ECE met PCCE integreren in versie 12.0 en hoger

Inhoud

Inleiding

In dit document worden de stappen beschreven om Enterprise Chat en Email (ECE) te integreren met Packaged Contact Center Enterprise (PCCE) in versies 12.0 en hoger

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Enterprise Chat en e-mail (ECE) 12.x
- Packaged Contact Center Enterprise (PCCE) 12.x

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

PCCE versie 12.0 introduceerde een nieuwe beheerinterface die bekend staat als het Single Pane of Glass (SPOG). Bijna al het beheer van het contactcentrum en de bijbehorende toepassingen wordt nu in deze interface uitgevoerd. Om zowel de ECE als de PCCE goed te integreren, moet u een aantal stappen ondernemen die uniek zijn voor deze integratie. Dit document begeleidt u bij dit proces.

Terminologie

In dit document worden deze termen gebruikt.

- Enterprise Chat and Email (ECE) - ECE is een product waarmee e-mail en chatverzoeken op dezelfde manier als spraakoproepen kunnen worden verzonden naar contactcenters.
- Single Pane of Glass (SPOG) - SPOG is de manier waarop PCCE-toediening wordt uitgevoerd in versie 12.0 en hoger. SPOG is een volledige herschrijven van het CCE-beheergereedschap dat vóór 12.0 in versies is gebruikt.
- certificaatautoriteit (CA) - een entiteit die digitale certificaten afgeeft in overeenstemming met het model van een openbare sleutelinfrastructuur (PKI). Er zijn twee soorten CA's die u kunt tegenkomen.Openbare CA - Een openbare CA is een waarvan de wortel- en intermediaire certificaten bij de meeste browsers en besturingssystemen zijn inbegrepen. Enkele veel voorkomende openbare CA's zijn IdenTrust, DigiCert, GoDaddy en GlobalSign.Private CA - Een particuliere CA is er een die binnen een bedrijf bestaat. Sommige particuliere CA's worden ondertekend door openbare CA's, maar meestal zijn dit standalone CA's en de certificaten die zij uitgeven worden alleen door computers in die organisatie vertrouwd.Binnen één van beide CA-typen zijn er twee soorten CA-servers.Root CA Server - De wortel CA server tekent zijn eigen certificaat. In de standaard, multi-tier PKI-inzet, is de Root CA offline en ontoegankelijk. Root CA in dit model geeft ook alleen certificaten uit aan een andere CA server die bekend staat als een Intermediate CA. Sommige bedrijven gebruiken slechts één-tier CA. In dit model geeft de Root CA certificaten uit die bedoeld zijn voor gebruik door een andere entiteit dan een andere CA server.Intermediate CA Server - De tussenliggende of

uitgegevende CA server geeft certificaten uit die bedoeld zijn voor gebruik door een andere entiteit dan een andere CA server.
- Microsoft Management Console (MMC) - Een toepassing die met Microsoft Windows meegeleverd is zodat verschillende invoegtoepassingen kunnen worden geladen. U kunt gebruikmaken van de ingebouwde knoppen om een aangepaste console te maken voor serverbeheer. Er zijn veel verschillende I/U-toetsen meegeleverd met Windows. Een korte lijst met voorbeelden bevat certificaten, apparaatbeheer, diskbeheer, Event Viewer en services.
- Network load Balancer (NLB) - een apparaat of toepassing die meerdere fysieke bronnen aan eindgebruikers aanbiedt met een gebruikelijke fysieke naam. NLB's komen heel veel voor bij webtoepassingen en -services. NLB's kunnen op veel manieren worden geïmplementeerd. Indien gebruikt met ECE, moet de NLB zodanig worden geconfigureerd dat gebruikerssessies terugkeren naar dezelfde fysieke back-end webserver door gebruik te maken van cookie-invoegen of een soortgelijke methode. Dit wordt een 'kleverige' sessie met koekje-invoeging genoemd. Sticky sessie verwijst naar de mogelijkheid van een taakverdeling om de sessie van een gebruiker voor alle interacties terug te geven naar dezelfde fysieke back-end server. Secure Socket Layer (SSL) Passthrough-SSL is een methode waarin de SSL-sessie bestaat tussen het eindgebruikersapparaat en de fysieke webserver waar de sessie van de gebruiker is toegewezen. SSL passthrough staat geen koekje-invoeging toe aangezien de HTTP sessie te allen tijde fysiek versleuteld is. De meeste NLB's ondersteunen kleverige sessie met SSL Passthrough door gebruik van stokkabellen die de servergegroeven en het clienthello-gedeelte van de sessie controleren en de unieke waarden in een tabel opslaan. Wanneer het volgende verzoek dat overeenkomt met deze waarden aan NLB wordt voorgelegd, kan de vanaf de stok-tabel gebruikte worden om de sessie terug te sturen naar dezelfde backend-server.SSL Offload - Wanneer een NLB voor SSL-offload is geconfigureerd zijn er twee SSL-sessies of tunnels voor een bepaalde eindgebruikerssessie. De eerste optie ligt tussen het eindgebruikersapparaat en de virtuele IP (VIP) die op de NLB voor de website is geconfigureerd. De tweede is tussen de back-end IP van NLB en de fysieke webserver waar de sessie van de gebruiker is toegewezen. SSL offload ondersteunt cookie-invoeging omdat de HTTP-stream volledig wordt gedecrypteerd terwijl op de NLB extra HTTP-cookies kunnen worden ingevoegd en sessiecontrole kan worden uitgevoerd. SSL offload wordt vaak gebruikt wanneer de webtoepassing geen SSL vereist maar voor de beveiliging. De huidige versies van de ECE ondersteunen de toegang tot de toepassing niet tijdens een niet-SSL-sessie.

Voorwaarden

Er zijn meerdere voorwaarden die moeten worden vervuld voordat u de twee systemen gaat integreren.

- Minimumniveau van de CE-pleister Versie 12.0(1) - ES37Versie 12.5(1) - Geen actueel minimum voor basisfunctionaliteit
  Webex Experience Management (WXM) Analyzer-functie vereist ES7
- Minimumniveau ECE-patchniveau Aanbevolen wordt om de meest recente Engineering Special (ES) van de ECE te gebruiken.Versie 12.0(1) - ES3 + ES3_ET1aVersie 12.5(1) - Geen actueel minimum voor basisfunctionaliteit
  WXM Analyzer-functie vereist ES1
- Configuratieitems Zorg ervoor dat u de ECE_Email, ECE_Chat en ECE_Outbound Media Routing Domain (MRD’s) associeert met de juiste Application Instance.Voor het PCCE 2000

Agent-implementatiemodel is de Application Instance MultiChannel.Voor het PCCE 4000/12000 Agent implementatiemodel, is de Application Instance in de vorm van {site}_ {rand_set}_ {application_instantie}.
Als u PC met de naam van de site als Main, randapparatuur als PS1 en toepassingsinstantie als multikanaals hebt geïnstalleerd, dan is de naam van de Application Instance Main_PS1_Multichannel.Opmerking: De naam van de Application Instance is hoofdlettergevoelig. Zorg ervoor dat u de naam correct typt wanneer u de ECE Webserver aan Voorbereiding toevoegt.

Integratiestappen

De details voor alle stappen in dit document zijn allemaal opgenomen in de documentatie voor zowel de ECE als de PCCE, maar ze worden niet op een lijst vermeld en ze staan niet allemaal in hetzelfde document. Zie de koppelingen aan het einde van dit document voor meer informatie.

Stap 1. SSL-certificaten configureren

U moet een certificaat genereren dat gebruikt wordt door de ECE-webserver. U kunt een zelfondertekend certificaat gebruiken, maar het is vaak gemakkelijker om een CA-ondertekend certificaat te gebruiken. Zelfgetekende certificaten zijn niet minder veilig dan door CA ondertekende certificaten, er zijn minder stappen om het certificaat aanvankelijk te maken, maar wanneer het certificaat moet worden vervangen, moet u het nieuwe certificaat aan de Java-toetsenborden op alle PC-beheergegevensservers uploaden. Als u een CA-ondertekend certificaat gebruikt, hoeft u alleen de wortel en, indien aanwezig, de tussentijdse certificaten aan de toetsenborden te uploaden.

