

Intégrer la CEE au PCCE dans les versions 12.0 et ultérieures

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Terminologie](#)

[Étapes préalables](#)

[Étapes d'intégration](#)

[Étape 1. Configurer les certificats SSL](#)

[Étape 1.1. Générer un certificat](#)

[Étape 1.2. Lier un certificat au site Web](#)

[Étape 2. Configurer SSO Administrateur de partition](#)

[Étape 2.1. Obtenir le 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 CEE à l'inventaire PCCE](#)

[Étape 4.1. Télécharger le certificat de serveur Web CEE dans le magasin de clés Java](#)

[Étape 4.2. Ajouter le serveur de données CEE à l'inventaire](#)

[Étape 4.3. Ajouter le serveur Web de la CEE à l'inventaire](#)

[Étape 5. Intégrer la CEE au PCCE](#)

[Étape 6. Valider l'intégration CEE](#)

[Dépannage](#)

[Noms et lieux des fichiers sur la CEE](#)

[Noms et emplacements des fichiers sur PCCE](#)

[Configuration du niveau de suivi](#)

[Collecte de fichiers journaux](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes à suivre pour intégrer Enterprise Chat and Email (ECE) à Packaged Contact Center Enterprise (PCCE) dans les versions 12.0 et ultérieures

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

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

- ECE 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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

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

Terminologie

Tout au long de ce document, ces termes sont utilisés.

- Conversation et messagerie électronique d'entreprise (ECE) - ECE est un produit qui permet aux demandes de messagerie électronique et de discussion d'être acheminées 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 PCCE Administration est fait dans la version 12.0 et ultérieure. SPOG est une réécriture complète de l'outil d'administration CCE utilisé dans les versions antérieures à 12.0.
- Autorité de certification (AC) : entité qui émet des certificats numériques conformément à un modèle d'infrastructure à clé publique (PKI). Vous pouvez rencontrer deux types d'AC. CA publique - Une CA publique est une CA dont les certificats racine et intermédiaire sont inclus dans la plupart des navigateurs et des systèmes d'exploitation. Parmi les CA publiques les plus courantes figurent IdenTrust, DigiCert, GoDaddy et GlobalSign. Autorité de certification privée : une autorité de certification privée existe au sein d'une société. Certaines autorités de certification privées sont signées par des autorités de certification publiques, mais la plupart du temps, il s'agit d'autorités de certification autonomes et les certificats qu'elles délivrent 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 d'autorité de certification racine : le serveur d'autorité de certification racine signe son propre certificat. Dans le déploiement d'ICP multicouche 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 appelé autorité de certification intermédiaire. Certaines entreprises choisissent d'utiliser uniquement une autorité de certification à 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 CA intermédiaire - Le serveur CA intermédiaire ou émetteur émet des certificats destinés à une entité autre qu'un autre serveur CA.

- Microsoft Management Console (MMC) : application incluse avec Microsoft Windows qui permet le chargement de 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 sont inclus dans Windows. Parmi les exemples suivants, citons les certificats, le gestionnaire de périphériques, la gestion des disques, l'observateur d'événements et les services.
- Équilibreur de charge réseau (NLB) : périphérique ou application présentant plusieurs ressources physiques aux utilisateurs finaux avec un nom physique commun. Les NLB sont très courants avec les applications et services Web. Les NLB peuvent être mis en oeuvre de plusieurs manières. Lorsqu'elle est utilisée avec ECE, la NLB doit être configurée de manière à garantir que les sessions utilisateur retournent au même serveur Web principal physique à l'aide d'un cookie-insert ou d'une méthode équivalente. C'est ce qu'on appelle une session collante avec cookie-insert. La session rémanente désigne simplement 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 où la session de l'utilisateur a été affectée. Le transfert SSL n'autorise pas l'insertion de cookies car la session HTTP est physiquement chiffrée en permanence. La plupart des NLB prennent en charge les sessions rémanentes avec le passage SSL en utilisant des tables de clé qui surveillent la partie serveur et client de la configuration de la session et stockent les valeurs uniques dans une table. Lorsque la requête suivante qui correspond à ces valeurs est présentée à la NLB, 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 utilisateur final donnée. La première est entre le périphérique de l'utilisateur final et l'adresse IP virtuelle (VIP) configurée sur le NLB pour le site Web. La seconde se situe entre l'adresse IP dorsale du NLB et le serveur Web physique sur lequel la session de l'utilisateur est affectée. Le délestage SSL prend en charge les cookies-insert car le flux HTTP est entièrement déchiffré alors que sur le NLB, des cookies HTTP supplémentaires peuvent être insérés et l'inspection de session peut être effectuée. Le délestage SSL est souvent utilisé lorsque l'application Web ne nécessite pas SSL, mais est fait pour la sécurité. Les versions actuelles de la CEE ne prennent pas en charge l'accès à l'application dans une session non SSL.

Étapes préalables

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

- Niveau de correctif PCCE minimum Version 12.0(1) - ES37Version 12.5(1) - Pas de minimum

actuel pour la fonctionnalité de base

La fonction d'analyse WebEx Experience Management (WXM) nécessite ES7

- Niveau de raccordement CEE minimum Il est recommandé que la CEE mette à disposition les toutes dernières offres spéciales d'ingénierie (ES).Version 12.0(1) - ES3 + ES3_ET1aVersion 12.5(1) - Pas de minimum actuel pour la fonctionnalité de base

La fonction Analyseur WXM nécessite ES1

- Éléments de configuration Assurez-vous d'associer les domaines de routage de support (MRD) ECE_Email, ECE_Chat et ECE_Outbound Media Routing Domains (ECE_Email, ECE_Chat et ECE_Outbound Media Routing Domains) à l'instance d'application appropriée.Pour le modèle de déploiement de l'agent PCCE 2000, l'instance d'application est MultiChannel.Pour le modèle de déploiement de l'agent PCCE 4000/12000, l'instance d'application prend la forme {site}_{périphérique_set}_{application_instance}. Si vous avez installé PCCE avec le nom du site comme Principal, le périphérique défini comme PS1 et l'instance d'application comme Multichannel, alors le nom de l'instance d'application est Main_PS1_Multichannel.**Note:** Le nom de l'instance d'application est sensible à la casse. Assurez-vous de taper correctement le nom lorsque vous ajoutez le serveur Web CEE 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 ni dans le même document. Reportez-vous aux liens figurant à la fin de ce document à pour plus de détails.

