Integrazione di ECE con PCCE nella versione 12.0 e successive

Sommario

Introduzione

In questo documento viene descritto come integrare Enterprise Chat and Email (ECE) con Packaged Contact Center Enterprise (PCCE) nella versione 12.0 e successive

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Enterprise Chat and Email (ECE) 12.x
- Packaged Contact Center Enterprise (PCCE) 12.x

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

PCCE versione 12.0 ha introdotto una nuova interfaccia di gestione nota come Single Pane of Glass (SPOG). Questa interfaccia consente di eseguire quasi tutta la gestione del contact center e delle applicazioni correlate. Per integrare correttamente sia ECE che PCCE, è necessario completare diversi passaggi specifici per questa integrazione. Questo documento guida l'utente in questo processo.

Terminologia

Nel presente documento vengono utilizzati questi termini.

- Enterprise Chat and Email (ECE) - ECE è un prodotto che consente di instradare le richieste di e-mail e chat agli agenti dei contact center nello stesso modo in cui vengono instradate le chiamate vocali.
- Single Pane of Glass (SPOG) - SPOG è il modo in cui viene eseguita l'amministrazione PCCE nella versione 12.0 e successive. SPOG è una riscrittura completa dello strumento di amministrazione CCE utilizzato nelle versioni precedenti alla 12.0.
- CA (Certification Authority) - Entità che rilascia certificati digitali in conformità a un modello PKI (Public Key Infrastructure). Esistono due tipi di CA.CA pubblica: una CA pubblica dispone di certificati radice e intermedi inclusi nella maggior parte dei browser e dei sistemi operativi. Alcune CA pubbliche comuni includono IdenTrust, DigiCert, GoDaddy e GlobalSign.CA privata - Una CA privata è una CA che esiste all'interno di una società. Alcune CA private sono firmate da CA pubbliche, ma nella maggior parte dei casi si tratta di CA autonome e i certificati da esse rilasciati sono considerati attendibili solo dai computer di tale organizzazione.In uno dei due tipi di CA sono disponibili due tipi di server CA.Server CA radice: il server CA radice firma il proprio certificato. Nella distribuzione PKI multilivello standard, la CA radice è offline e inaccessibile. La CA radice in questo modello rilascia inoltre certificati solo a un altro server CA noto come CA intermedia. Alcune aziende scelgono di utilizzare solo una CA a livello singolo. In questo modello, la CA radice emette certificati destinati a essere utilizzati da un'entità diversa da un altro server CA.Server CA intermedio - Il

server CA intermedio o emittente rilascia certificati destinati a essere utilizzati da un'entità diversa da un altro server CA.
- Microsoft Management Console (MMC) - Applicazione inclusa in Microsoft Windows che consente il caricamento di vari snap-in. È possibile utilizzare gli snap-in per creare una console personalizzata per l'amministrazione del server. In Windows sono disponibili diversi snap-in. Un breve elenco di esempi include Certificati, Gestione dispositivi, Gestione disco, Visualizzatore eventi e Servizi.
- Bilanciamento carico di rete: dispositivo o applicazione che presenta più risorse fisiche agli utenti finali con un nome fisico comune. Gli NLB sono molto comuni con le applicazioni e i servizi Web. Gli NLB possono essere implementati in molti modi. Se utilizzato con ECE, Bilanciamento carico di rete deve essere configurato in modo da garantire che le sessioni utente ritornino allo stesso server Web back-end fisico utilizzando cookie-insert o un metodo equivalente. Questa sessione è denominata sessione permanente con cookie-insert. Per sessione sticky si intende semplicemente la capacità di un load balancer di restituire la sessione di un utente allo stesso server back-end fisico per tutte le interazioni. Secure Sockets Layer (SSL) Passthrough - SSL passthrough è un metodo in cui la sessione SSL esiste tra il dispositivo dell'utente finale e il server Web fisico a cui è stata assegnata la sessione dell'utente. La passthrough SSL non consente l'inserimento di cookie poiché la sessione HTTP è sempre crittografata fisicamente. La maggior parte dei bilanciamenti del carico di rete supporta la sessione permanente con SSL Passthrough tramite tabelle di controllo che controllano la parte relativa a serverhello e clienthello dell'impostazione della sessione e memorizzano i valori univoci in una tabella. Quando la richiesta successiva che corrisponde a questi valori viene presentata a Bilanciamento carico di rete, è possibile utilizzare la tabella stick per restituire la sessione allo stesso server back-end.Offload SSL: quando Bilanciamento carico di rete è configurato per lo offload SSL, esistono due sessioni o tunnel SSL per ogni sessione utente finale. La prima è tra il dispositivo dell'utente finale e l'indirizzo IP virtuale (VIP) configurato in Bilanciamento carico di rete per il sito Web. Il secondo si trova tra l'indirizzo IP back-end di Bilanciamento carico di rete e il server Web fisico a cui è assegnata la sessione dell'utente. L'offload SSL supporta l'inserimento di cookie, in quanto il flusso HTTP viene completamente decrittografato mentre è attivo Bilanciamento carico di rete, in cui è possibile inserire ulteriori cookie HTTP ed eseguire l'ispezione della sessione. L'offload SSL viene spesso utilizzato quando l'applicazione Web non richiede SSL ma viene invece eseguito per motivi di sicurezza. Le versioni correnti di ECE non supportano l'accesso all'applicazione in una sessione non SSL.