Als u meerdere webservers in uw toepassing hebt, moet u deze richtlijnen bekijken. De specifieke stappen die vereist zijn om een netwerkloadstabilisator te configureren vallen niet binnen het bereik van dit document. Neem indien nodig contact op met de verkoper van de taakverdeling voor ondersteuning.

Hoewel dit niet nodig is, vereenvoudigt een taakverdeler de implementatie sterk

Toegang tot de ECE-toepassing op elke webserver moet SSL gebruiken, ongeacht de gebruikte belastingsbalansmethode

De taakbalk kan worden ingesteld als SSL-passthrough of SSL-offload

Als SSL passthrough is gekozen, moet dit worden gedaan: U moet alle certificeringsbewerkingen vanaf één server uitvoeren

Nadat het certificaat correct is geconfigureerd moet u het certificaat exporteren en ervoor zorgen dat de privé-toets wordt opgenomen in een PFX-bestand (persoonlijke informatie-uitwisseling)

U moet het PFX-bestand naar alle andere webservers in de implementatie kopiëren en vervolgens het certificaat in IS importeren

Als SSL offload wordt geselecteerd, kan elke webserver worden geconfigureerd met hun eigen SSL-certificaat

Opmerking: Als u meerdere webservers hebt en SSL-passthrough op uw webserver kiest, of als u een gemeenschappelijk certificaat op alle servers wilt hebben, moet u één webserver kiezen om stap 1 uit te voeren, dan moet u het certificaat importeren naar alle andere webservers.
Als u SSL offload kiest, moet u deze stappen op alle webservers uitvoeren. U moet ook een certificaat definiëren voor gebruik in de taakverdeling.

Stap 1.1: genereert een certificaat

U kunt deze sectie overslaan als u al een certificaat hebt gemaakt of gewonnen, en op andere manieren een van de twee opties kiezen.

Optie 1. Gebruik een zelfondertekend certificaat

1. Navigeer naar IIS-administratie.
2. Selecteer de servernaam in de linker Connections-boom.
3. Lokaliseer **servercertificaten** in het midden en dubbelklik op om deze te openen.
4. Selecteer **Zelfondertekend certificaat maken...** van het deelvenster Handelingen rechts.
5. Kies in het venster **Certificaat maken** een naam in het **venster** Automatisch **maken** en voer **een naam in voor het certificaat:** doos. Deze naam is hoe het certificaat in het selectieproces in de volgende grote stap verschijnt. Deze naam hoeft niet overeen te komen met de gewone naam van het certificaat en heeft geen invloed op de wijze waarop het certificaat aan de eindgebruiker verschijnt.
6. Zorg ervoor dat **Persoonlijk** is geselecteerd in **Selecteer een certificaatwinkel voor het nieuwe certificaat:** uitroldoos.
7. Selecteer **OK** om het certificaat te maken.
8. Ga verder naar de volgende grote stap, **Bind certificaat naar website**.

Optie 2. Gebruik een door CA ondertekend certificaat

Voor CA-ondertekende certificaten moet u een certificaataanvraag (CSR) genereren. Het CSR is een tekstbestand dat vervolgens naar de CA wordt verzonden waar het wordt ondertekend en vervolgens wordt het ondertekende certificaat samen met de vereiste CA-certificaten teruggegeven en aan de CSR is voldaan. U kunt ervoor kiezen dit te doen via IIS-beheer of via de Microsoft Management Console (MMC). De methode van het LIS Beheer is veel gemakkelijker zonder speciale kennis vereist maar staat u slechts toe om de velden te configureren die in het attribuut van het Onderwerp van het certificaat worden opgenomen en de bit lengte te wijzigen. Voor geldmarktfondsen zijn extra stappen vereist en u beschikt over een grondige kennis van alle velden die vereist zijn in een geldig CSR. Het wordt ten zeerste aanbevolen dat u MMC alleen gebruikt als u een matige tot deskundige ervaring hebt met het maken en beheren van certificaten. Als uw plaatsing ECE door meer dan één volledig gekwalificeerde naam moet worden benaderd of als u een deel van het certificaat behalve het onderwerp en de bit length moet veranderen, moet u de MMC methode gebruiken.

1. Via i Gebruik deze stappen om een certificaataanvraag (CSR) te genereren via IDS Manager.Navigeer naar IIS-administratie.Selecteer de servernaam in de linker Connections-boom.Lokaliseer **servercertificaten** in het midden en dubbelklik op om deze te

openen.Selecteer **certificaataanvraag maken...** van het deelvenster Handelingen rechts. De wizard **Certificaat aanvragen** verschijnt.Typ de waarden in het formulier voor uw systeem op de pagina **Eigenschappen** van de **naam**. Alle velden moeten worden ingevoerd. Selecteer **Volgende** om verder te gaanLaat op de pagina **Eigenschappen van cryptografische serviceproviders** de standaardselectie voor **cryptografische serviceproviders:**. Verander de **bitlengte:** tot een minimum van **2048**. Selecteer **Volgende** om verder te gaanSelecteer in de pagina **Bestandsnaam** een plaats waar u het CSR-bestand wilt opslaan.Geef het bestand door aan de CA. Wanneer u het ondertekende certificaat hebt ontvangen, kopieert u het naar de webserver en gaat u verder met de volgende stap.Selecteer op dezelfde locatie in IS Manager de optie **Complete certificaataanvraag** in het deelvenster **Handelingen**. De wizard verschijnt.Kies in de pagina **Reactie van** de **certificaatinstantie** opgeven het certificaat dat door uw CA is meegeleverd. Geef een naam in het **Friendly** vakje. Deze naam is hoe het certificaat in het selectieproces in de volgende grote stap verschijnt. Zorg ervoor dat de **optie Een certificaatopslaan voor het nieuwe certificaat selecteert:** de vervolgkeuzelijst is ingesteld op **Persoonlijk**.Selecteer **OK** om het certificaat te uploaden.Ga verder naar de volgende grote stap, **Bind certificaat naar website**.