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 l'autorité de certification, il y a moins d'étapes pour créer le certificat au départ, mais lorsque le certificat doit être remplacé, vous devez vous rappeler de télécharger le nouveau certificat dans les keystores Java sur tous les serveurs de données d'administration PCCE. Si vous utilisez un certificat signé par l'autorité de certification, vous n'avez qu'à télécharger les certificats racine et, le cas échéant, intermédiaires dans les keystores.

Si votre déploiement comporte plusieurs serveurs Web, vous devez revoir ces directives. Les étapes spécifiques requises pour configurer un équilibreur de charge réseau ne sont pas couvertes par ce document. Veuillez contacter votre fournisseur d'équilibreur de charge pour obtenir de l'aide si nécessaire.

Bien qu'il ne soit pas nécessaire, un équilibreur de charge simplifie considérablement la mise en oeuvre

L'accès à l'application CEE 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 transfert SSL ou déchargement SSL

Si vous choisissez le transfert SSL, ceci doit être fait : Vous devez effectuer toutes les opérations

de certificat à partir d'un serveur

Une fois le certificat correctement configuré, vous devez exporter le certificat et vous assurer que la clé privée est incluse dans un fichier d'échange d'informations personnelles (PFX)

Vous devez copier le fichier PFX sur tous les autres serveurs Web du déploiement, puis importer le certificat dans IIS

Si le téléchargement SSL est choisi, chaque serveur Web peut être configuré avec son propre certificat SSL individuel

Note: Si vous avez plusieurs serveurs Web et que vous choisissez le transfert SSL sur votre serveur Web, ou si vous souhaitez avoir un certificat commun sur tous les serveurs, vous devez choisir un serveur Web sur lequel effectuer l'étape 1, puis importer le certificat sur tous les autres serveurs Web.

Si vous choisissez le téléchargement 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 Administration IIS.
2. Sélectionnez le nom du serveur dans l'arborescence Connexions à gauche.
3. Recherchez **les certificats de serveur** dans le volet central et double-cliquez pour l'ouvrir.
4. Sélectionnez **Créer un certificat auto-signé...** dans le volet Actions à 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** : de la boîte de dialogue. Ce nom indique comment le certificat apparaît dans le processus de sélection à l'étape principale suivante. Ce nom n'a pas besoin de correspondre au nom commun du certificat et n'affecte pas la manière dont le certificat apparaît à l'utilisateur final.
6. Assurez-vous que **Personal** est sélectionné dans le **magasin de certificats Sélectionner un nouveau certificat** : dans la liste déroulante.
7. Sélectionnez **OK** pour créer le certificat.
8. Passez à l'étape principale suivante, **Lier le certificat au site Web**.

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

Les certificats signés par l'autorité de certification exigent que vous génériez 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 CA requis sont retournés et le CSR rempli. Vous pouvez choisir de le faire via l'administration IIS ou via la console de gestion Microsoft (MMC). La méthode d'administration IIS est beaucoup plus facile, sans connaissance particulière requise, mais vous permet seulement de configurer les champs inclus dans l'attribut Subject du certificat et de modifier la longueur de bit. MMC nécessite des étapes

supplémentaires et vous devez posséder une connaissance approfondie de tous les champs requis dans un CSR valide. Il est fortement recommandé d'utiliser MMC uniquement si vous avez une expérience modérée à experte en matière de création et de gestion de certificats. Si votre déploiement nécessite que ECE soit accessible par plusieurs noms complets ou si vous devez modifier une partie du certificat, à l'exception de l'objet et de la longueur de bit, vous devez utiliser la méthode MMC.

1. Via l'administration IIS Utilisez ces étapes pour générer une demande de signature de certificat (CSR) via le Gestionnaire IIS. Accédez à Administration IIS. Sélectionnez le nom du serveur dans l'arborescence Connexions à gauche. Recherchez **les certificats de serveur** dans le volet central et double-cliquez pour l'ouvrir. Sélectionnez **Créer une demande de certificat...** dans le volet Actions à droite. L'Assistant **Demander un certificat** apparaît. Sur la page **Propriétés du nom distinctif**, entrez les valeurs dans le formulaire de votre système. Tous les champs doivent être entrés. Sélectionnez **Suivant** pour continuer. Sur la page **Propriétés du fournisseur de services de chiffrement**, conservez la sélection par défaut pour **le fournisseur de services de chiffrement** :. Modifiez la **longueur du bit** : jusqu'à un minimum de **2048**. Sélectionnez **Suivant** pour continuer. Sur la page **Nom du fichier**, sélectionnez l'emplacement où vous souhaitez enregistrer le fichier CSR. Fournir le fichier à l'AC. Lorsque vous avez reçu le certificat signé, copiez-le sur le serveur Web et passez à l'étape suivante. Dans le même emplacement dans le Gestionnaire IIS, sélectionnez **Compléter la demande de certificat** dans le volet **Actions**. L'Assistant s'affiche. 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 **Sélectionner un magasin de certificats pour le nouveau certificat** : est défini sur **Personnel**. Sélectionnez **OK** pour terminer le téléchargement du certificat. Passez à l'étape principale suivante, **Lier le certificat au site Web**.
2. Via Microsoft Management Console (MMC) Utilisez ces étapes pour générer une CSR via MMC. Cette méthode vous permet de personnaliser chaque aspect de la CSR. Cliquez avec le bouton droit sur le bouton Démarrer et sélectionnez Exécuter. Tapez **mmc** dans la zone run et sélectionnez **OK**. Ajoutez le composant logiciel enfichable Certificat à la fenêtre MMC. Sélectionnez **Fichier**, puis **Ajouter/Supprimer un composant logiciel enfichable....** La zone **Ajouter ou supprimer des composants logiciels enfichables** apparaît. Dans la liste de gauche, recherchez **Certificats**, puis sélectionnez **Add >**. La zone du composant logiciel enfichable Certificats s'affiche. Sélectionnez l'option **Compte d'ordinateur**, puis sélectionnez **Suivant >**. Assurez-vous que **l'ordinateur local : (l'ordinateur sur lequel se trouve cette console)** est sélectionné dans la page **Sélectionner un ordinateur**, puis sélectionnez **Terminer**. Sélectionnez **OK** pour fermer la zone **Ajouter ou supprimer des composants logiciels enfichables**. Générer le CSR Dans le volet gauche, développez **Certificats (Local Computer)**, puis **Personal** et sélectionnez le dossier **Certificats**. Cliquez avec le bouton droit sur le dossier **Certificats** et accédez à **Toutes les tâches > Opérations avancées >** puis sélectionnez **Créer une demande personnalisée...** L'Assistant **Inscription de certificat** apparaît. Sélectionnez **Suivant** dans l'écran d'introduction. Sur la page **Sélectionner une stratégie d'inscription de certificat**, sélectionnez **Continuer sans stratégie d'inscription**, répertoriée sous **Demande personnalisée**, puis sélectionnez **Suivant**. Sur la page **Demande personnalisée**, assurez-vous que le **modèle** sélectionné est **(sans modèle) la clé GNC**, et que le **format de demande** est approprié pour votre autorité de certification. **PKCS #10**