Passi prerequisiti

Prima di iniziare l'integrazione dei due sistemi, è necessario completare alcuni prerequisiti.

- Livello di patch PCCE minimo Versione 12.0(1) - ES37Versione 12.5(1) - Nessun minimo corrente per la funzionalità di base
  La funzionalità Webex Experience Management (WXM) Analyzer richiede ES7
- Livello patch ECE minimo Èconsigliabile che gli ECE eseguano il più recente Programma speciale di progettazione (ES) disponibile.Versione 12.0(1) - ES3 + ES3_ET1aVersione 12.5(1) - Nessun minimo corrente per la funzionalità di base
  La funzionalità WXM Analyzer richiede ES1
- Elementi di configurazione Accertarsi di associare i domini di routing dei supporti (MRD)

ECE_Email, ECE_Chat ed ECE_Outbound all'istanza corretta dell'applicazione.Per il modello di distribuzione dell'agente PCCE 2000, l'istanza dell'applicazione è MultiChannel.Per il modello di distribuzione dell'agente PCCE 4000/12000, l'istanza dell'applicazione è nel formato {site}_{peripheral_set}_{application_instance}.
Se PCCE è stato installato con il nome del sito come Principale, la periferica impostata come PS1 e l'istanza dell'applicazione come Multicanale, il nome dell'istanza dell'applicazione è Main_PS1_Multichannel.**Nota:** Il nome dell'istanza dell'applicazione fa distinzione tra maiuscole e minuscole. Accertarsi di digitare correttamente il nome quando si aggiunge il server Web ECE all'inventario.

Fasi di integrazione

I dettagli relativi a tutti i passaggi descritti in questo documento sono descritti nella documentazione sia per ECE che per PCCE, ma non sono riportati in un elenco e non sono contenuti nello stesso documento. Per ulteriori informazioni, fare riferimento ai link riportati alla fine di questo documento.

Passaggio 1. Configurare i certificati SSL

Ènecessario generare un certificato che verrà utilizzato dal server Web ECE. È possibile utilizzare un certificato autofirmato, ma spesso è più semplice utilizzare un certificato firmato dalla CA. I certificati autofirmati non sono meno sicuri dei certificati firmati dall'autorità di certificazione, sono disponibili meno passaggi per la creazione iniziale del certificato, ma quando è necessario sostituire il certificato, è necessario ricordarsi di caricare il nuovo certificato nei keystore Java in tutti i server dati di amministrazione PCCE. Se si utilizza un certificato firmato da un'autorità di certificazione, è necessario caricare solo i certificati radice e, se presenti, i certificati intermedi nei keystore.

Se nella distribuzione sono presenti più server Web, è necessario rivedere queste linee guida. I passaggi specifici necessari per configurare un servizio di bilanciamento del carico di rete non rientrano nell'ambito di questo documento. Se necessario, contattare il fornitore del servizio di bilanciamento del carico.