2. Via Microsoft Management Console (MMC) Gebruik deze stappen om een CSR via MMC te genereren. Met deze methode kunt u elk aspect van de CSR aanpassen.Klik met de rechtermuisknop op de knop Start en selecteer Uitvoeren.Typ **mmc** in het aanloopvak en selecteer **OK**.Voeg het certificaat toe onverwacht aan het MMC venster. Selecteer **Bestand** en **voeg/verwijder Magnetisch-in toe...**. Het vakje **Magnetisch toevoegen of verwijderen** verschijnt.Zoek in de lijst links **certificaten** en selecteer **Toevoegen >**. Het vakje Certificaten magnetisch verschijnt.Selecteer de optie **Computer-account** en selecteer **Volgende >**.Zorg ervoor dat **lokale computer: (De computer waarop deze console is ingeschakeld)** is geselecteerd op de pagina **Computer selecteren** en vervolgens **Voltooien**.Selecteer **OK** om het vakje **Toevoegen of Magnetisch-ins verwijderen** te sluiten.CSR genereren Vul in het linker venster **certificaten** uit **(Local Computer)** en **kies** de map **Certificaten**.Klik met de rechtermuisknop op de map **Certificaten** en navigeer naar **Alle taken > Geavanceerde bewerkingen >** selecteer **Aangepaste aanvraag maken...**. De wizard **certificaatinschrijving** verschijnt.Selecteer **Volgende** op het introductiescherm.Selecteer in de pagina **Beleid voor** inschrijving van het **Certificaat selecteren** de optie **Verwerken zonder inschrijvingsbeleid**, vermeld onder **Aangepaste aanvraag** en selecteer **Volgende**.Zorg er in de pagina **Aangepaste aanvraag** voor dat de **geselecteerde sjabloon** is **(geen sjabloon) CNG-toets** en de **aanvraagindeling** is geschikt voor uw CA. **PKCS #10** werkt met Microsoft CA. Selecteer **Volgende** om verder te gaan naar de volgende pagina.Selecteer op de pagina **certificaatinformatie** de vervolgkeuzelijst naast de woorddetails en selecteer vervolgens de knop **Eigenschappen**. Het formulier **certificaateigenschappen** wordt weergegeven.Het is buiten het bereik van dit document om alle opties voor het formulier **certificaateigenschappen** te geven. Raadpleeg de Microsoft-documentatie voor meer informatie. Hier volgen een paar opmerkingen en tips. Zorg ervoor dat u alle vereiste waarden in de **Onderwerp naam** vult**:** deel van het **Betreft:** tabZorg ervoor dat de waarde die voor **Vaak wordt opgegeven** ook in de **Alternatieve naam** is vermeld**:** sectieStel het **type in:** Typ op **DNS** de URL in de **waarde:** Selecteer vervolgens de knop **Toevoegen >**Als u meerdere URL's wilt gebruiken om toegang te krijgen tot ECE-documenten, geef dan elke alternatieve naam in dit zelfde veld en selecteer **Toevoegen >** na elkZorg ervoor dat u de **grootte** van de **sleutel** in het **tabblad Private Key** op een waarde van meer dan 1024 instelt.Als u van plan bent het te gebruiken certificaat op meerdere webservers uit te voeren, zoals vaak gebeurt in een HA-installatie, zorg er dan voor dat u **Make privé-key exportbaar** maakt. Wanneer dit niet het geval is, kan

het certificaat niet op een later tijdstip worden uitgevoerdDe waarden die u invoert en de selecties die u maakt, worden niet gevalideerd. U moet ervoor zorgen dat u alle vereiste informatie verstrekt of dat CA niet in staat is om de CSR te voltooienNadat u alle geselecteerde opties hebt geselecteerd, **geeft U OK** de wizard terug. Selecteer **Volgende** om verder te gaan naar de volgende pagina.In **Waar wil je de offline aanvraag opslaan?** Selecteer een bestandsnaam op een locatie waar u toegang tot kunt krijgen. Voor de meeste CA's moet u **Base 64** selecteren als de indeling.Geef het bestand op aan uw CA. Wanneer zij het certificaat hebben getekend en u het certificaat hebben teruggegeven, kopieert u het certificaat naar de webserver en gaat u verder met de laatste stappen.In het programma certificaatbeheer onverwacht-in voor MMC, navigeer naar **certificaten (lokale computer) > Persoonlijk**, klik met de rechtermuisknop op **Certificaten** en kies **Alle taken > Importeren...**. De **Wizard Certificaat importeren** verschijnt.Selecteer **Volgende** op het inleidende scherm.Selecteer in het scherm **Bestand om te importeren** het certificaat dat door uw CA is ondertekend en selecteer vervolgens **Volgende**.Zorg ervoor dat u **alle certificaten in de volgende winkel** selecteert.Zorg ervoor dat **persoonlijk** is geselecteerd in de **certificaatwinkel:** Selecteer vervolgens **Volgende**.Bekijk het laatste scherm en selecteer **Voltooien** om de import te voltooien.U kunt nu de MMC-console sluiten. Als u wordt gevraagd de console-instellingen op te slaan, kunt u **Nee** selecteren. Dit heeft geen invloed op de certificaatinvoer.Ga verder naar de volgende grote stap, **Bind certificaat naar website**.

Stap 1.2. Bindcertificaat op de website

Voorzichtig: U moet ervoor zorgen dat het veld hostname leeg is en dat de optie Naam server vereisen niet is geselecteerd in het vak Site-binding bewerken. Als een van deze opties is geconfigureerd faalt SPOG wanneer het probeert te communiceren met de ECE

1. Open Internet Information Services (IS) Manager als u dit niet eerder hebt gedaan.
2. In het linker venster **Connections** navigeer naar **locaties** en selecteer **Standaard website**. Zorg ervoor dat u de juiste naam van de site selecteert als u er voor hebt gekozen om een andere naam dan de standaard website te gebruiken.
3. Selecteer **Bindingen...** in het deelvenster **Handelingen** rechts. Het vakje **Site Bindings** verschijnt. Als er geen rij met het **type** is, **https** en **Port**, **443**, vul het volgende in. Ga anders naar de volgende grote stap. Selecteer de knop **Add...** en het dialoogvenster **Add Site Binding** verschijnt.Selecteer **https** in het **type:** uitvallen.Zorg ervoor dat het **IP-adres:** vervolgkeuzelijst geeft **alle niet-toegewezen** en de **poort** weer**:** veld is **443**.Zorg ervoor dat u de **hostnaam** verlaat**:** Het veld is leeg en de optie **Naam server vereisen is** niet geselecteerd.In het **SSL-certificaat:** Selecteer de certificaatnaam die overeenkomt met de naam die u eerder hebt gemaakt. Als u niet zeker weet welk certificaat u moet kiezen, gebruikt u de knop **Select...** om de certificaten op de server te bekijken en zoekenGebruik de knop **Beeld...** om het gekozen certificaat te bekijken en te controleren of de gegevens juist zijnSelecteer **OK** om de selectie op te slaan.Selecteer de rij die **https** toont in de kolom Type en selecteer vervolgens de knop **Bewerken...**. Het dialoogvenster **Site-binding bewerken** verschijnt. Zorg ervoor dat het **IP-adres:** vervolgkeuzelijst geeft **alle niet-toegewezen** en de **poort** weer**:** veld is **443**.Zorg ervoor dat de **hostnaam:** Het veld is leeg en de optie **Naam server vereisen** is niet geselecteerd.In het **SSL-certificaat:** Selecteer de certificaatnaam die overeenkomt met de naam die u eerder hebt gemaakt. Als u niet zeker weet welk certificaat u moet kiezen, gebruikt u de knop **Select...** om de certificaten op de server te bekijken en

zoekenGebruik de knop **Beeld...** om het gekozen certificaat te bekijken en te controleren of de gegevens juist zijnSelecteer **OK** om de selectie op te slaan.Selecteer **Close** om naar IS Manager terug te keren.
4. U kunt nu de IIS Manager sluiten.

Stap 2. Administrator-taak configureren

Met de configuratie van de beheerder van de afdeling kunt de ECE automatisch een gebruikersaccount voor het niveau van de afdeling maken voor een beheerder die de ECE-indeling in SPOG opent.

> Opmerking: U dient de beheerder van de afdeling te configureren, ook al bent u niet van plan om Agent of supervisor SSO in te schakelen.

Stap 2.1. Verkrijg Active Directory (AD)-certificaat en maak Keystore.

Deze stap is vereist om de recente beveiligingswijzigingen aan te pakken die Microsoft heeft aangekondigd.

Zie voor meer informatie https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows.