fonctionne avec l'autorité de certification Microsoft. Sélectionnez **Suivant** pour passer à la page suivante. Sur la page **Informations sur le certificat**, sélectionnez la liste déroulante en regard du mot **Détails**, puis cliquez sur le bouton **Propriétés**. Le formulaire **Propriétés du certificat** apparaît. Ce document ne couvre pas toutes les options du formulaire **Propriétés du certificat**. Pour plus d'informations, reportez-vous à la documentation Microsoft. Voici quelques notes et astuces sur ce formulaire. Assurez-vous de renseigner toutes les valeurs requises dans le **nom d'objet** : section du **sujet** : onglet Assurez-vous que la valeur fournie pour le **nom commun** est également fournie dans le **nom alternatif** : section Définissez le **type** : dans **DNS**, tapez l'URL dans la **valeur** : , puis sélectionnez le bouton **Ajouter >**. Si vous souhaitez utiliser plusieurs URL pour accéder à la CEE, indiquez chaque autre nom dans ce même champ et sélectionnez **Ajouter >** après chaque Assurez-vous de définir la **taille de clé** de l'onglet **Clé privée** sur une valeur supérieure à 1024. Si vous prévoyez d'exporter le certificat à utiliser sur plusieurs serveurs Web, comme c'est souvent le cas dans une installation HA, assurez-vous que vous sélectionnez **Rendre la clé privée exportable**. Si ce n'est pas le cas, il est impossible d'exporter le certificat ultérieurement Les valeurs que vous entrez et les sélections que vous faites ne sont pas validées. Vous devez vous assurer que vous fournissez toutes les informations requises ou que l'AC peut ne pas être en mesure de remplir le CSR Une fois toutes les sélections sélectionnées, **OK** pour revenir à l'Assistant. Sélectionnez **Suivant** pour passer à la page suivante. Dans la section **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, sélectionnez **Base 64** comme format. Fournissez le fichier à votre CA. Une fois qu'ils l'ont signé et vous ont renvoyé le certificat, copiez-le sur le serveur Web et passez aux dernières étapes. 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. Sélectionnez **Suivant** dans l'écran d'introduction. Dans l'écran **Fichier à importer**, sélectionnez le certificat qui a été signé par votre autorité de certification, puis sélectionnez **Suivant**. Assurez-vous de sélectionner **Placer tous les certificats dans le magasin suivant**. Assurez-vous que **Personal** est sélectionné dans le **magasin de certificats** : , puis sélectionnez **Suivant**. Vérifiez l'écran final, puis sélectionnez **Terminer** pour terminer l'importation. Vous pouvez maintenant fermer la console MMC. Si vous êtes invité à enregistrer les paramètres de la console, vous pouvez sélectionner **Non**. Cela n'affecte pas l'importation du certificat. Passez à l'étape principale suivante, **Lier le certificat au site Web**.

Étape 1.2. Lier un certificat au site Web

Attention : Vous devez vous assurer que le champ **hostname** est vide et que l'option **Require Server Name Indication** n'est pas sélectionnée dans la zone **Edit Site Binding**. Si l'un de ces paramètres est configuré, **SPOG** échoue lorsqu'il tente de communiquer avec la CEE

1. Ouvrez le **Gestionnaire des services Internet (IIS)** si vous ne l'avez pas fait précédemment.
2. Dans le volet **Connexions** à gauche, accédez à **Sites** et sélectionnez **Site Web par défaut**. Assurez-vous de sélectionner le nom de site correct si vous avez choisi d'utiliser un nom de site autre que **Site Web par défaut**.
3. Sélectionner **des liaisons...** dans le volet **Actions** à droite. La zone **Liaisons de site** apparaît. S'il n'y a pas de ligne avec le **Type**, **https** et **Port**, **443**, complétez ce qui suit. Sinon, passez à

l'étape principale suivante. Sélectionnez l'**option Ajouter...** , la zone **Ajouter une liaison de site** apparaît.Sélectionnez **https** dans le **type** : dans la liste déroulante.Assurez-vous que l'**adresse IP** : La liste déroulante affiche **All Unregistered** et le **port** : est **443**.Assurez-vous de quitter le **nom d'hôte** : vide et l'**option Exiger l'indication du nom du serveur** n'est pas sélectionnée.Dans le **certificat SSL** : sélectionnez le nom du certificat correspondant à celui que vous avez créé précédemment. Si vous ne savez pas quel certificat choisir, utilisez la **commande Sélectionner...** pour afficher et rechercher les certificats présents sur le serveurUtiliser la **vue...** pour afficher le certificat choisi et vérifier que les détails sont correctsSélectionnez **OK** pour enregistrer votre sélection.Sélectionnez la ligne qui affiche **https** dans la colonne Type, puis sélectionnez **Modifier...** bouton. La zone **Modifier la liaison de site** apparaît. Assurez-vous que l'**adresse IP** : La liste déroulante affiche **All Unregistered** et le **port** : est **443**.Assurez-vous que le **nom d'hôte** : Le champ est vide et l'**option Exiger l'indication du nom du serveur** n'est pas sélectionnée.Dans le **certificat SSL** : sélectionnez le nom du certificat correspondant à celui que vous avez créé précédemment. Si vous ne savez pas quel certificat choisir, utilisez la **commande Sélectionner...** pour afficher et rechercher les certificats présents sur le serveurUtiliser la **vue...** pour afficher le certificat choisi et vérifier que les détails sont correctsSélectionnez **OK** pour enregistrer votre sélection.Sélectionnez **Fermer** pour revenir au Gestionnaire IIS.