Sebbene non sia necessario, un load balancer semplifica notevolmente l'implementazione

L'accesso all'applicazione ECE su ogni server Web deve utilizzare SSL indipendentemente dal metodo di bilanciamento del carico utilizzato

Il servizio di bilanciamento del carico può essere configurato come passthrough SSL o offload SSL

Se si sceglie SSL passthrough, è necessario procedere come segue: È necessario eseguire tutte le operazioni sui certificati da un server

Dopo aver configurato correttamente il certificato, è necessario esportarlo e verificare che la chiave privata sia inclusa in un file PFX (Personal Information Exchange)

Ènecessario copiare il file PFX in tutti gli altri server Web della distribuzione, quindi importare il certificato in IIS

Se si sceglie l'offload SSL, ogni server Web può essere configurato con il proprio certificato SSL

> **Nota:** Se si dispone di più server Web e si sceglie SSL pass-through sul server Web o se si desidera avere un certificato comune su tutti i server, è necessario scegliere un server Web per eseguire il passaggio 1 su, quindi importare il certificato su tutti gli altri server Web. Se si sceglie offload SSL, è necessario eseguire la procedura seguente in tutti i server Web. È inoltre necessario generare un certificato da utilizzare nel servizio di bilanciamento del carico.

Passaggio 1.1. Generare un certificato

Èpossibile ignorare questa sezione se è già stato creato o ottenuto un certificato, altrimenti scegliere una delle due opzioni.

Opzione 1. Utilizzare un certificato autofirmato

1. Passare ad Amministrazione IIS.
2. Selezionare il nome del server nella struttura Connessioni a sinistra.
3. Individuare **Certificati server** nel riquadro centrale e fare doppio clic per aprirlo.
4. Selezionare **Crea certificato autofirmato...** dal riquadro Azioni a destra.
5. Nella finestra **Crea certificato autofirmato**, scegliere e immettere un nome in **Specificare un nome descrittivo per il certificato:** casella. Questo nome indica la modalità di visualizzazione del certificato nel processo di selezione nel passaggio principale successivo. Questo nome non deve necessariamente corrispondere al nome comune del certificato e non influisce sulla modalità di visualizzazione del certificato per l'utente finale.
6. Verificare che sia selezionato **Personale** nell'**archivio Selezionare un certificato per il nuovo certificato:** casella a discesa.
7. Selezionare **OK** per creare il certificato.
8. Procedere al passaggio principale successivo, **Associare il certificato al sito Web**.

Opzione 2. Utilizzare un certificato firmato dalla CA

I certificati firmati dalla CA richiedono la generazione di una richiesta di firma del certificato (CSR). Il CSR è un file di testo che viene quindi inviato alla CA in cui è firmato, quindi vengono restituiti il certificato firmato e i certificati CA richiesti e il CSR viene soddisfatto. È possibile scegliere di eseguire questa operazione tramite Amministrazione IIS o Microsoft Management Console (MMC). Il metodo di amministrazione di IIS è molto più semplice, senza necessità di conoscenze speciali, ma consente solo di configurare i campi inclusi nell'attributo Subject del certificato e di modificare la lunghezza in bit. MMC richiede operazioni aggiuntive e garantisce una conoscenza approfondita di tutti i campi richiesti in un CSR valido. Si consiglia di utilizzare MMC solo se si dispone di un'esperienza di livello moderato o esperto nella creazione e nella gestione dei certificati. Se la distribuzione richiede che sia possibile accedere a ECE con più nomi completi o se è necessario modificare qualsiasi parte del certificato ad eccezione dell'oggetto e della lunghezza in bit, è necessario utilizzare il metodo MMC.

1. Tramite Amministrazione IIS Utilizzare la procedura seguente per generare una richiesta di firma del certificato (CSR) tramite Gestione IIS.Passare ad Amministrazione IIS.Selezionare

il nome del server nella struttura Connessioni a sinistra.Individuare **Certificati server** nel riquadro centrale e fare doppio clic per aprirlo.Selezionare **Crea richiesta certificato...** dal riquadro Azioni a destra. Verrà visualizzata la **Richiesta guidata certificato**.Nella pagina **Proprietà nome distinto** immettere i valori nel modulo per il sistema in uso. È necessario immettere tutti i campi. Scegliere **Avanti** per continuare.Nella pagina **Proprietà provider del servizio di crittografia** lasciare invariata la selezione predefinita per **Provider del servizio di crittografia:**. Modificare la **lunghezza** del **bit:** a un minimo di **2048**. Scegliere **Avanti** per continuare.Nella pagina **Nome file** selezionare la posizione in cui si desidera salvare il file CSR.Fornire il file alla CA. Dopo aver ricevuto il certificato firmato, copiarlo sul server Web e procedere al passaggio successivo.Nella stessa posizione in Gestione IIS, selezionare **Completa richiesta certificato** nel riquadro **Azioni**. Verrà visualizzata la procedura guidata.Nella pagina **Specifica risposta Autorità di certificazione** scegliere il certificato fornito dalla CA. Assegnare un nome nella casella **Nome descrittivo**. Questo nome indica la modalità di visualizzazione del certificato nel processo di selezione nel passaggio principale successivo. Verificare che nell'area **Selezionare un archivio certificati per il nuovo certificato:** è impostato su **Personale**.Selezionare **OK** per completare il caricamento del certificato.Procedere al passaggio principale successivo, **Associare il certificato al sito Web**.

