifications de sécurité annoncées par Microsoft. Si la mise à jour n'est pas appliquée et que les modifications ne sont pas apportées au domaine, cela peut être ignoré.

Pour plus d'informations, consultez les détails de Microsoft KB4520412.

1. Obtenez le certificat SSL, au format Base 64, auprès de votre serveur AD que vous fournissez dans le formulaire de configuration de l'administrateur de partition. Une méthode est illustrée.
    1. Utilisez une station de travail pour télécharger et installer une copie d'OpenSSL pour Windows à partir de OpenSSL. L'édition Light est adéquate.
    2. Lancez l'invite de commandes OpenSSL.
    3. Exécutez cette commande. Remplacez le nom du serveur par le nom complet de votre contrôleur de domaine du catalogue global.
       openssl s_client -connect gcdcsrv01.example.local:3269
    4. Dans le résultat, localisez la ligne de certificat du serveur.

```
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. Copiez le résultat du début de « -----BEGIN CERTIFICATE----- » vers « -----END

CERTIFICATE----- ». Assurez-vous que les lignes BEGIN CERTIFICATE et END CERTIFICATE sont incluses.
6. Collez les informations que vous avez copiées dans un nouveau fichier texte, puis enregistrez-les sur l'ordinateur avec une extension crt.

2. Copiez le fichier de certificat sur l'un des serveurs d'applications.
3. Ouvrez une session RDP sur le serveur d'applications où vous avez copié le certificat.
4. Créez un nouveau keystore Java.
   1. Ouvrez une invite de commandes sur le serveur d'applications.
   2. Accédez au répertoire bin du kit de développement Java (JDK) ECE.
   3. Exécutez cette commande. Remplacez les valeurs comme il convient.
      keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c : \ece\pcce\mydomain.jks -storepass MyP@ssword
5. Dans les versions antérieures à la version 12.6, copiez le keystore sur le même chemin sur tous les autres serveurs d'applications de votre environnement. Avec la version 12.6, copiez le magasin de clés à un emplacement accessible à partir de la station de travail où vous configurez ECE.

Étape 2.2. Configurez ECE avec les informations d'accès LDAP (Lightweight Directory Access Protocol) AD.

1. À partir d'une station de travail ou d'un ordinateur équipé d'Internet Explorer 11, accédez à l'URL de partition Business.

   Conseil : la partition d'entreprise est également appelée partition 1. Pour la plupart des installations, la partition Business est accessible via une URL similaire à, https://ece.example.com/default.

2. Connectez-vous en tant que pa et fournissez le mot de passe pour votre système.
3. Une fois que vous êtes connecté, sélectionnez le lien Administration sur la console initiale.
4. Accédez au dossier SSO Configuration, Administration > Partition: default > Security > SSO and Provisioning.
5. Dans le volet supérieur de droite, sélectionnez l'entrée Configuration de l'administration des partitions.
6. Dans le volet inférieur de droite, entrez les valeurs de vos protocoles LDAP (Lightweight Directory Access Protocol) et AD.
   1. URL LDAP - Il est recommandé d'utiliser le nom d'un contrôleur de domaine de catalogue global (GC).
      Si vous n'utilisez pas de catalogue global, vous pouvez voir une erreur dans les journaux ApplicationServer comme suit.
      Exception dans l'authentification LDAP <@>
      javax.naming.PartialResultException : référence(s) de continuation non traitée(s) ; nom restant 'DC=example,DC=com'
      - Le port de catalogue global non sécurisé est 3268
      - Le port du catalogue global sécurisé est 3269
   2. Attribut DN : userPrincipalName doit être sélectionné.
   3. Base - Cette opération n'est pas obligatoire si vous utilisez un catalogue global. Dans

le cas contraire, vous devez fournir le format LDAP de base approprié.