4. Vous pouvez maintenant fermer le Gestionnaire IIS.

Étape 2. Configurer SSO Administrateur de partition

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

Note: 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 le certificat Active Directory (AD) et créer un magasin de clés.

Cette étape est nécessaire pour traiter les changements de sécurité récemment annoncés par Microsoft.

Pour plus de détails, consultez le site <https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows>.

1. Obtenez le certificat SSL, au format Base 64, de votre serveur AD que vous fournissez dans le formulaire Configuration de l'administrateur de partition.
2. Copiez le fichier de certificat sur l'un des serveurs d'applications.
3. Ouvrez une session RDP sur le serveur d'applications sur lequel vous avez copié le certificat.
4. Créez une clé Java comme suit. Ouvrez une invite de commande sur le serveur d'applications.Accédez au répertoire bin du kit de développement Java (JDK) de la CEE.Exécutez cette commande. Remplacez les valeurs selon les besoins.
keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c:\ece\pce\mydomain.jks -storepass MyP@ssword
5. Copiez le magasin de clés sur le même chemin sur tous les autres serveurs d'applications de

vosre environnement.

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 avec **Internet Explorer 11**, accédez à l'URL de la partition Business. **Astuce** : La partition Business 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 indiquez le mot de passe de votre système.
3. Une fois que vous êtes connecté, sélectionnez le lien **Administration** sur la console initiale.
4. Accédez au dossier **Configuration SSO** comme suit, **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, saisissez les valeurs de vos protocoles LDAP (Lightweight Directory Access Protocol) et AD. **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 ; nom restant 'DC=exemple, DC=com' Le port de catalogue global non sécurisé est 3268Le port du catalogue global sécurisé est 3269**Attribut DN** - Il doit s'agir de userPrincipalName.**Base** - Ce n'est pas nécessaire si vous utilisez un GC, sinon, vous devez fournir le format LDAP approprié de base.**DN pour la recherche LDAP** - À moins que votre domaine n'autorise la liaison anonyme, vous devez fournir le nom unique d'un utilisateur avec la possibilité de se lier à LDAP et de rechercher dans l'arborescence des répertoires.

Conseil : le moyen le plus simple de trouver la valeur correcte pour l'utilisateur est d'utiliser l'outil Utilisateurs et ordinateurs Active Directory. Activez **Fonctions avancées** dans le menu **Affichage**. Accédez à l'objet utilisateur, puis cliquez avec le bouton droit de la souris et sélectionnez **Propriétés**. Sélectionnez l'onglet **Attributs**. Sélectionnez le bouton **Filtrer**, puis sélectionnez **Afficher uniquement les attributs avec des valeurs**. Recherchez **DisquetName** dans la liste, puis double-cliquez pour afficher la valeur. Mettez en surbrillance la valeur affichée, puis copiez-la et collez-la dans un éditeur de texte. Copiez et collez la valeur du fichier texte dans le champ **DN pour la recherche LDAP**.

La valeur doit être similaire à, CN=pcceadmin, CN=Users, DC=exemple, DC=local**Mot de passe** - À moins que votre domaine n'autorise la liaison anonyme, vous devez fournir le mot de passe spécifié par l'utilisateur.**SSL activé sur LDAP** - Ce champ doit être considéré comme obligatoire pour la plupart des clients.**Emplacement du magasin de clés** - Il doit s'agir de l'emplacement du magasin de clés où vous avez importé le certificat SSL à partir d'AD. Dans l'exemple, il s'agit de c:\ece\pcce\mydomain.jks, comme l'illustre l'image :

Properties: Partition Administrator Configuration



SSO Configuration

	Name	Value
<input checked="" type="radio"/>	LDAP URL *	ldaps://gcdcsrv01.example.local:3269
<input checked="" type="radio"/>	DN attribute *	userPrincipalName
	Base	
<input checked="" type="radio"/>	DN for LDAP search	CN=pcceadmin,CN=Users,DC=example,DC=local
<input checked="" type="radio"/>	Password	*****
<input checked="" type="radio"/>	SSL enabled on LDAP	Yes
<input checked="" type="radio"/>	Keystore location *	c:\ece\pcce\mydomain.jks

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 sauter cette section.

Il existe deux scénarios supplémentaires avec toutes les versions où cette étape peut être requise. La première est lorsque la CEE a été installée dans une configuration haute disponibilité. La deuxième, et plus fréquente, 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 de la CEE sur un serveur portant le nom d'hôte UCSVRECEWEB.example.com, mais que les utilisateurs accèdent aux pages Web de la CEE 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.

Astuce : Utilisez un éditeur de texte tel que Notepad++ au lieu de Bloc-notes ou Wordpad, car ils n'interprètent pas correctement les extrémités de ligne.

1. Ouvrez une session de bureau à distance sur tous les serveurs Web de la CEE dans votre déploiement.
2. Accédez à ce chemin d'accès, {ECE_HOME}\eService\templates\finesse\gadget\spog.
3. Recherchez 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 pour qu'elles correspondent à votre déploiement.

Le 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' sur tous les autres serveurs Web de votre déploiement.