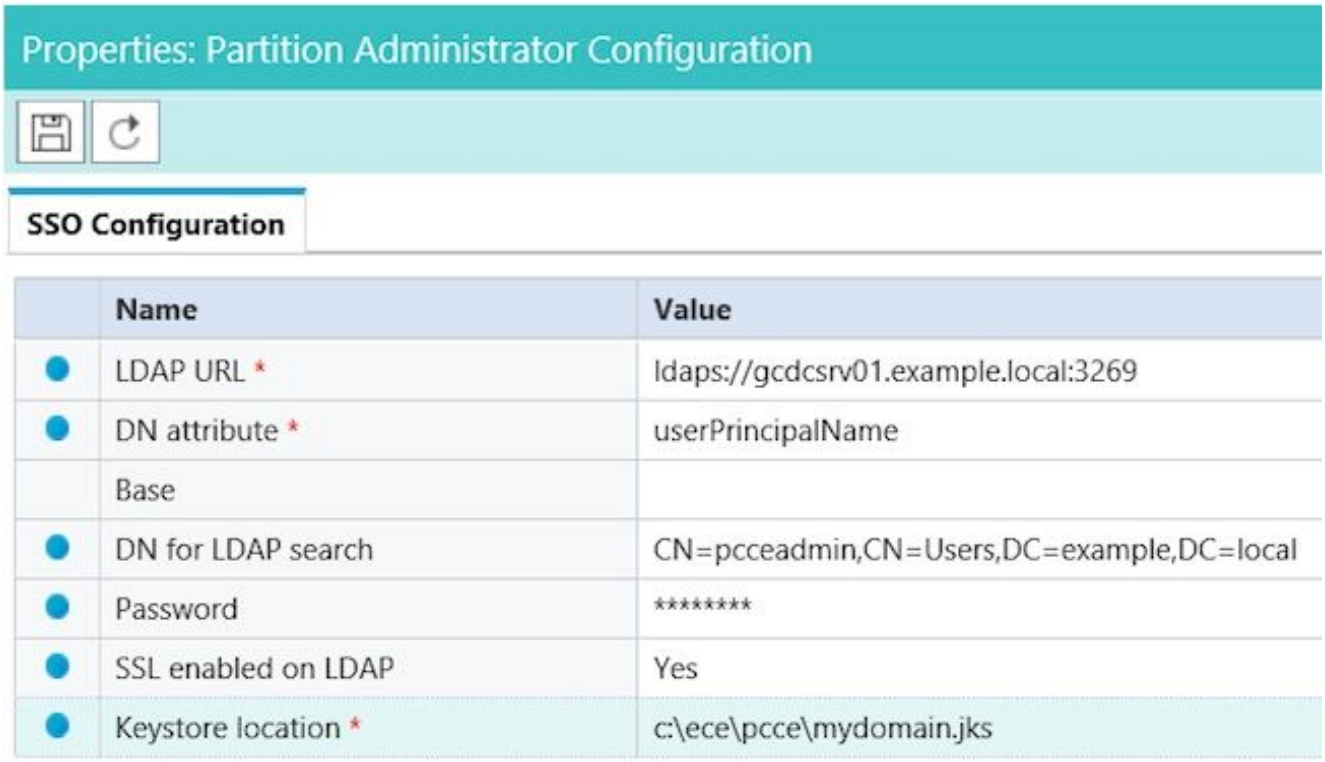
1. Verkrijg het SSL-certificaat, in Base64-indeling, van uw AD-server die u in het formulier Administrator Configuration van de afdeling specificeert.
2. Kopieert het certificaatbestand naar een van de toepassingsservers.
3. Open een RDP-sessie naar de toepassingsserver waar u het certificaat hebt gekopieerd.
4. Maak als volgt een nieuw Java-toetsenbord aan. Open een opdrachtmelding op de toepassingsserver.Verandert naar de directory van de ECE Java Development Kit (JDK).Start deze opdracht. Vervang de waarden indien van toepassing.
keytool -import -trustcacerts -alias mydomaincontroller-file C:\temp\domainctl.crt -keystore c:\ece\pcce\mydomain.jks -storepass MyP@ssword
5. Kopieer de toetsencombinatie naar hetzelfde pad op alle andere toepassingsservers in uw omgeving.

Stap 2.2. Configureer ECE met LAN-toegangsinformatie (LDAP) met lichtgewicht Directory Access Protocol.

1. Vanuit een werkstation of computer met **Internet Explorer 11**, navigeer naar de Business Division URL. **Tip**: De Business Division is ook bekend als Partition 1. Voor de meeste installaties kan de Business Division worden benaderd via een URL die gelijk is aan, https://ece.example.com/default.
2. Meld u aan als **u** het wachtwoord voor uw systeem wilt invoeren.
3. Nadat u met succes hebt aangemeld, selecteert u de koppeling **Administratie** op de eerste console.
4. Navigeer als volgt naar de map **SSO-configuratie**, **Beheer > Partitie: standaard > Security > SSO en Provisioning**.
5. Selecteer in het bovenste venster aan de rechterkant de ingang van de **configuratie van de**

afdeling.

6. Typ in het onderste venster rechts de waarden voor uw Lichtgewicht Directory Access Protocol (LDAP) en AD. **LDAP URL** - Gebruik als beste praktijk de naam van een GC-controller (Global Catalog Domain Controller).
   Als u geen GC gebruikt, ziet u als volgt een fout in de logbestanden van Application Server. Uitzondering in LDAP-verificatie <@>
   javax.name.PartialResultException: niet-verwerkte voortzettingsreferentie(s); resterende naam 'DC=voorbeeld, DC=com' Niet-beveiligde Global Catalyst-poort is 3268Secure Global Catalyst-poort is 3269**DN attribuut** - Dit moet userPrincipalName zijn.**Base** - Dit is niet vereist als u een GC gebruikt, anders moet u het juiste basis-LDAP-formaat leveren.**DNA voor LDAP-zoekfunctie** - Tenzij je domein anoniem laat, moet je de vooraanstaande naam van een gebruiker opgeven met de mogelijkheid om aan LDAP te binden en de directory boom te doorzoeken.
   Tip - De makkelijkste manier om de juiste waarde voor de gebruiker te vinden is het gereedschap Actieve Gebruikers en Computers van de Map te gebruiken. Geavanceerde functies inschakelen in het menu **Beeld**.Navigeer naar het gebruikersobject en klik met de rechtermuisknop op het object en kies **Eigenschappen**.Selecteer het tabblad **Eigenschappen**.Selecteer de knop **Filter** en selecteer **Alleen eigenschappen met waarden tonen**.Vind **achterhaaldeNaam** in de lijst en dubbelklik op om de waarde te bekijken.Markeren de weergegeven waarde en kopiëren en plakken naar een teksteditor.Kopieer en plak de waarde uit het tekstbestand naar het **DNA voor het** veld **LDAP**. De waarde dient gelijk te zijn aan, CN=pcceadmin, CN=Gebruikers, DC=voorbeeld, DC=local**Wachtwoord** - Tenzij uw domein anoniem toelaat, moet u het wachtwoord voor de gebruiker-gespecificeerd verstrekken.**SSL ingeschakeld op LDAP** - Dit veld moet voor de meeste klanten als verplicht worden beschouwd.**Locatie voor Keystore** - Dit moet de locatie zijn van de keystore waar u het SSL-certificaat uit AD importeert. In het voorbeeld is dit c:\ece\pcce\mydomain.jks, zoals in de afbeelding wordt getoond:



7. Selecteer het pictogram van de diskette om de wijzigingen op te slaan.

Stap 3. Controleer het configuratiebestand

Voor alle 12.0-installaties is voltooiing van deze sectie verplicht. Mogelijk kunt u deze sectie overslaan voor een andere versie dan 12.0.
Er zijn twee extra scenario's met alle versies waarin deze stap kan worden vereist. Het eerste is wanneer de ECE is geïnstalleerd in een instelling met hoge beschikbaarheid. Het tweede, en meest gebruikelijk is wanneer de host naam van de webserver niet overeenkomt met de naam die u gebruikt om ECE-toegang te krijgen. Bijvoorbeeld, als u de ECE Webserver op een server met de gastnaam, UCSVRECEWEB.voorbeeldcom installeert, maar de gebruikers hebben toegang tot de ECE-webpagina's met de URL, chat.voorbeeld.com, dan moet deze sectie worden voltooid. Als de hostname van de server en de URL waarmee u ECE-toegang hebt, hetzelfde zijn en als u versie 12.5 of hoger hebt geïnstalleerd, kunt u deze stap overslaan en de sectie voltooien.

Vervang {ECE_HOME} met de fysieke plaats waar u ECE hebt geïnstalleerd. Bijvoorbeeld, als u ECE op **C:\Cisco** hebt geïnstalleerd, dan plaats {ECE_HOME} met **C:\Cisco** in elke plaats.