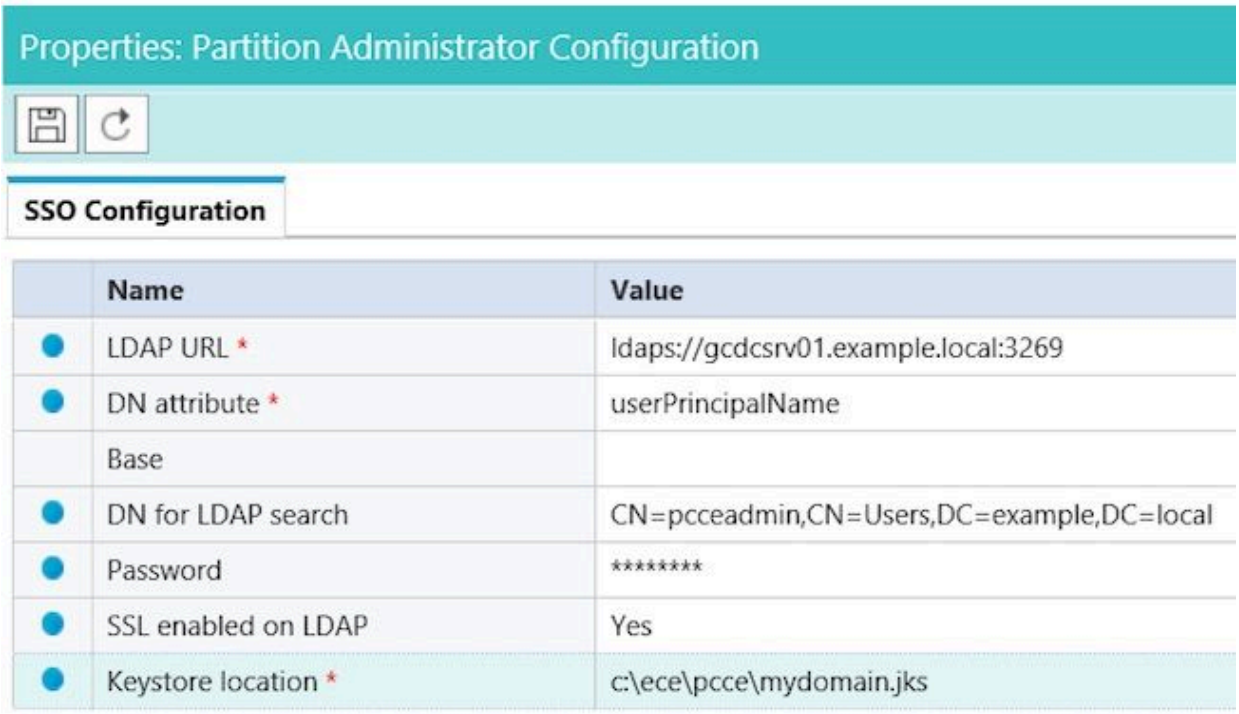
4. DN pour la recherche LDAP - À moins que votre domaine n'autorise la liaison anonyme, vous devez fournir le nom distinctif d'un utilisateur avec la possibilité de se lier à LDAP et de rechercher dans l'arborescence de l'annuaire.

Conseil : le moyen le plus simple de trouver la valeur correcte pour l'utilisateur est d'utiliser l'outil Utilisateurs et ordinateurs Active Directory. Ces étapes montrent comment rechercher cette valeur.

---

   1. Dans le menu Affichage, sélectionnez l'option Fonctionnalités avancées.
   2. Accédez à l'objet utilisateur, puis cliquez avec le bouton droit de la souris et choisissez Propriétés.
   3. Sélectionnez l'onglet Attributs.
   4. Cliquez sur le bouton Filtre, puis sélectionnez Afficher uniquement les attributs avec des valeurs.
   5. Recherchez nomDistinctName dans la liste, puis double-cliquez pour afficher la valeur.
   6. Mettez en surbrillance la valeur affichée, puis copiez-la et collez-la dans un éditeur de texte.
   7. Copiez et collez la valeur du fichier texte dans le champ DN pour recherche LDAP.
      La valeur doit être similaire à, CN=pcceadmin, CN=Users, DC=example, DC=local

5. Password : saisissez le mot de passe de l'utilisateur spécifié.
6. SSL activé sur LDAP - Ce champ peut être considéré comme obligatoire pour la plupart des clients.
7. Emplacement du magasin de clés - Il doit s'agir de l'emplacement du magasin de clés où vous avez importé le certificat SSL depuis AD. Dans l'exemple, il s'agit de c:\ece\pcce\mydomain.jks, comme indiqué dans l'image :



7. Sélectionnez l'icône de la disquette pour enregistrer les modifications.

Étape 3. Valider le fichier de configuration

Cette section est obligatoire pour toutes les installations 12.0. Pour toute version autre que 12.0, vous pouvez ignorer cette section.
Cette étape peut être requise dans deux autres scénarios, toutes versions confondues. La première est lorsque l'ECE a été installé dans une configuration haute disponibilité. La seconde, et plus courante, est lorsque le nom d'hôte du serveur Web ne correspond pas au nom que vous utilisez pour accéder à ECE. Par exemple, si vous installez le serveur Web ECE sur un serveur dont le nom d'hôte est UCSVRECEWEB.example.com, mais que les utilisateurs accèdent aux pages Web ECE avec l'URL chat.example.com, cette section doit être remplie. Si le nom d'hôte du serveur et l'URL avec laquelle vous accédez à ECE sont identiques et si vous avez installé la version 12.5 ou ultérieure, vous pouvez ignorer cette étape et compléter la section.

Remplacez {ECE_HOME} par l'emplacement physique où vous avez installé ECE. Par exemple, si vous avez installé ECE sur C:\Cisco, remplacez {ECE_HOME} par C:\Cisco dans chaque emplacement.

Conseil : utilisez un éditeur de texte tel que Notepad++ au lieu de Bloc-notes ou Wordpad car ceux-ci n'interprètent pas correctement les fins de ligne.