Étape 4. Ajouter CEE à l'inventaire PCCE

À partir de la version 12.0, PCCE dispose de 3 options de déploiement différentes : 2000 agents (2K Agent), 4000 agents (4K Agent) et 12000 agents (12K Agent). Ces trois options de déploiement peuvent être séparées en deux groupes : 2K Agent et 4K/12K Agent. Ils sont séparés de cette façon, car il y a plusieurs différences fondamentales dans leur apparence dans SPOG. Une comparaison très poussée des deux méthodes suit 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 la CEE au PCCE. Ce document suppose également que votre installation PCCE est terminée et que vous pouvez accéder à d'autres aspects de la solution et les configurer.

- Déploiement de 2 000 agents La configuration initiale des composants PCCE s'effectue entièrement via l'administration CCE et est automatisée De nouveaux composants sont ajoutés à la page Inventaire par le biais d'une zone contextuelle dans laquelle vous entrez les détails tels que l'adresse IP ou le nom d'hôte, ainsi que les informations d'identification nécessaires ou la configuration spécifique au composant.
- Déploiement de 4 000 et 12 000 agents La plupart de la configuration initiale reflète les étapes utilisées pour UCCE Les composants sont ajoutés via un fichier CSV (Comma-Separated Values) que vous téléchargez à partir de l'administration CCE, remplissez par installation spécifique, puis 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 sont ajoutés via des fichiers CSV contenant les informations requises

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

1. Si des certificats auto-signés sont utilisés Ouvrez une connexion Bureau à distance au serveur principal de données d'administration (ADS) côté A. Ouvrez Internet Explorer 11 en tant qu'administrateur et accédez à la partition d'entreprise de la CEE. Sélectionnez l'icône d'un cadenas à droite de la barre d'URL, puis sélectionnez **Afficher les certificats**. Dans la zone **Certificat**, sélectionnez l'onglet **Détails**. Sélectionnez **Copier dans le fichier...** en bas de l'onglet. Dans l'**Assistant Exportation de certificat**, sélectionnez **Suivant** jusqu'à ce que vous atteigniez la page **Exporter le format de fichier**. Assurez-vous de sélectionner le format **X.509 (.CER)** codé **en base-64**. Enregistrez le certificat à un emplacement tel que **c:\Temp\certificates** sur le serveur ADS pour terminer l'exportation. Copiez le certificat sur tous les autres serveurs ADS. Ouvrez une invite de commande administrative. Accédez au répertoire d'accueil Java, puis au répertoire bin. Vous pouvez accéder au répertoire d'accueil de Java à l'aide de la commande suivante : **cd %JAVA_HOME%\bin** Sauvegardez le fichier **cacerts** actuel. Copiez le fichier **cacerts** de **%JAVA_HOME%\lib\security** vers un autre emplacement. Exécutez cette commande pour importer le certificat que vous avez enregistré

précédemment. Si votre mot de passe 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 <nom de domaine complet du serveur de la CEE> -file <emplacement où vous avez enregistré le certificat>Redémarrez le serveur ADS.Répétez les étapes 8 à 12 sur les autres serveurs ADS.

2. Si des certificats signés par l'autorité de certification sont utilisés Obtenez le certificat racine et intermédiaire au format DER/PEM et copiez-les à un emplacement tel que **C:\Temp\certificates** sur tous les serveurs ADS. **Note:** Contactez votre administrateur AC pour obtenir ces certificats. Ouvrez une connexion de bureau à distance à l'ADS principal côté A.Ouvrez une invite de commande administrative.Accédez au répertoire d'accueil Java, puis au répertoire bin. Vous pouvez accéder au répertoire d'accueil de Java à l'aide de la commande suivante : **cd %JAVA_HOME%\bin**Sauvegardez le fichier **cacerts** actuel. Copiez le fichier **cacerts** de **%JAVA_HOME%\lib\security** vers un autre emplacement.Exécutez cette commande pour importer le certificat que vous avez enregistré précédemment. Si votre mot de passe 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 la racine de l'autorité de certification> -file <Emplacement où vous avez enregistré le certificat racine>Répétez l'étape 6. et importer le certificat intermédiaire s'il y en a.Redémarrez le serveur ADS.Répétez les étapes 2 à 12 sur tous les autres serveurs ADS.

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

- Bien que le serveur de données doive exister dans l'inventaire du système, aucune communication directe n'est effectuée entre l'ADS PCCE et le serveur de données
- Lorsque ECE est déployé dans le déploiement de 1 500 agents, le serveur de données est le serveur de services
- Lorsque ECE est installé dans une configuration HA, les deux serveurs Services doivent être ajoutés

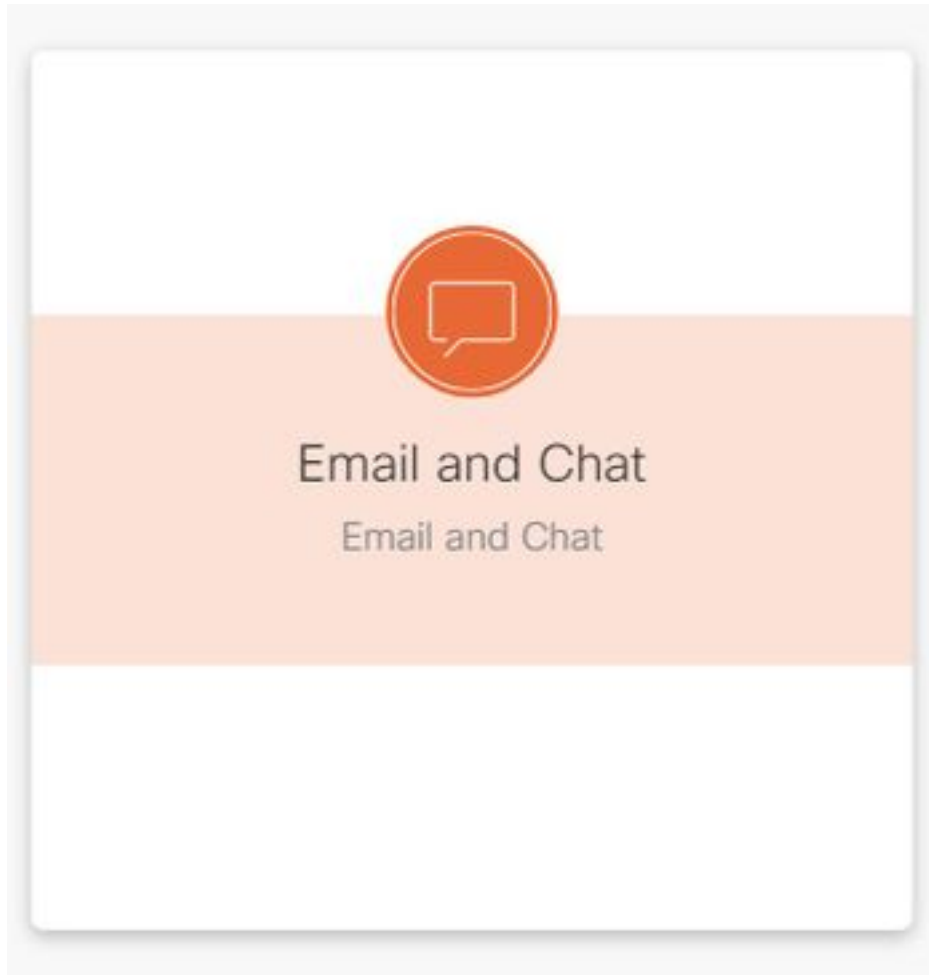
Étape 4.3. Ajouter le serveur Web de la CEE à l'inventaire