> **Tip**: Gebruik een teksteditor zoals Kladblok+ in plaats van een kladblok of Wordpad omdat deze de regel-uiteinden niet goed interpreteren.

1. Open een externe bureausessie aan alle ECE-webservers in uw installatie.
2. Navigeer naar dit pad, **{ECE_HOME}\eService\templates\finesse\gadget\spog**.
3. Pak de **spog_klaar.**jsfile en maak een reservekopie in een veilige plaats.
4. Open het huidige **spog_fig.**jsfile in een teksteditor.
5. Zoek deze twee lijnen en update ze om uw plaatsing aan te passen.
   Het web_server_protocol moet https zijn, update indien nodig.
   Update web_server_name om de volledig gekwalificeerde naam te vinden die u aan ECE toewees om te gebruiken. Voorbeeld: **ece.example.com** var web_server_protocol = "https";var web_server_name = "ece.voorbeeld.com";
6. Veranderingen opslaan.
7. Herhaal op alle andere webservers in uw implementatie.

Stap 4: Toevoegen van de ECE aan de EG-inventaris

Sinds 12.0 heeft PCCE 3 verschillende inzetopties, 2000 Agent (2K Agent), 4000 Agent (4K Agent) en 12000 Agent (12K Agent). Deze drie inzetopties kunnen in twee groepen worden gescheiden, 2K Agent en 4K/12K Agent. Zij worden op deze manier van elkaar gescheiden omdat er verschillende fundamentele verschillen zijn in hoe zij er in SPOG uitzien. Dit punt volgt op een zeer hoge vergelijking van de twee methoden. Dit document bevat geen specifieke stappen om een onderdeel aan de inventaris toe te voegen. Zie de koppelingen aan het einde van dit document voor de specifieke informatie over dit proces. Dit deel bevat specifieke details die moeten worden geverifieerd wanneer u ECE aan PCCE toevoegt. Dit document gaat er ook van uit dat uw PCCE-installatie volledig is en dat u toegang kunt krijgen tot andere aspecten van de oplossing en deze kunt configureren.

- 2K Agent-implementaties De eerste configuratie van de PCCE-componenten gebeurt volledig via de CCE-administratie en wordt geautomatiseerdEr worden nieuwe componenten in de voorraadpagina toegevoegd via een pop-upvenster waarin u de details zoals de IP of Hostname en alle benodigde aanmeldingsgegevens of componentspecifieke configuratie invoert
- 4K- en 12K Agent-implementaties Een groot deel van de eerste configuratie spiegelt de voor

UCCE gebruikte stappenComponenten worden toegevoegd via een CSV-bestand (Comma-Separated Values) dat u van CCE-beheer downloadt, per uw specifieke installatie vult en vervolgens uploadtDe eerste toepassing vereist dat enkele specifieke onderdelen in het eerste CSV-bestand worden opgenomenComponenten die niet waren toegevoegd toen het systeem aanvankelijk was ingesteld, worden toegevoegd via CSV-bestanden die de benodigde informatie bevatten

Stap 4.1. Upload ECE-webservercertificaat voor Java-toetsenbord

1. Indien zelfgetekende certificaten worden gebruikt Open een externe desktopverbinding naar de primaire, side-A Administration Data Server (ADS).Open Internet Explorer 1.1 als beheerder en navigeer naar de ECE-business partitie.Selecteer het pictogram van een hangslot aan de rechterkant van de URL-balk en kies vervolgens **Certificaten bekijken**.Selecteer in het vakje **certificaatnummer** het tabblad **Details**.Selecteer **Kopie naar bestand...** onder in het tabblad.Selecteer in de **wizard Certificaat exporteren** de optie **Volgende** totdat u de pagina **Exporteren** van **Bestand** hebt bereikt. Zorg ervoor dat u **Base-64 gecodeerde X.509 (.CER)**-indeling selecteert.Sla het certificaat op een locatie zoals **c:\Temp\certificates** op de ADS-server op om de export te voltooien.Kopieert het certificaat naar alle andere ADS-servers.Open een melding van de beheeropdracht.Wijzig de directory Java en vervolgens de directory Bin. De lokale folder van Java kan als volgt worden benaderd. **cd %JAVA_HOME%\bin**Een back-up van het huidige activeringsbestand. Kopieer het bestand vanaf **%JAVA_HOME%** \lib\security naar een andere locatie.Start deze opdracht om het certificaat te importeren dat u eerder hebt opgeslagen. Als uw wachtwoord voor het opslaan niet 'verandert' is, update de opdracht om uw installatie aan te passen.
keytool-keystore ../lib/security/cakerts -storepass change -import-alias <FQDN ECE server> -file <locatie waar u certificaat> opgeslagen heeft Start de ADS server opnieuw.Herhaal stap 8-12 op de andere ADS-servers.
2. Indien CA-ondertekende certificaten worden gebruikt Verkrijg het wortel- en tussencertificaat in het DER/PEM-formaat en kopieer het naar een locatie zoals **C:\Temp\certificates** op alle ADS-servers. Opmerking: Neem contact op met de CA-beheerder om deze certificaten te verkrijgen. Open een externe bureauverbinding naar de primaire, zij-A ADS.Open een melding van de beheeropdracht.Wijzig de directory Java en vervolgens de directory Bin. De lokale folder van Java kan als volgt worden benaderd. **cd %JAVA_HOME%\bin**Een back-up van het huidige activeringsbestand. Kopieer het bestand vanaf **%JAVA_HOME%** \lib\security naar een andere locatie.Start deze opdracht om het certificaat te importeren dat u eerder hebt opgeslagen. Als uw wachtwoord voor het opslaan niet 'verandert' is, update de opdracht om uw installatie aan te passen.
keytool-keystore ../lib/security/cacerts-storepass change -trustcerts-import -alias <Name CA root> -file <Location waar u het wortelcertificaat opslaat>Herhaal Stap 6. en voer het tussentijdse certificaat indien aanwezig in.Start de ADS server opnieuw.Herhaal stap 2-12 op alle andere ADS-servers.

Stap 4.2 Voeg de ECE-gegevensserver aan de inventaris toe

- Terwijl de gegevensserver in de systeeminventaris moet bestaan, wordt er geen directe communicatie tussen de PCCE ADS en de gegevensserver uitgevoerd
- Wanneer ECE wordt ingezet in de 1500-Agent-implementatie, is de Data Server de Services