---

1. Ouvrir une session Bureau à distance sur tous les serveurs Web ECE de votre déploiement.
2. Accédez à ce chemin d'accès, {ECE_HOME}\eService\templates\finesse\gadget\spog.
3. Localisez le fichier spog_config.jsfile et effectuez une copie de sauvegarde dans un emplacement sûr.
4. Ouvrez le fichier spog_config.jsfile actuel dans un éditeur de texte.
5. Localisez ces deux lignes et mettez-les à jour en fonction de votre déploiement.

Le protocole web_server_protocol doit être https, mis à jour si nécessaire.
Mettez à jour le nom_serveur_web pour qu'il corresponde au nom complet que vous avez attribué pour accéder à ECE. Exemple : ece.example.com
    - var web_server_protocol = "https";
    - var web_server_name = "ece.example.com";
6. Enregistrez les modifications.
7. Répétez l'opération sur tous les autres serveurs Web de votre déploiement.

Étape 4. Ajouter ECE à l'inventaire PCCE

À partir de la version 12.0, PCCE dispose de 3 options de déploiement différentes : 2 000 agents (2 000 agents), 4 000 agents (4 000 agents) et 12000 agents (12 000 agents). Ces trois options de déploiement peuvent être divisées en deux groupes : l'agent 2K et l'agent 4K/12K. Ils sont séparés de cette façon, car il y a plusieurs différences fondamentales dans leur apparence dans SPOG. Une comparaison de très haut niveau des deux méthodes fait suite à ce paragraphe. Ce document ne donne pas d'étapes spécifiques pour ajouter un composant à l'inventaire. Veuillez consulter les liens à la fin de ce document pour plus de détails sur ce processus. Cette section couvre des détails spécifiques qui doivent être vérifiés lorsque vous ajoutez ECE à PCCE. Ce document suppose également que votre installation PCCE est terminée et que vous êtes en mesure d'accéder à d'autres aspects de la solution et de les configurer.

- Déploiement de 2 000 agents
    - La configuration initiale des composants PCCE s'effectue entièrement via l'administration CCE et est automatisée
    - Les nouveaux composants sont ajoutés dans la page d'inventaire via une fenêtre contextuelle dans laquelle vous entrez les détails, tels que l'adresse IP ou le nom d'hôte, ainsi que les informations d'identification ou la configuration spécifique du composant
- Déploiement d'agents 4 000 et 12 000
    - La plupart des configurations initiales reflètent les étapes utilisées pour UCCE
    - Les composants sont ajoutés via un fichier de valeurs séparées par des virgules (CSV) que vous téléchargez à partir de CCE Administration, que vous remplissez en fonction de votre installation spécifique, puis que vous téléchargez
    - Le déploiement initial nécessite l'inclusion de certains composants spécifiques dans le premier fichier CSV
    - Les composants qui n'ont pas été ajoutés lors de la configuration initiale du système le sont via des fichiers CSV contenant les informations requises

Étape 4.1. Télécharger le certificat du serveur Web ECE dans le magasin de clés Java

1. Si des certificats auto-signés sont utilisés
    1. Ouvrez une connexion Bureau à distance au serveur de données d'administration (ADS) principal côté A.
    2. Ouvrez Internet Explorer 11 en tant qu'administrateur et accédez à la partition d'entreprise ECE.
    3. Sélectionnez l'icône d'un cadenas à droite de la barre d'URL, puis choisissez Afficher

les certificats.
4. Dans la zone Certificat, sélectionnez l'onglet Détails.
5. Sélectionnez Copier dans un fichier... en bas de l'onglet.
6. Dans l'Assistant Exportation de certificat, sélectionnez Suivant jusqu'à ce que vous atteigniez la page Format de fichier d'exportation. Veillez à sélectionner le format X.509 (.CER) codé en base 64.
7. Enregistrez le certificat à un emplacement tel que c:\Temp\certificates sur le serveur ADS pour terminer l'exportation.
8. Copiez le certificat sur tous les autres serveurs ADS.
9. Ouvrez une invite de commandes d'administration.
10. Accédez au répertoire d'accueil Java, puis au répertoire bin. Le répertoire d'accueil Java est accessible de la manière suivante. cd %JAVA_HOME%\bin
11. Sauvegardez le fichier cacerts actuel. Copiez le fichier cacerts de %JAVA_HOME%\lib\security vers un autre emplacement.
12. Exécutez cette commande pour importer le certificat que vous avez enregistré précédemment. Si le mot de passe de votre keystore n'est pas « changeit », mettez à jour la commande pour qu'elle corresponde à votre installation.
keytool -keystore ../lib/security/cacerts -storepass changeit -import -alias <FQDN du serveur ECE> -file <Emplacement où vous avez enregistré le certificat>
13. Redémarrez le serveur ADS.
14. Répétez les étapes 8 à 12 sur les autres serveurs ADS.

2. Si des certificats signés par une autorité de certification sont utilisés
    1. Obtenez le certificat racine et le certificat intermédiaire au format DER/PEM et copiez-les à un emplacement tel que C:\Temp\certificates sur tous les serveurs ADS.