2. Tramite Microsoft Management Console (MMC) Per generare un CSR tramite MMC, eseguire la procedura seguente. Questo metodo consente di personalizzare ogni aspetto del CSR.Fare clic con il pulsante destro del mouse sul pulsante Start e selezionare Esegui.Digitate **mmc** nella casella run e selezionate **OK**.Aggiungere lo snap-in Certificato alla finestra di MMC. Selezionare **File**, quindi **Aggiungi/Rimuovi snap-in...**. Verrà visualizzata la casella **Aggiungi o rimuovi snap-in**.Nell'elenco a sinistra, individuare **Certificati** e selezionare **Aggiungi >**. Verrà visualizzata la casella Snap-in certificati.Selezionare l'opzione **Account computer,** quindi selezionare **Avanti >**.Verificare che il **computer locale: (il computer su cui si trova questa console)** è selezionato nella pagina **Seleziona computer**, quindi selezionare **Fine**.Selezionare **OK** per chiudere la casella **Aggiungi o rimuovi snap-in**.Genera CSR Nel riquadro sinistro espandere **Certificati (computer locale)** quindi **Personale** e selezionare la cartella **Certificati**.Fare clic con il pulsante destro del mouse sulla cartella **Certificati** e selezionare **All Tasks > Advanced Operations >** quindi selezionare **Create Custom Request...**. Verrà visualizzata la procedura guidata **Registrazione certificato**.Selezionare **Avanti** nella schermata di introduzione.Nella pagina **Selezione criterio di registrazione certificati** selezionare **Procedi senza criterio di registrazione**, elencato in **Richiesta personalizzata**, quindi selezionare **Avanti**.Nella pagina **Richiesta personalizzata**, verificare che il **modello** selezionato sia **(Nessun modello) chiave CNG** e che il **formato della richiesta** sia appropriato per la CA in uso. **PKCS #10** funziona con la CA Microsoft. Selezionare **Successivo** per passare alla pagina successiva.Nella pagina **Informazioni certificato** selezionare l'elenco a discesa accanto alla parola **Dettagli**, quindi scegliere il pulsante **Proprietà**. Verrà visualizzato il modulo **Proprietà certificato**.Non è nell'ambito di questo documento fornire tutte le opzioni per il modulo **Proprietà certificato**. Per ulteriori informazioni, consultare la documentazione Microsoft. Di seguito sono riportate alcune note e alcuni suggerimenti relativi a questo modulo. Assicurarsi di popolare tutti i valori obbligatori nel **nome soggetto:** sezione della **materia:** schedaAssicurarsi che il valore fornito per **Nome comune** sia incluso anche in **Nome alternativo:** sezioneImpostare il **tipo:** per **DNS**, digitare l'URL nel campo **Valore:** , quindi selezionare il pulsante **Add**Se si desidera utilizzare più URL per accedere ad ECE, fornire ciascun nome alternativo in questo campo e selezionare **Add >** dopo ciascunaAssicurarsi di impostare le **dimensioni** della **chiave** nella scheda **Chiave privata** su un valore maggiore di 1024.Se si prevede di esportare il certificato per utilizzarlo