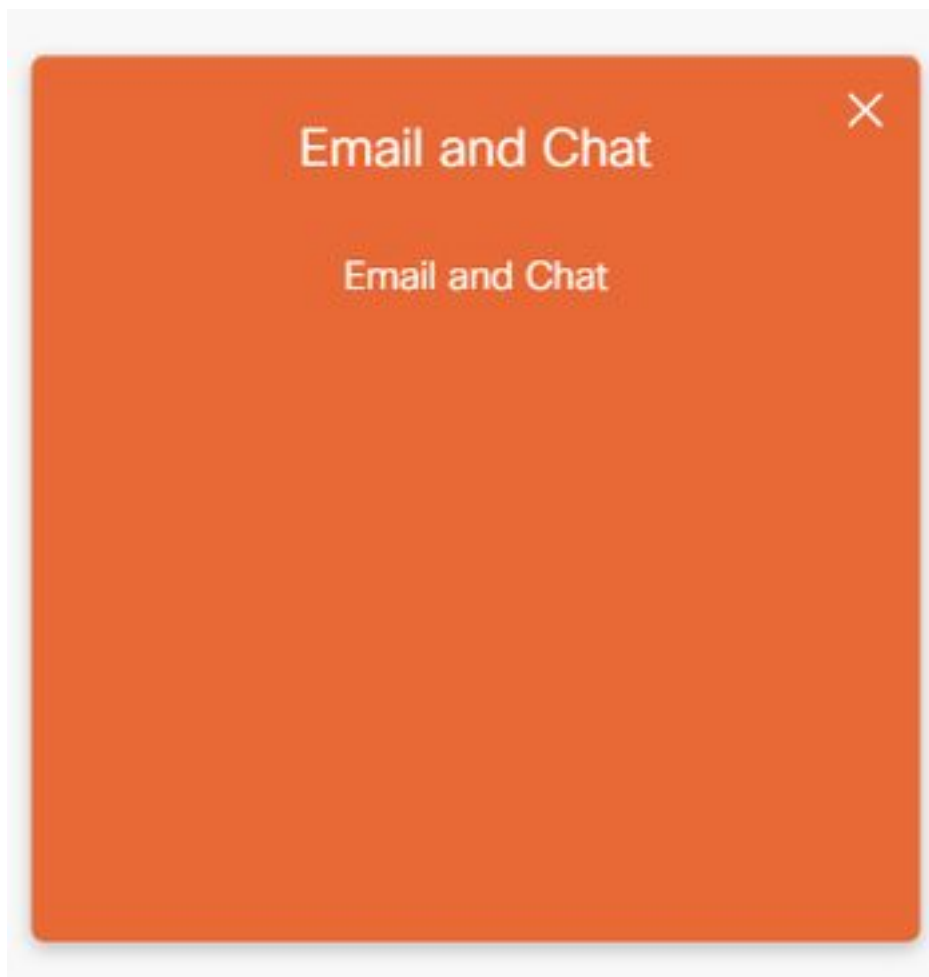
- Assurez-vous d'ajouter le serveur Web avec le nom complet Ce nom doit correspondre au nom commun dans le certificat CEE ou doit figurer dans la liste des noms de remplacement de sujet (SAN)Vous ne devez pas utiliser uniquement le nom d'hôte ou l'adresse IP
- Le nom d'utilisateur et le mot de passe de la CEE doivent correspondre aux informations d'identification de l'AP
- Assurez-vous que l'instance d'application est correcte Le nom de l'instance d'application est sensible à la cassePour les déploiements 2000 Agent PCCE, l'instance d'application est multicanalPour les déploiements PCCE d'agent 4000/12000, l'instance d'application contient le site et le jeu de périphériques faisant partie du nom
- Lorsque ECE est installé avec plus d'un serveur 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 en tant que nom complet du serveur Web.
- Si vous avez plusieurs déploiements CEE, ou si vous choisissez d'ajouter chaque serveur

Web en déploiement avec plusieurs, vous pouvez choisir le serveur Web approprié lorsque vous ouvrez le gadget ECE dans SPOG.