     Remarque : contactez votre administrateur CA pour obtenir ces certificats.

    2. Ouvrez une connexion Bureau à distance au serveur principal, côté A.
    3. Ouvrez une invite de commandes d'administration.
    4. Accédez au répertoire d'accueil Java, puis au répertoire bin. Le répertoire d'accueil Java est accessible de la manière suivante. cd %JAVA_HOME%\bin
    5. Sauvegardez le fichier cacerts actuel. Copiez le fichier cacerts de %JAVA_HOME%\lib\security vers un autre emplacement.
    6. Exécutez cette commande pour importer le certificat que vous avez enregistré précédemment. Si le mot de passe de votre keystore n'est pas « changeit », mettez à jour la commande pour qu'elle corresponde à votre installation.
    keytool -keystore ../lib/security/cacerts -storepass changeit -trustcacerts -import -alias <Nom de l'autorité de certification racine> -file <Emplacement où vous avez enregistré le certificat racine>
    7. Répétez l'étape 6 et importez le certificat intermédiaire, le cas échéant.
    8. Redémarrez le serveur ADS.
    9. Répétez les étapes 2 à 12 sur tous les autres serveurs ADS.

Étape 4.2. Ajouter le serveur de données ECE à l'inventaire

- Bien que le serveur de données doive exister dans l'inventaire du système, aucune

communication directe n'est établie entre le serveur PCCE ADS et le serveur de données
- Lorsqu'ECE est déployé dans le déploiement de 1 500 agents, le serveur de données est le serveur de services
- Lorsque l'ECE est installé dans une configuration haute disponibilité, ajoutez uniquement le serveur de services côté A

Étape 4.3. Ajouter le serveur Web ECE à l'inventaire

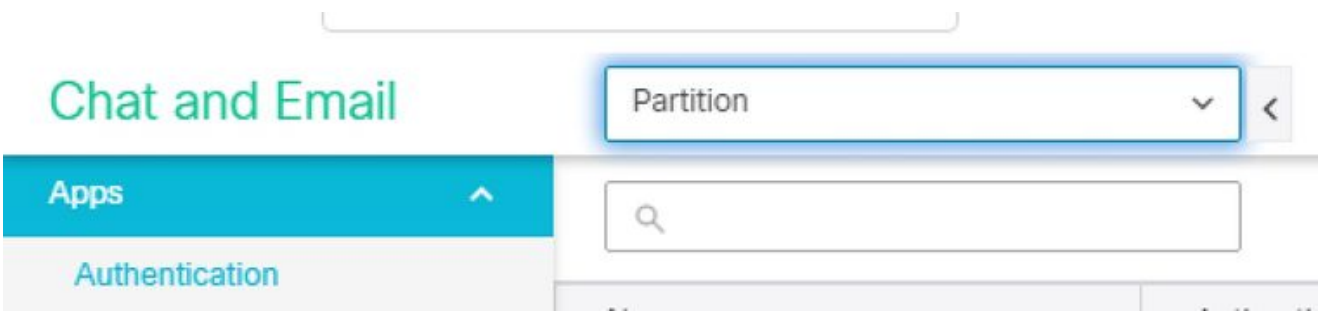
- Assurez-vous d'ajouter le serveur Web avec le nom complet
  - Ce nom doit correspondre soit au nom commun figurant dans le certificat ECE, soit figurer dans la liste des noms de remplacement des sujets (SAN)
  - Vous ne devez pas utiliser uniquement le nom d'hôte ou l'adresse IP
- Le nom d'utilisateur et le mot de passe pour ECE doivent être les identifiants de connexion pa
- Vérifiez que l'instance d'application est correcte
  - Le nom de l'instance d'application est sensible à la casse
  - Pour les déploiements PCCE de l'agent 2000, l'instance d'application est multicanal
  - Pour les déploiements d'agent PCCE 4000/12000, l'instance d'application contient le site et le périphérique définis dans le nom
- Lorsqu'ECE est installé avec plusieurs serveurs Web, par exemple dans le déploiement 1500 Agent ou dans un déploiement 400 Agent HA, vous pouvez utiliser l'URL qui pointe vers votre équilibreur de charge ou l'URL qui pointe vers chaque serveur Web individuel comme nom complet du serveur Web. La meilleure pratique consiste à utiliser un équilibreur de charge.
- Si vous disposez de plusieurs déploiements ECE ou si vous choisissez d'ajouter chaque serveur Web individuel dans le déploiement avec plusieurs déploiements, vous devez choisir le serveur Web approprié lorsque vous ouvrez le gadget ECE dans SPOG.

Étape 5. Intégrer ECE et PCCE

1. Connectez-vous à CCE Administration en tant qu'administrateur.
2. Sélectionnez la carte E-mail et discussion, puis le lien E-mail et discussion comme illustré dans l'image.



3. Vérifiez le serveur actuellement sélectionné dans la liste déroulante Device Name. Si vous avez ajouté les deux serveurs Web dans une installation haute disponibilité, vous pouvez choisir l'un ou l'autre. Si vous ajoutez ultérieurement un deuxième déploiement ECE à votre système, veillez à sélectionner le serveur approprié avant de continuer.