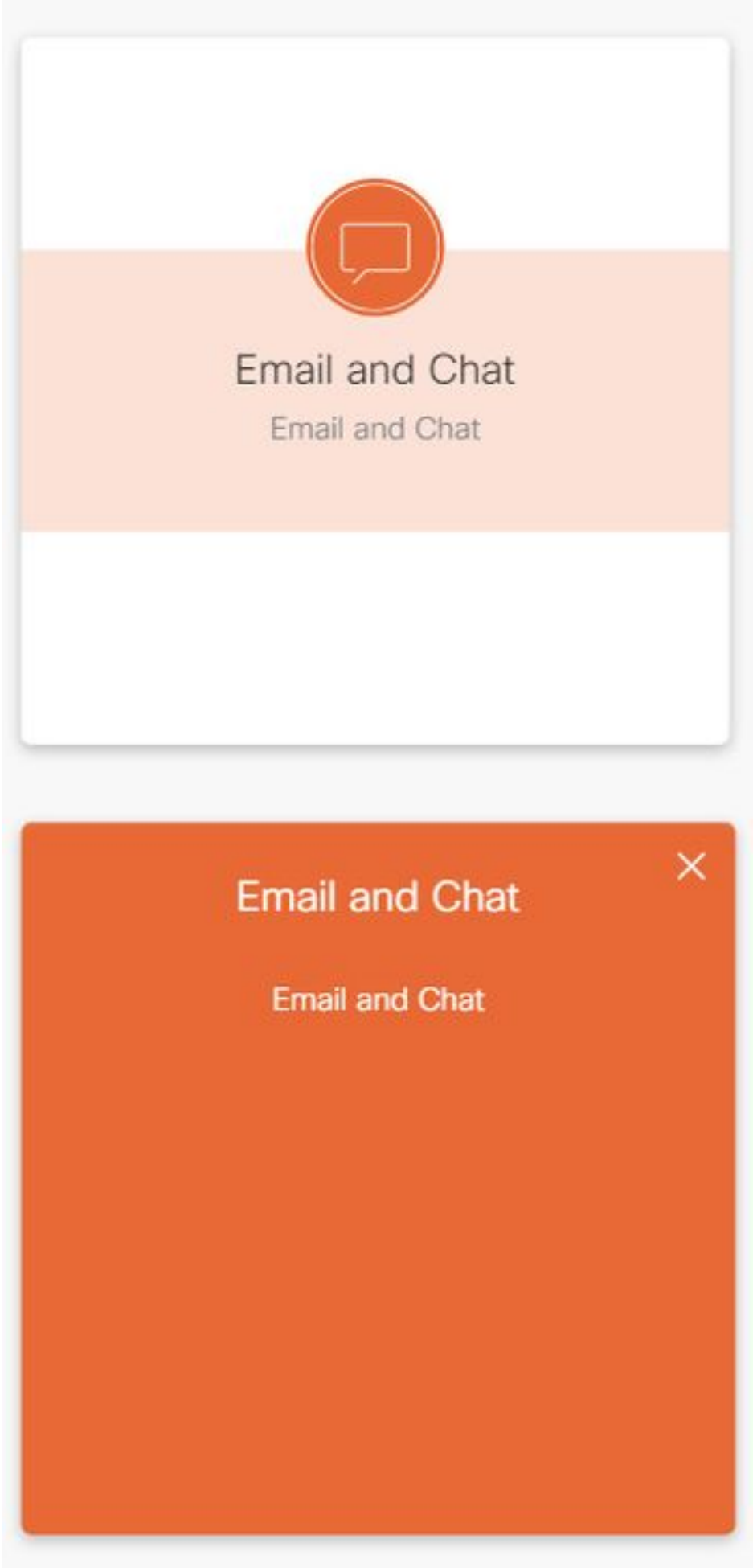
Server
- Wanneer ECE in een HA-configuratie is geïnstalleerd, moeten beide servicesservers worden toegevoegd

Stap 4.3. Voeg de ECE-webserver aan de inventaris toe

- Zorg ervoor dat u de webserver met de volledige naam toevoegt Deze naam moet overeenstemmen met de algemene naam in het ECE-certificaat of moet worden vermeld als een van de Onderwerp Alternative Name (SAN's)U dient niet alleen de hostnaam of IP-adres te gebruiken
- De gebruikersnaam en het wachtwoord voor ECE moeten de volledige inlogreferenties zijn
- Zorg ervoor dat de Application Instance juist is De naam van de toepassingsinstantie is hoofdlettergevoeligVoor de 2000 Agent PCCE-implementaties is de Application Instance MultiChannelVoor de 4000/12000 Agent PCCE-implementaties bevat de Application Instance de locatie en de perifere reeks die deel uitmaken van de naam
- Wanneer ECE met meer dan één webserver is geïnstalleerd, bijvoorbeeld in de 1500 Agent-implementatie of in een 400 Agent HA-toepassing, kunt u de URL gebruiken die op uw taakbalk wijst of de URL die op elke afzonderlijke webserver wijst als de volledig gekwalificeerde naam van de webserver.
- Als je meer dan één ECE-versie hebt, of als je ervoor kiest elke afzonderlijke webserver in plaatsing toe te voegen met meer dan één, kies je de juiste webserver wanneer je de ECE-gadget in SPOG opent.

Stap 5. Integratie van de ECE met de PCCE

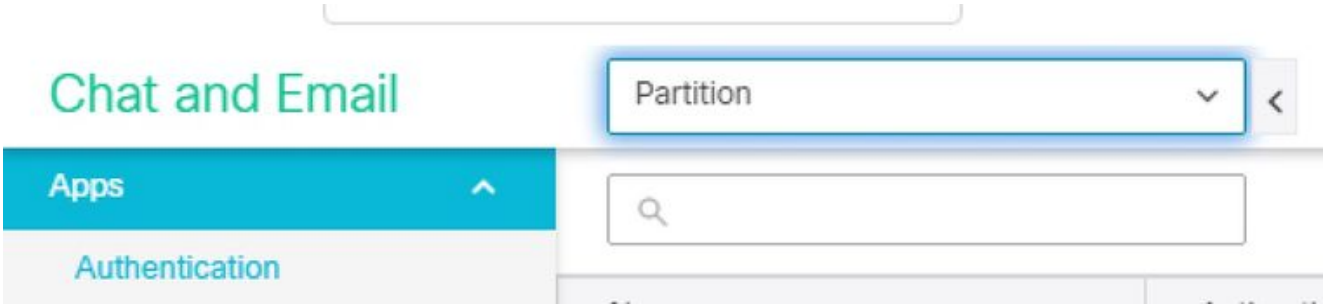
1. Meld u aan bij CCE-beheerder.
2. Selecteer de kaart **E-mail en Chat**, vervolgens de link **e-mail en Chat** zoals in de afbeelding.



3. Bekijk de huidige geselecteerde server in de vervolgkeuzelijst Apparaatnaam. Als u beide webservers in een HA-installatie hebt toegevoegd, kunt u één van beide webservers kiezen.

Als u later een tweede ECE-implementatie aan uw systeem toevoegt, zorg er dan voor dat u de juiste server selecteert voordat u verdergaat.

4. Selecteer in de vervolgkeuzelijst naast **Chat en E-mail** de optie **Verdeling** of **Global** zoals in de afbeelding.