su più server Web, come spesso avviene in un'installazione a disponibilità elevata, assicurarsi di selezionare **Rendi esportabile la chiave privata**. In caso contrario, non sarà possibile esportare il certificato in un secondo momentoI valori immessi e le selezioni effettuate non vengono convalidati. È necessario accertarsi di fornire tutte le informazioni necessarie o che l'autorità di certificazione non sia in grado di completare il CSRDopo aver effettuato tutte le selezioni, **OK** per tornare alla procedura guidata. Selezionare **Successivo** per passare alla pagina successiva.In **Dove si desidera salvare la richiesta offline?** selezionare un nome file in una posizione accessibile. Per la maggior parte delle CA, selezionare **Base 64** come formato.Fornire il file alla CA. Dopo averlo firmato e averti restituito il certificato, copiarlo sul server Web e procedere con gli ultimi passaggi.Nello snap-in Gestione certificati per MMC passare a **Certificati (computer locale) > Personali**, fare clic con il pulsante destro del mouse su **Certificati** e scegliere **Tutte le attività > Importa...**. Verrà visualizzata l'**Importazione guidata certificati**.Selezionare **Avanti** nella schermata introduttiva.Nella schermata **File da importare** selezionare il certificato firmato dalla CA, quindi scegliere **Avanti**.Assicurarsi di selezionare **Inserisci tutti i certificati nel seguente archivio**.Verificare che nell'**archivio certificati** sia selezionato **Personale:** , quindi scegliere **Avanti**.Esaminare la schermata finale, quindi selezionare **Finish** (Fine) per completare l'importazione.Èora possibile chiudere la console MMC. Se viene richiesto di salvare le impostazioni della console, è possibile selezionare **No**. Ciò non influisce sull'importazione del certificato.Procedere al passaggio principale successivo, **Associare il certificato al sito Web**.

Passaggio 1.2. Associazione del certificato al sito Web

Attenzione: Assicurarsi che il campo hostname sia lasciato vuoto e che l'opzione Require Server Name Indication non sia selezionata nella casella Modifica associazione sito. Se uno di questi è configurato, SPOG fallisce quando tenta di comunicare con ECE

1. Aprire Gestione Internet Information Services (IIS) se non è già stato fatto in precedenza.
2. Nel riquadro **Connessioni** a sinistra passare a **Siti** e selezionare **Sito Web predefinito**. Se si sceglie di utilizzare un nome di sito diverso da Sito Web predefinito, assicurarsi di selezionare il nome del sito corretto.
3. Selezionare **Associazioni...** dal riquadro **Azioni** a destra. Verrà visualizzata la casella **Associazioni sito**. Se non è presente una riga con **Type**, **https** e **Port**, **443**, attenersi alla seguente procedura. In caso contrario, procedere al passaggio principale successivo. Selezionare il pulsante **Aggiungi...** per visualizzare la casella **Aggiungi associazione sito**.Selezionare **https** nel campo **Type:** a discesa.Verificare che l'**indirizzo IP:** L'elenco a discesa mostra **All Unassigned** (Tutti non assegnati) e la **porta:** è **443**.Accertarsi di lasciare invariato il **nome** dell'**host:** vuoto e l'opzione **Richiedi indicazione nome server** non è selezionata.Nel **certificato SSL:** selezionare il nome del certificato corrispondente a quello creato in precedenza. Se non si è certi del certificato da scegliere, utilizzare il pulsante **Seleziona...** per visualizzare e cercare i certificati presenti sul serverUtilizzare il pulsante **Visualizza...** per visualizzare il certificato scelto e verificare che i dettagli siano correttiSelezionare **OK** per salvare la selezione.Selezionare la riga che mostra **https** nella colonna Type, quindi selezionare il pulsante **Edit...**. Verrà visualizzata la casella **Modifica associazione sito**. Verificare che l'**indirizzo IP:** L'elenco a discesa mostra **All Unassigned** (Tutti non assegnati) e la **porta:** è **443**.Verificare che il **nome** dell'**host:** è stato lasciato vuoto e l'opzione **Richiedi indicazione nome server** non è selezionata.Nel **certificato SSL:** selezionare

il nome del certificato corrispondente a quello creato in precedenza. Se non si è certi del certificato da scegliere, utilizzare il pulsante **Seleziona...** per visualizzare e cercare i certificati presenti sul serverUtilizzare il pulsante **Visualizza...** per visualizzare il certificato scelto e verificare che i dettagli siano correttiSelezionare **OK** per salvare la selezione.Selezionare **Chiudi** per tornare a Gestione IIS.

4. Èora possibile chiudere Gestione IIS.

Passaggio 2. Configurare l'SSO dell'amministratore della partizione

La configurazione SSO di Amministrazione partizioni consente a ECE di creare automaticamente un account utente a livello di partizione per qualsiasi amministratore che apra il gadget ECE in SPOG.

> **Nota:** È necessario configurare l'SSO dell'amministratore delle partizioni anche se non si intende abilitare l'SSO dell'agente o del supervisore.

Passaggio 2.1. Ottenere il certificato di Active Directory (AD) e creare l'archivio chiavi.

Questo passaggio è necessario per risolvere le recenti modifiche alla sicurezza annunciate da Microsoft.