4. Dans la liste déroulante en regard de Chat and Email, sélectionnez Partition ou Global comme indiqué dans l'image.



5. Dans le menu supérieur, sélectionnez Integration, puis sélectionnez la flèche en regard de Unified CCE et sélectionnez le second Unified CCE comme illustré dans l'image.



6. Renseignez les valeurs de l'onglet AWDB Details pour votre installation, puis sélectionnez le bouton Save.
7. Sélectionnez l'onglet Configuration et complétez ceci comme suit.
    1. Sélectionnez la liste déroulante en regard de Instance d'application et sélectionnez l'instance d'application créée pour ECE.

> Remarque : il ne doit pas s'agir de l'instance d'application qui commence par UQ.

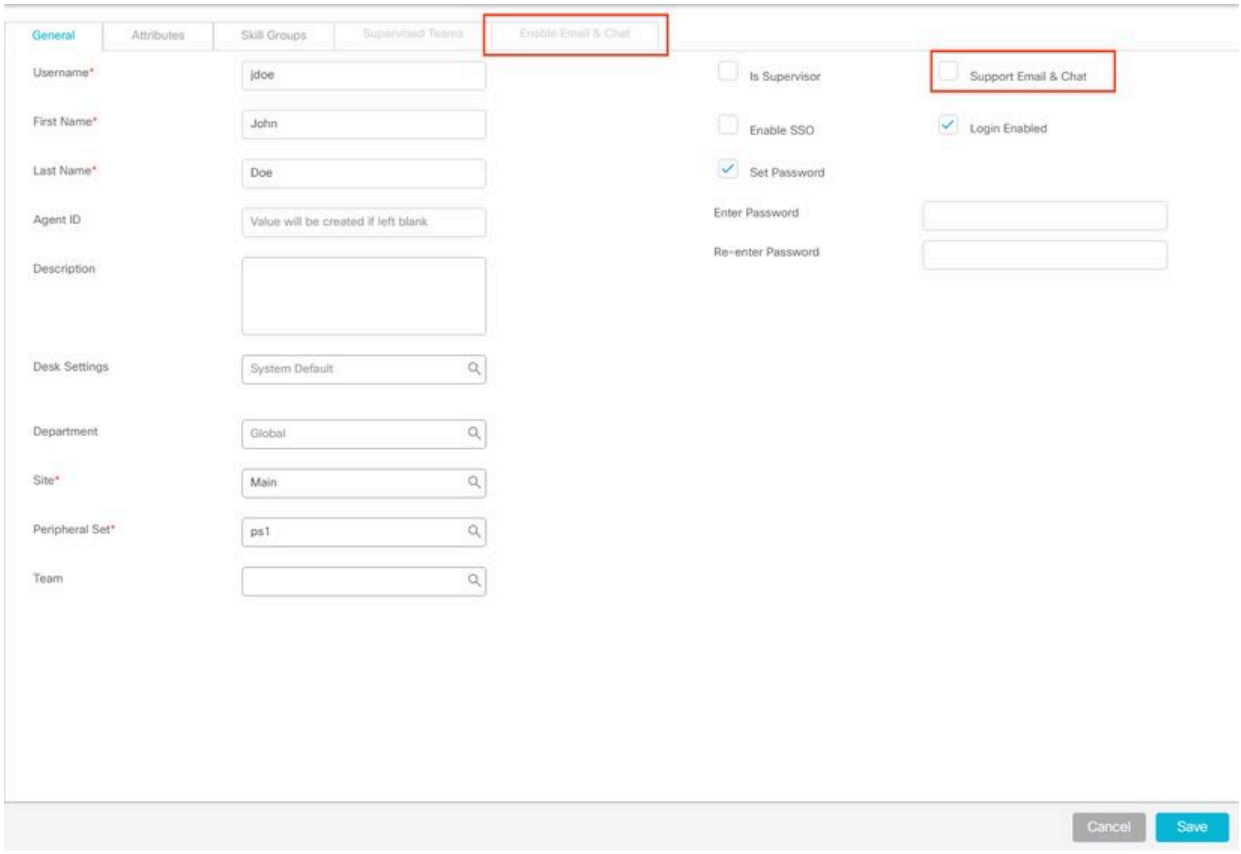


    2. Sélectionnez le cercle vert avec le bouton blanc plus signe sélectionnez l'agent PG.
        1. Sélectionnez la PG agent (ou les PG agent s'il y en a plusieurs).
        2. Sélectionnez Enregistrer une fois que vous avez ajouté toutes les PG d'agent.

> Avertissement : lorsque vous sélectionnez Enregistrer, le système est connecté en permanence à PCCE et ne peut pas être annulé. Si des erreurs se sont produites dans cette section, vous devez désinstaller complètement ECE et supprimer toutes les bases de données, puis installer ECE comme s'il s'agissait d'une nouvelle installation.