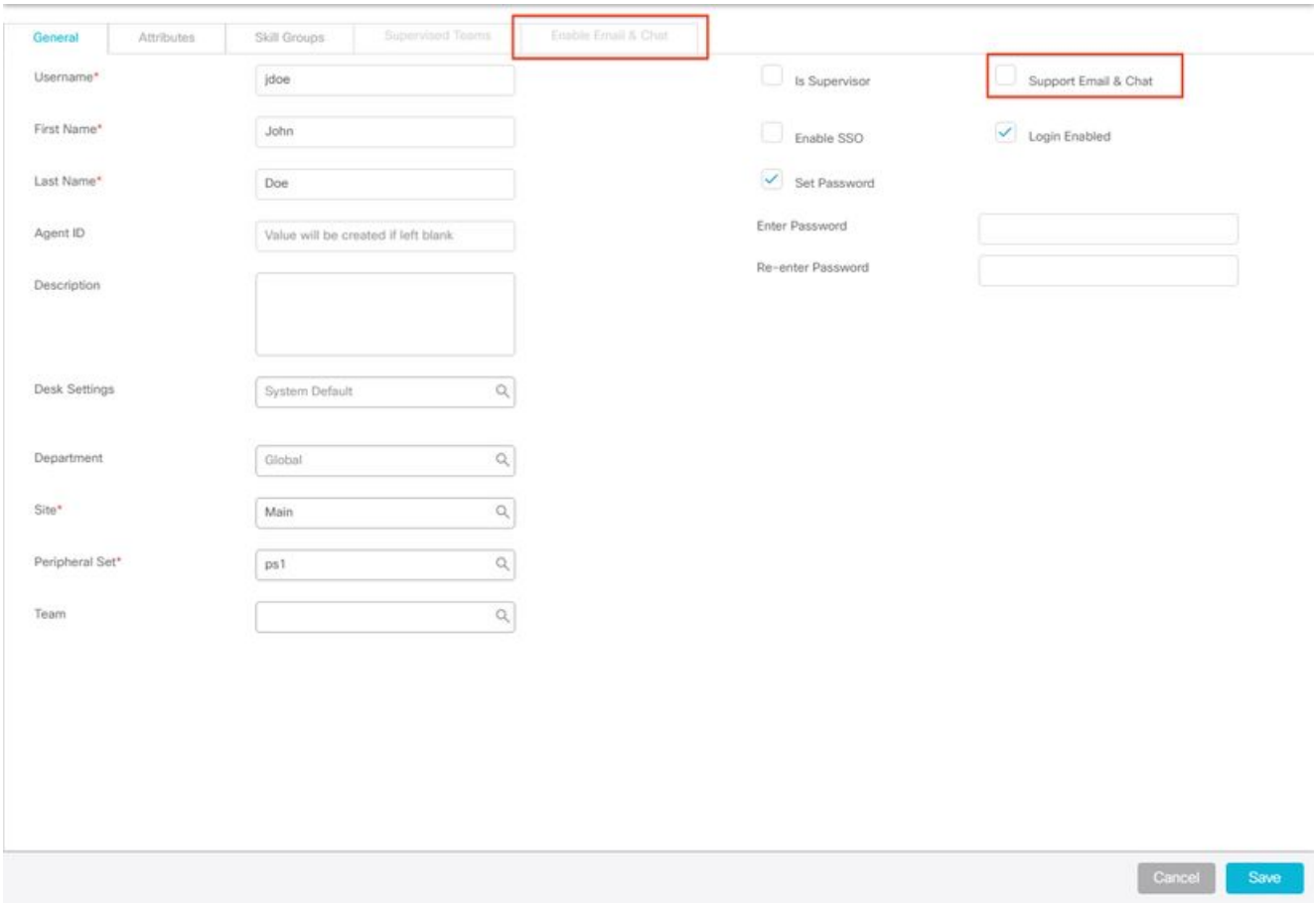


5. Selecteer in het bovenste menu de optie **Integratie**, selecteer vervolgens de pijl naast **Unified CCE** en selecteer de tweede **Unified CCE** zoals in de afbeelding.

6. Populeer de waarden in het tabblad **AWDB Details** voor uw installatie en selecteer vervolgens de knop **Opslaan**.
7. Selecteer het tabblad **Configuration** en vul dit als volgt in. Selecteer de vervolgkeuzelijst naast **Application Instance** en selecteer de Application Instance die is gemaakt voor ECE. Opmerking: Dit mag niet de Application Instance zijn die met UQ begint.Selecteer de groene cirkel met de knop wit plus teken  Selecteer de Agent PG. Selecteer de Agent PG (of Agent PG's als meer dan een).Selecteer **Opslaan** als u alle Agent-pagina's hebt toegevoegd. **Waarschuwing**: Nadat u **Save** the systeem hebt geselecteerd, is de verbinding met PCCE permanent en kan deze niet worden ongedaan gemaakt. Als er fouten worden gemaakt in dit hoofdstuk, moet u ECE -installatie volledig verwijderen en alle databases laten vallen, en ECE installeren alsof het een nieuwe installatie is.

Stap 6. Bevestiging van de ECE-integratie

1. Controleer in CCE-beheer of er geen waarschuwingen in de statusbalk bovenaan worden weergegeven. Als er signaleringen zijn, selecteert u het woord **Waarschuwingen** en controleert u de inventarispagina om er zeker van te zijn dat geen van de waarschuwingen voor de ECE-servers zijn.
2. Selecteer **Gebruikers** en **agents** in de navigatiebalk links.
3. Selecteer een agent uit de lijst en controleer dit. U dient nu een nieuw aanvinkvakje voor **Support Email & Chat** te zien op het **tabblad General**.U dient nu een nieuw tabblad te zien met het label **E-mail inschakelen en chatten** zoals in de afbeelding wordt weergegeven.



4. Schakel een testmiddel in voor ECE. Selecteer het aanvinkvakje **Support Email & Chat** en houd er rekening mee dat het tabblad **Enable Email & Chat** nu kan worden geselecteerd.Selecteer het tabblad **E-mail inschakelen en** geef waarde op in het veld **Schermnaam**.Selecteer **Opslaan** om de gebruiker bij te werken.U zou een succesbericht moeten ontvangen.
5. Controleer of de ECE is bijgewerkt. Selecteer de knop **Overzicht** en kies vervolgens de link **E-mail en de** sleutel tot **Chatfunctie**.Selecteer in de vervolgkeuzelijst naast **Chat en E-mail** de naam die overeenkomt met de afdeling van de agent. Opmerking: De afdeling Onderhoud van de ECE heeft alle objecten die deel uitmaken van het mondiale departement van PCCE. De service is dus een gereserveerde waarde.Selecteer in het bovenste menu de optie **Gebruikersbeheer** en selecteer vervolgens **Gebruikers** in het menu onder **Afdrukken en e-mail**.Bevestig dat u de nieuwe agent in de lijst ziet.

Problemen oplossen

Aanbevolen wordt om verschillende tools te downloaden en op de ECE-servers te houden. Hierdoor kan de oplossing veel gemakkelijker worden opgelost en kan de oplossing in de loop der tijd beter worden onderhouden.

- Een teksteditor zoals Kladblok+
- Een archiefgereedschap zoals 7-Zip
- Eén van de vele Tail voor Windows-programma's
  Een paar voorbeelden zijn: Baretail -https://www.baremetalsoft.com/baretail/Tail voor Win32 - http://tailforwin32.sourceforge.net/

Om problemen met de integratie op te lossen moet u eerst van bepaalde belangrijke logbestanden

en de locatie van elke logbestanden op de hoogte zijn.

1. **Bestandsnaam en locaties op ECE**

   Er zijn veel logbestanden op het ECE-systeem, dit zijn alleen de logbestanden die het meest behulpzaam zijn wanneer u probeert een probleem met integratie op te lossen.

   Server-sleutel:C = Collaboration ServerA = toepassingsserverS = serviceserverM = Messaging ServerDe meeste logbestanden hebben ook twee andere logbestanden die bij hen gekoppeld zijn.eg_log_ {SERVERNAME}_ {PROCESS}.log - Primair proceslogboekeg_log_dal_conpool_ {SERVERNAME}_ {PROCES}.log - gebruik van de verbindingspooleg_log_query_timeout_ {SERVERNAME}_ {PROCESS}.log - Bijgewerkt wanneer een query FALT vanwege time-out
2. **Bestandsnaam en locaties op PCCE**

   PCCE-documenten voor integratieproblemen zijn allemaal te vinden op de zijkant van het ADS. Hier zijn de logbestanden die het belangrijkst zijn omdat u problemen met de integratie oplost. Elk van deze bevindt zich in, **C:\icm\tomcat\logs**.

   Van deze stammen zijn de eerste drie de vaakst opgevraagde en bekeken.Gebruik deze stappen om sporen in te stellen en de benodigde stammen te verzamelen.
3. **Configuratie handelsniveau**Dit punt is alleen van toepassing op de ECE. De logboeken die van PCCE worden vereist hebben hun spoorniveau ingesteld door Cisco en kunnen niet worden gewijzigd. Vanaf een werkstation of computer met **Internet Explorer 11**, navigeer naar de System partitie URL. **Tip**: De systeempartitie is ook bekend als Partitie 0. Voor de meeste installaties kan de systeempartitie worden benaderd via een URL die gelijk is aan, https://ece.example.com/systemMeld u aan **als** zodanig en geef het wachtwoord op voor uw systeem.Nadat u met succes hebt aangemeld, selecteert u de koppeling **Systeem** op de eerste console.In de systeempagina vouwt u **System > Shared Resources > Logger > Processen uit.**In het bovenste, rechter deelvenster vindt u het proces dat u wilt wijzigen om het overtrekken te wijzigen en het vervolgens te selecteren.
   Opmerking: In een HA-systeem en in een systeem met meer dan één toepassingsserver worden de processen meer dan eens vermeld. Om er zeker van te zijn dat u de gegevens opneemt, stelt u het spoorniveau in voor alle servers die het proces bevatten.Selecteer in het onderste, rechter deelvenster de vervolgkeuzelijst voor **maximaal** overtrekken en selecteer de gewenste waarde.
   Er zijn 8 spoorniveaus gedefinieerd in ECE. De 4 in deze lijst zijn de meest gebruikte. 2 - Fout - standaard sporenniveau voor processen4 - Info - Trace-niveau dat algemeen wordt gebruikt voor de oplossing van problemen6 - DBquery - Vaak behulpzaam voor het