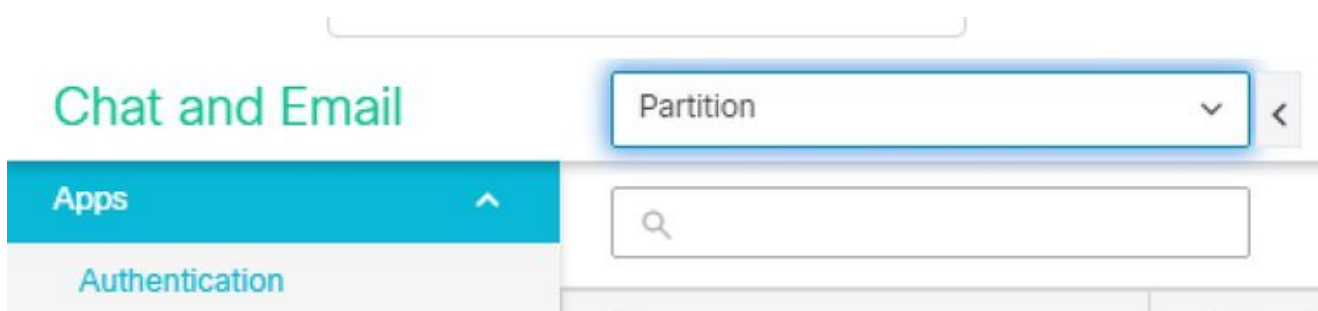
Étape 5. Intégrer la CEE au PCCE

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 indiqué dans l'image.






3. Examinez le serveur sélectionné dans la liste déroulante Device Name (Nom du périphérique). Si vous avez ajouté les deux serveurs Web dans une installation haute disponibilité, vous pouvez choisir l'un ou l'autre serveur Web. Si vous ajoutez un deuxième déploiement ECE à votre système ultérieurement, assurez-vous de sélectionner le serveur approprié avant de continuer.
4. Dans la liste déroulante en regard de **Discussion et e-mail**, sélectionnez **Partition** ou **Global** comme indiqué dans l'image.



5. Dans le menu supérieur, sélectionnez **Intégration**, puis cliquez sur la flèche en regard de **Unified CCE** et sélectionnez le second **Unified CCE** comme indiqué dans l'image.



6. Remplissez les valeurs de l'onglet **Détails AWDB** pour votre installation, puis sélectionnez le bouton **Enregistrer**.
7. Sélectionnez l'onglet **Configuration** et complétez ceci comme suit. Sélectionnez la liste déroulante en regard de **l'instance d'application** et sélectionnez l'instance d'application créée pour ECE. **Note:** Il ne doit pas s'agir de l'instance d'application qui commence par

UQ. Sélectionnez le cercle vert avec le bouton blanc plus le signe  sélectionnez Agent PG. Sélectionnez le groupe de compétences de l'agent (ou les groupes de compétences de l'agent si plusieurs groupes de compétences sont nécessaires). Sélectionnez **Enregistrer** une fois que vous avez ajouté tous les groupes de compétences d'agent. **Avertissement :** Une fois que vous avez sélectionné **Enregistrer** le système est connecté de manière permanente à PCCE et ne peut pas être annulé. Si des erreurs sont commises 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 CEE

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 **Utilisateurs**, puis **Agents** dans la barre de navigation de gauche.
3. Sélectionnez un agent dans la liste et vérifiez-le. Vous devriez maintenant voir une nouvelle case à cocher pour **l'e-mail et la discussion de support** dans l'onglet **Général**. Vous devriez maintenant voir un nouvel onglet intitulé **Activer la messagerie électronique et la discussion** comme illustré dans l'image.

4. Activez un agent de test pour ECE. Activez la case à cocher **Support Email & Chat** et notez que l'onglet **Enable Email & Chat** peut maintenant être sélectionné. Sélectionnez l'onglet **Activer le courrier électronique et la discussion** et indiquez une valeur dans le champ **Nom de l'écran**. Sélectionnez **Enregistrer** pour mettre à jour l'utilisateur. Vous devriez recevoir un message de réussite.
5. Vérifier que la CEE a été mise à jour. Sélectionnez le bouton de navigation **Vue d'ensemble**, puis sélectionnez la carte et le lien **E-mail et conversation**. Dans la liste déroulante en regard de **Chat and Email**, sélectionnez le nom qui correspond au service de l'agent. **Note:** Le service Service de la CEE détient tous les objets appartenant au service Global du PCCE. Le service de nom de service est donc une valeur réservée. Dans le menu supérieur, sélectionnez **Gestion des utilisateurs**, puis sélectionnez **Utilisateurs** dans le menu sous **Discussion et courrier électronique**. Vérifiez que le nouvel agent apparaît dans la liste.

Dépannage

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

- Éditeur de texte tel que Notepad++
- Un outil d'archivage tel que 7-Zip
- Un des nombreux programmes Tail for Windows

Voici quelques exemples : Baretail - <https://www.baremetalsoft.com/baretail/> Queue pour Win32 - <http://tailforwin32.sourceforge.net/>

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 lieux des fichiers sur la CEE

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

Clé de 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 de processus principale
eg_log_dal_connpool_{SERVERNAME}_{PROCESS}.log - Utilisation du pool de connexion
eg_log_query_timeout_{SERVERNAME}_{PROCESS}.log - Mise à jour en cas d'échec d'une requête en raison d'un délai d'attente

2. Noms et emplacements des fichiers sur PCCE

Les journaux PCCE pour les problèmes d'intégration se trouvent tous sur la liste des services de distribution de services (ADS) côté A. Voici les journaux les plus importants lors du dépannage des problèmes d'intégration. Chacun de ces sites se trouve à l'adresse, C:\icm\tomcat\logs.

Parmi ces journaux, les trois premiers sont les plus fréquemment demandés et examinés. Utilisez ces étapes pour définir des niveaux de suivi et collecter les journaux requis.

- 3. Configuration du niveau de suivi** Cette section ne s'applique qu'à la CEE. Les journaux requis à partir de PCCE ont leur niveau de suivi défini par Cisco et ne peuvent pas être modifiés. À partir d'une station de travail ou d'un ordinateur avec **Internet Explorer 11**, accédez à l'URL de la partition système. **Astuce** : 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> Connectez-vous en tant que **sa** et fournissez le mot de passe de votre système. Une fois que vous êtes connecté, sélectionnez le lien **Système** sur la console initiale. Dans la page Système, développez **System > Shared Resources > Logger > Processes**. Dans le volet supérieur droit, recherchez le processus que vous souhaitez modifier le niveau de suivi et sélectionnez-le.