Étape 6. Valider l'intégration ECE

1. Dans CCE Administration, vérifiez qu'aucune alerte n'apparaît dans la barre d'état supérieure. S'il y a des alertes, sélectionnez le mot Alertes et consultez la page Inventaire pour vous assurer qu'aucune des alertes ne concerne les serveurs de la CEE.
2. Sélectionnez Users, puis Agents dans la barre de navigation de gauche.
3. Sélectionnez un agent dans la liste et vérifiez-le.
    1. Une nouvelle case à cocher Support Email & Chat s'affiche désormais dans l'onglet General.
    2. Vous voyez maintenant un nouvel onglet intitulé Enable Email & Chat comme indiqué dans l'image.



4. Activer un agent de test pour ECE.
    1. Activez la case à cocher Support Email & Chat et notez que l'onglet Enable Email & Chat peut désormais être sélectionné.
    2. Sélectionnez l'onglet Enable Email & Chat et indiquez une valeur dans le champ Screen Name.
    3. Sélectionnez Enregistrer pour mettre à jour l'utilisateur.
    4. Vous recevez un message de réussite.
5. Vérifier que l'ECE a été mis à jour.
    1. Cliquez sur le bouton de navigation Vue d'ensemble, puis sélectionnez la carte E-mail et Chat et le lien.
    2. Dans le menu déroulant en regard de Chat and Email, sélectionnez le nom qui correspond au service de l'agent.

> Remarque : Le service dans ECE contient tous les objets appartenant au service global dans PCCE. Le nom de service Service est donc une valeur réservée.

1. Dans le menu supérieur, sélectionnez Gestion des utilisateurs, puis Utilisateurs dans le menu sous Discussion et e-mail.
2. Vérifiez que vous voyez le nouvel agent dans la liste.

Dépannage

Il est recommandé de télécharger plusieurs outils et de les conserver sur les serveurs ECE. Cela facilite considérablement le dépannage et la maintenance de la solution au fil du temps.

- Un éditeur de texte tel que Bloc-notes++
- Un outil d'archivage tel que 7-Zip
- L'un des nombreux programmes Tail pour Windows
  En voici quelques exemples :
  - Queue De Barre
  - Queue pour Win32

Pour résoudre les problèmes d'intégration, vous devez d'abord connaître certains fichiers journaux clés et l'emplacement de chacun d'eux.

1. Noms et emplacements des fichiers sur la CEE

   Il existe de nombreux journaux sur le système ECE, ce sont ceux qui sont les plus utiles lorsque vous essayez de résoudre un problème d'intégration.

Fichier journal	Serveur	Convention de nom	Description
Serveur d'applications	C/A	eg_log_{HOSTNAME}_ApplicationServer.log	Journaux du serveur Wildfly
Affectation d'agent externe	C/S	eg_log_{HOSTNAME}_EAAS-process.log	Interaction avec la PG MR
Messagerie d'agent externe	C/S	eg_log_{HOSTNAME}_EAMS-process.log	Interaction avec le serveur CTI
Journaux racine	C/A/M/S	egpl_root_{HOSTNAME}.log	Journaux inter-processus, HazelCast, erreurs générales
État du composant	C/A/M/S	eg_log_{HOSTNAME}_component-status.log	Démarrage du processus et fin de la copie du fichier
Lanceur de processus	C/A/M/S	eg_log_{HOSTNAME}_ProcessLauncher.log	Journaux généraux pour le démarrage des services et des processus
Gestionnaire	C/S	eg_log_{HOSTNAME}_DSMController.log	Journaux indiquant le

de services distribués			démarrage et l'arrêt du processus sur le serveur de services

Clé du serveur :

- C = Serveur colocalisé
- A = Serveur d'applications
- S = Serveur de services
- M = Serveur de messagerie

La plupart des fichiers journaux ont également deux autres journaux qui leur sont associés.

- eg_log_{SERVERNAME}_{PROCESS}.log - Journal du processus principal
- eg_log_dal_connpool_{SERVERNAME}_{PROCESS}.log - Utilisation du pool de connexions
- eg_log_query_timeout_{SERVERNAME}_{PROCESS}.log - Mis à jour lorsqu'une requête échoue en raison d'un délai d'attente

2. Noms et emplacements des fichiers sur PCCE

Les journaux PCCE pour les problèmes d'intégration sont tous situés sur le côté-A ADS. Voici les journaux qui sont les plus importants lorsque vous dépannez des problèmes d'intégration. Chacun de ces éléments se trouve dans, C:\icm\tomcat\logs.