diagnosticeren van problemen in een vroeg stadium van de instelling of meer complexe kwesties7 - Debug - zeer omslachtige uitvoer, alleen vereist bij de meest complexe kwestiesOpmerking: Geen proces dient bij 6 te worden bewaard - dBquery moet worden uitgevoerd voor een langere tijd, en in het algemeen alleen met TAC-richtlijn.De meeste processen moeten op spoorniveau, 2-fout blijven. Als u niveau 7 of 8 selecteert, moet u ook een maximale duur instellen. Wanneer de maximale duur is bereikt, keert het spoorniveau terug naar de laatste ingestelde waarde.
Nadat het systeem is ingesteld, veranderen deze vier processen in overtrekken van niveau 4.EAAS-procesEAMS-procesdx-procesrx-procesSelecteer het pictogram Opslaan om het nieuwe niveau voor overtrekken in te stellen.

4. Log bestandsverzameling

Open een externe desktopsessie naar de server waar de gewenste proceslogbestanden aanwezig zijn.Blader naar de locatie van het logbestand. ECE-servers De logbestanden zijn als volgt geschreven.Standaard zijn logbestanden geschreven bestanden met een maximale grootte van 5 MBWanneer één logbestand het ingestelde maximum bereikt, wordt het anders genoemd in het formaat, {LOGNAME}.log.<#}ECE houdt de vorige 49 logbestanden plus het huidige bestand bijHet huidige logbestand eindigt altijd met .log en geen nummer naLogs zijn niet gearchiveerd of gecomprimeerdDe meeste stammen hebben een gemeenschappelijke structuurGebruik <@> om de secties te verwijderenLogs worden altijd in GMT+0000-tijd geschrevenECE-stammen bevinden zich op verschillende plaatsen op basis van de specifieke installatie.400 Agent-implementaties eenzijdig Server: Collaboration-serverPlaats: {ECE_HOME} \eService_RT\logsHoge beschikbaarheid servers: Beide geCollaboreerde serversPlaats: {ECE_HOME} \eService\logsMap die voor het DFS-aandeel (Distributed File System) zijn gemaakt, bevatten alleen logbestanden voor installatie en upgrades.Alleen de server die de rol Distributed Systems Manager (DSM) bezit, schrijft logbestanden voor de onderdelen die deel uitmaken van de servicerol DSM rol-eigenaar is te vinden in het tabblad Processen van Windows Automation Manager. Er zijn 10-15 Java processen op deze server die niet op de secundaire server staan.Onderdelen onder DSM omvatten: EAAS, EAMS, Retriever, Dispatcher, Werkstroom, enz.1500 Agent-implementaties Logs op de server die de rol opslaatPlaats: {ECE_HOME} \eService\logsMet uitzondering van de servicesserver werken en schrijven alle servers logbestanden voor alle processen die met de component verbonden zijnBij een hoge beschikbaarheid werkt de Services server in de configuratie Active/StandbyAlleen de server die de functie Distributed Systems Manager (DSM) bezit, schrijft logbestandenDSM-roleneigenaar kan worden geïdentificeerd aan de hand van het aantal processen dat in Windows Automation Manager wordt gezien. Er zijn 10-15 Java processen die op de primaire server worden uitgevoerd en slechts 4 Java processen op de secundaire serverPCS-servers De vereiste stammen van PCCE zijn te vinden op, C:\icm\tomcat\logsTomcat-stammen worden niet gerold of gearchiveerdAantekeningen worden in lokale servertijd geschrevenVerzamel alle logbestanden die zijn aangemaakt of aangepast nadat de kwestie is waargenomen.

Een volledige uitleg van de documenten en de kwesties die worden gezien, valt buiten het toepassingsgebied van dit document. Een aantal gemeenschappelijke kwesties, wat ze moeten beoordelen en een aantal mogelijke oplossingen zijn de volgende. certificaatgerelateerde problemen Certificaat niet geïmporteerd Gedrag: Wanneer u probeert het ECE-pad in SPOG te openen, ziet u de fout: "Er is een fout opgetreden tijdens het laden van de pagina. Neem contact op met de beheerder."Controleer: Het Catalina log on PCCE voor fouten die vergelijkbaar zijn met deze javax.net.ssl.SHLHandshakeException: sun.security.validator.validatorException: PKIX-pad gebouw mislukt: sun.security.provider.certpath.SunCertPathBuilderException: geen geldig certificatiepad voor het gevraagde doel vindenResolutie: Zorg ervoor dat u het ECE Web Server Certificaat of de geëigende CA certificaten in toetsenbord op ADS hebt ingevoerdcertificaatontbreekt Gedrag: Wanneer u probeert het ECE-pad in SPOG te openen, ziet u een fout die aangeeft dat de veelgebruikte naam van het certificaat of de alternatieve naam van het onderwerp niet overeenkomt met de ingestelde naam.Controleer: Vestig het SSL-certificaatResolutie: Zorg ervoor dat het veld Gemeenschappelijke naam in het Onderwerp, of een van de DNS-velden in de Onderwerp Alternate Name de volledig gekwalificeerde naam bevat die u in SPOG hebt ingevoerd als de naam van de Web Server.Systeemproblemen Service niet gestart Gedrag: Wanneer u probeert om het ECE-gadget in SPOG te openen, zie u de fout, "De webpagina bij https:// {URL} kan tijdelijk laag zijn of het kan permanent naar een nieuw adres verplaatst zijn."Controleer: Bevestig dat de Windows Service - Cisco Service is gestart op alle ECE-servers met uitzondering van de webserver. Herzie de logbestanden Opstarten op de toepassingsserver voor foutenResolutie: Start de Cisco-service op alle ECE-services.Configuratieprobleem LDAP-configuratie Gedrag: Wanneer u probeert het ECE-pad in SPOG te openen, ziet u de fout: "Er is een fout opgetreden tijdens het laden van de pagina. Neem contact op met de beheerder."Controleer: Verhoog het overtrek-niveau van de Application Server naar niveau 7-Debug en probeer vervolgens de inlognaam opnieuw te bekijken en het logbestand van de Application Server te bekijken. Zoek het woord LDAP.Resolutie: Vestig de LBP-configuratie voor de beheerder van de afdeling om er zeker van te zijn dat dit correct is.

Gerelateerde informatie

Dit zijn de belangrijke documenten die u grondig moet herzien voordat u een ECE-installatie of -integratie start. Dit is geen volledige lijst van ECE-documenten.

> **Voorzichtig:** De meeste ECE-documenten hebben twee versies. Zorg ervoor dat u de versies voor PCCE downloaden en gebruikt. De documenttitel heeft hetzij **voor Packaged Contact Center Enterprise** of **(voor PCCE)** of **(voor UCCE en PCCE)** na het versienummer.

Zorg ervoor dat u de startpagina voor Cisco Enterprise Chat en E-mail documentatie voor updates voorafgaand aan installatie, upgrade of integratie controleert.

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

- 12.0 Installatie- en configuratiegids voor ondernemingen en e-mailHandleiding voor Enterprise Chat en E-mail upgradeAdministrator's gids voor Enterprise- en e-mailbeheer
- 12.5 Installatie- en configuratiegids voor ondernemingen en e-mailHandleiding voor Enterprise Chat en E-mail upgradeAdministrator's gids voor Enterprise- en e-mailbeheer