Note: Dans un système HA et dans un système comportant plusieurs serveurs d'applications, les processus sont répertoriés plusieurs fois. Pour vous assurer de capturer les données, définissez le niveau de suivi pour tous les serveurs qui contiennent le processus. Dans le volet inférieur droit, sélectionnez la liste déroulante **Niveau de suivi maximal** et sélectionnez la valeur appropriée.

La CEE définit 8 niveaux de suivi. Les 4 de cette liste sont ceux qui sont utilisés le plus souvent.

- 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
- Debug - Sortie très détaillée, requise uniquement dans les problèmes les plus complexes
Note: Aucun processus ne doit être maintenu à 6 - Dbquery pendant une longue période, et généralement uniquement avec les conseils du TAC. La plupart des processus doivent rester au niveau de trace, 2-Error. 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, modifiez ces quatre processus pour tracer le niveau 4. EAAS-processus
Processus EAMSdx-processrx-process
Sélectionnez l'icône Enregistrer pour définir le nouveau niveau de suivi.

4. Collecte de fichiers journaux

Ouvrez une session Bureau à distance sur le serveur où le processus enregistre les journaux nécessaires. Accédez à l'emplacement du fichier journal. Serveurs CEE 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.{#}. ECE conserve les 49 fichiers journaux précédents plus 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 de la CEE sont situés à différents endroits en fonction de l'installation spécifique.

400 déploiements d'agents Monoface
Serveur : Serveur colocalisé
Emplacement: {ECE_HOME}\eService_RT\logs
Haute disponibilité
Serveurs : Les deux serveurs partagés
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 propriétaire du rôle Distributed Systems Manager (DSM) écrit les journaux des composants qui font partie du rôle Services. Le propriétaire du rôle DSM se trouve dans l'onglet Processus du Gestionnaire des tâches de Windows. Il y a 10 à 15 processus Java sur ce serveur qui ne sont pas sur le serveur secondaire. Les composants sous DSM incluent EAAS, EAMS, Retriever, Dispatcher, Workflow, etc.

1 500 déploiements d'agents
Journaux situés sur le serveur qui héberge le rôle
Emplacement: {ECE_HOME}\eService\logs
À l'exception du serveur 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 propriétaire du rôle Distributed Systems Manager (DSM) écrit les journaux. Le propriétaire du rôle DSM peut être identifié par le nombre de processus affichés dans le Gestionnaire des tâches de Windows. Il y a 10 à 15 processus Java qui s'exécutent sur le serveur principal et seulement 4 processus Java sur le serveur secondaire.

Serveurs PCCE
Les journaux requis de PCCE sont disponibles à l'adresse suivante :
C:\icm\tomcat\logs
Les journaux Tomcat ne sont pas restaurés ou archivés. Les journaux sont écrits dans l'heure du serveur local. Collecter tous les journaux qui ont été créés ou modifiés

après l'observation du problème.

Une explication complète des journaux et des problèmes qui s'affichent dépasse le cadre de ce document. Voici quelques questions courantes, les points à examiner et quelques solutions possibles.

Problèmes liés au certificat

Certificat non importé

Comportement : Lorsque vous tentez d'ouvrir le gadget ECE dans SPOG, l'erreur suivante s'affiche : « Une erreur s'est produite lors du chargement de la page. Contactez l'administrateur. »

Vérifier : La connexion Catalina à PCCE pour les erreurs similaires à celles-ci

`javax.net.ssl.SSLHandshakeException : sun.security.validator.ValidatorException : Échec de la construction du chemin PKIX :`

`sun.security.provider.certpath.SunCertPathBuilderException` : chemin de certification valide introuvable vers la cible demandée

Résolution : Assurez-vous d'avoir importé le certificat de serveur Web CEE ou les certificats d'autorité de certification appropriés dans le magasin de clés de l'ADS

Incompatibilité de certificat

Comportement : Lorsque vous tentez d'ouvrir le gadget ECE dans SPOG, une erreur s'affiche, indiquant que le nom commun ou le nom alternatif de l'objet du certificat 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 du nom secondaire de l'objet contient le nom complet que vous avez entré dans SPOG en tant que nom de serveur Web.

Problèmes système

Service non démarré

Comportement : Lorsque vous essayez d'ouvrir le gadget ECE dans SPOG, l'erreur s'affiche : « La page Web à l'adresse `https://{url}` peut être temporairement désactivée ou avoir été déplacée définitivement vers une nouvelle adresse. »

Vérifier : Vérifiez que le service Windows - Service Cisco a été démarré sur tous les serveurs CEE, à l'exception du serveur Web. Examiner les journaux racine sur le serveur d'applications à la recherche d'erreurs

Résolution : Démarrez le service Cisco sur tous les services CEE.

Problème de configuration

Configuration LDAP

Comportement : Lorsque vous tentez d'ouvrir le gadget ECE dans SPOG, l'erreur suivante s'affiche : « Une erreur s'est produite lors du chargement de la page. Contactez l'administrateur. »

Vérifier : Augmentez le niveau de suivi du serveur d'applications au niveau 7- Debug, puis recommencez la connexion et consultez le journal du serveur d'applications. Recherchez le mot LDAP.

Résolution : Validez la configuration LDAP pour l'authentification unique Administrateur de partition pour 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 CEE. Il ne s'agit pas d'une liste exhaustive de documents de la CEE.

Attention : La plupart des documents de la CEE ont deux versions. Assurez-vous de télécharger et d'utiliser les versions de PCCE. Le titre du document est soit **pour Packaged Contact Center Enterprise**, soit **(Pour PCCE)** ou **(Pour UCCE et PCCE)** après le numéro de version.

Assurez-vous de consulter la page de démarrage de la documentation 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 des e-mails et des conversations d'entreprise](#)[Guide de mise à niveau des e-mails et des conversations d'entreprise](#)[Guide de l'administrateur de messagerie et de conversation d'entreprise](#)
- 12.5 [Guide d'installation et de configuration des e-mails et des conversations d'entreprise](#)[Guide de mise à niveau des e-mails et des conversations d'entreprise](#)[Guide de l'administrateur de messagerie et de conversation d'entreprise](#)