Fichier journal	Convention de nom	Description
CCBU	CCBU.{AAAA}-{MM}-{JJ}T{hh}-{mm}-{ss}.{msec}.startup.log	Journal principal pour CCE Admin et toutes les applications Web associées
Erreur CCBU	Erreur.{AAAA}-{MM}-{JJ}T{hh}-{mm}-{ss}.{msec}.startup.log	Erreurs détectées par l'administrateur CCE et les applications Web associées
Catalina	catalina.{AAAA}-{MM}-{JJ}.log	Journal natif Tomcat, affiche les erreurs de certificat
stdout Tomcat	tomcat9-stdout.{AAAA}-{MM}-{JJ}.log	Messages de journal sortants standard de Tomcat
souchet Tomcat	tomcat9-stderr.{AAAA}-{MM}-{JJ}.log	Messages du journal d'erreurs standard de Tomcat

Parmi ces journaux, les trois premiers sont les plus fréquemment demandés et examinés.

Suivez ces étapes pour définir les niveaux de suivi et collecter les journaux requis.

3. Configuration du niveau de suivi

Cette section ne s'applique qu'à l'ECE. Le niveau de trace des journaux requis de PCCE est défini par Cisco et ne peut pas être modifié.

1. À partir d'une station de travail ou d'un ordinateur équipé d'Internet Explorer 11, accédez à l'URL de partition système.

   Conseil : la partition système est également appelée Partition 0. Pour la plupart des installations, la partition système est accessible via une URL similaire à https://ece.example.com/system

2. Connectez-vous en tant que sa et indiquez le mot de passe de votre système.
3. Une fois que vous êtes connecté, sélectionnez le lien System sur la console initiale.
4. Dans la page Système, développez Système > Ressources partagées > Journaliseur > Processus.
5. Dans le volet supérieur droit, recherchez le processus dont vous souhaitez modifier le niveau de suivi et sélectionnez-le.
   Remarque : dans un système haute disponibilité et dans un système comportant plusieurs serveurs d'applications, les processus sont répertoriés plusieurs fois. Pour vous assurer que vous capturez les données, définissez le niveau de suivi pour tous les serveurs qui contiennent le processus.
6. Dans le volet inférieur droit, sélectionnez la liste déroulante Niveau de suivi maximal et sélectionnez la valeur appropriée.
   L'ECE définit 8 niveaux à l'état de traces. Les 4 éléments de cette liste sont ceux qui sont le plus souvent utilisés.
   - 2 - Erreur - Niveau de suivi par défaut pour les processus
   - 4 - Info - Niveau de suivi généralement utilisé pour la résolution des problèmes
   - 6 - Dbquery - Souvent utile pour diagnostiquer les problèmes au début de la configuration ou les problèmes plus complexes
   - 7 - Débogage - Sortie très détaillée, uniquement requise dans les problèmes les plus complexes

   Remarque : ne laissez aucun processus à 6 - Dbquery ou supérieur pour une durée prolongée, et généralement uniquement avec les conseils du TAC.

   Conserver le niveau de suivi de la plupart des processus, 2-Erreur. Si vous sélectionnez le niveau 7 ou 8, vous devez également sélectionner une durée maximale. Lorsque la durée maximale est atteinte, le niveau de suivi revient au dernier niveau défini.
   Une fois le système configuré, remplacez ces quatre processus par le niveau de suivi 4.

   - processus EAAS
   - procédé EAMS

- procédé dx
- procédé rx

7. Sélectionnez l'icône d'enregistrement pour définir le nouveau niveau de suivi.

4. Collecte des fichiers journaux

1. Ouvrez une session Bureau à distance sur le serveur sur lequel les journaux de processus sont nécessaires.
2. Accédez à l'emplacement du fichier journal.
    1. Serveurs ECE

       Les journaux sont écrits comme suit.

       - Par défaut, les journaux sont des fichiers écrits d'une taille maximale de 5 Mo
       - Lorsqu'un fichier journal atteint le maximum configuré, il est renommé au format {LOGNAME}.log.{#}
       - L'ECE conserve les 49 fichiers journaux précédents ainsi que le fichier actuel
       - Le journal actuel se termine toujours par.log et aucun numéro après
       - Les journaux ne sont ni archivés ni compressés
       - La plupart des journaux ont une structure commune
       - Les fichiers journaux utilisent **<@>** pour séparer les sections
       - Les journaux sont toujours écrits en GMT+0000

       Les journaux ECE sont situés à différents endroits en fonction de l'installation spécifique.

        1. 400 déploiements d'agents
            1. Monoface
                - Serveur : serveur colocalisé
                - Emplacement : {ECE_HOME}\eService_RT\logs
            2. Haute disponibilité
                - Serveurs : deux serveurs colocalisés
                - Emplacement : {ECE_HOME}\eService\logs
                - Le répertoire créé pour le partage DFS (Distributed File System) contient uniquement des journaux d'installation et de mise à niveau.
                - Seul le serveur qui possède le rôle Distributed Systems Manager (DSM) écrit des journaux pour les composants faisant partie du rôle Services
                    - Le propriétaire du rôle GSD se trouve dans l'onglet Processus du Gestionnaire des tâches de Windows. Ce serveur comporte de 10 à 15 processus Java qui ne se trouvent pas sur le serveur secondaire.
                    - Les composants de DSM sont les suivants : EAAS, EAMS,

Retriever, Dispatcher, Workflow, etc.

2. 1 500 déploiements d'agents
    - Journaux situés sur le serveur qui héberge le rôle
    - Emplacement : {ECE_HOME}\eService\logs
    - À l'exception du serveur de services, tous les serveurs fonctionnent et écrivent des journaux pour tous les processus associés au composant
    - Dans un déploiement à haute disponibilité, le serveur de services fonctionne en configuration active/veille
    - Seul le serveur qui possède le rôle Distributed Systems Manager (DSM) écrit les journaux
    - Le propriétaire du rôle GSD peut être identifié par le nombre de processus affichés dans le Gestionnaire des tâches de Windows. Entre 10 et 15 processus Java s'exécutent sur le serveur principal et seulement 4 processus Java sur le serveur secondaire

2. Serveurs PCCE
    - Les journaux requis de PCCE sont disponibles à l'adresse : C:\icm\tomcat\logs
    - Les journaux Tomcat ne sont pas restaurés ou archivés
    - Les journaux sont écrits en heure du serveur local

3. Collecter tous les journaux créés ou modifiés après l'observation du problème.
   Une explication complète des journaux et des problèmes observés dépasse le cadre de ce document. Voici quelques problèmes courants, ce qu'il faut revoir et quelques solutions possibles.
    - Problèmes liés aux certificats
        - Certificat non importé
            - Comportement : Lorsque vous essayez d'ouvrir le gadget ECE dans SPOG, vous voyez l'erreur, "Une erreur s'est produite lors du chargement de la page. Veuillez contacter l'administrateur."
            - Vérifier : la connexion Catalina sur PCCE pour les erreurs similaires à celles-ci
              javax.net.ssl.SSLHandshakeException : sun.security.validator.ValidatorException : échec de la création du chemin PKIX : sun.security.provider.certpath.SunCertPathBuilderException : impossible de trouver un chemin de certification valide vers la cible demandée
            - Résolution : assurez-vous que vous avez importé le certificat de serveur Web ECE ou les certificats CA appropriés dans le keystore sur l'ADS
        - Non-concordance du certificat
            - Comportement : lorsque vous tentez d'ouvrir le gadget ECE dans SPOG, une erreur s'affiche, indiquant que le nom commun du certificat ou le nom secondaire de l'objet ne correspond pas au nom configuré.
            - Vérifier : valider le certificat SSL
            - Résolution : assurez-vous que le champ Nom commun de l'objet ou

l'un des champs DNS de l'autre nom de l'objet contient le nom complet que vous avez entré dans SPOG comme nom de serveur Web.

- Problèmes système
  - Service non démarré
    - Comportement : lorsque vous tentez d'ouvrir le gadget ECE dans SPOG, l'erreur suivante s'affiche : « La page Web de https://{url} est peut-être temporairement inactive ou elle a été déplacée définitivement vers une nouvelle adresse. »
    - Vérifiez : vérifiez que le service Windows - Service Cisco a été démarré sur tous les serveurs ECE, à l'exception du serveur Web. Recherchez les erreurs dans les journaux racine du serveur d'applications
    - Résolution : Démarrez le service Cisco sur tous les services ECE.
- Problème de configuration
  - Configuration LDAP
    - Comportement : Lorsque vous essayez d'ouvrir le gadget ECE dans SPOG, vous voyez l'erreur, "Une erreur s'est produite lors du chargement de la page. Veuillez contacter l'administrateur."
    - Check : augmentez le niveau de suivi du serveur d'applications au niveau 7 - Debug, puis tentez à nouveau de vous connecter et consultez le journal du serveur d'applications. Recherchez le mot LDAP.
    - Résolution : validez la configuration LDAP pour l'authentification unique de l'administrateur de partition afin de vous assurer qu'elle est correcte.

Informations connexes

Il s'agit des documents clés que vous devez examiner en détail avant de commencer une installation ou une intégration ECE. Il ne s'agit pas d'une liste exhaustive des documents de la CEE.

⚠ Attention : La plupart des documents de la CEE ont deux versions. Veuillez vous assurer que vous téléchargez et utilisez les versions qui sont destinées à PCCE. Le titre du document est pour Packaged Contact Center Enterprise ou (Pour PCCE) ou (Pour UCCE et PCCE) après le numéro de version.

Assurez-vous de consulter la page de démarrage de la documentation de Cisco Enterprise Chat and Email pour toute mise à jour avant toute installation, mise à niveau ou intégration.

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

- 12.0

    - Guide d'installation et de configuration de la messagerie instantanée et du courrier électronique
    - Guide de mise à niveau Enterprise Chat and Email
    - Guide de l'administrateur de la messagerie et du chat d'entreprise
- 12.5
    - Guide d'installation et de configuration de la messagerie instantanée et du courrier électronique
    - Guide de mise à niveau Enterprise Chat and Email
    - Guide de l'administrateur de la messagerie et du chat d'entreprise

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.