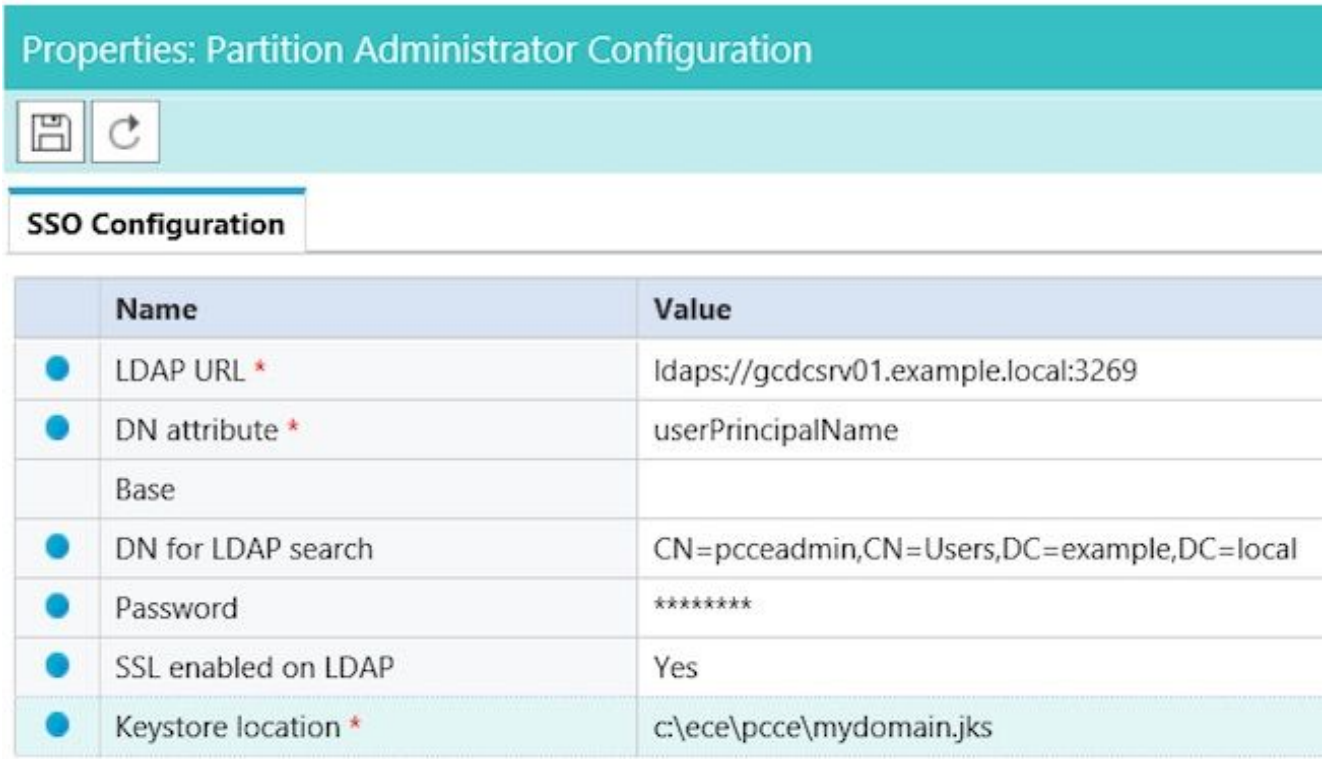
Per maggiori informazioni, visitare il sito https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows.

1. Ottenere dal server AD il certificato SSL in formato Base 64 fornito nel modulo Configurazione amministratore partizioni.
2. Copiare il file del certificato in uno dei server applicazioni.
3. Aprire una sessione RDP nel server applicazioni in cui è stato copiato il certificato.
4. Creare un nuovo keystore Java come indicato di seguito. Aprire un prompt dei comandi sul server applicazioni.Passate alla directory bin ECE Java Development Kit (JDK).Eseguire questo comando. Sostituire i valori appropriati.
   keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c:\ece\pcce\mydomain.jks -storepass MyP@ssword
5. Copiare il keystore nello stesso percorso in tutti gli altri Application Server dell'ambiente.

Passaggio 2.2. Configurare ECE con le informazioni di accesso LDAP (Lightweight Directory Access Protocol) di AD.

1. Da una workstation o da un computer con **Internet Explorer 11**, passare all'URL della partizione Business. **Suggerimento**: La partizione business è anche nota come partizione 1. Per la maggior parte delle installazioni, è possibile accedere alla partizione business tramite un URL simile a https://ece.example.com/default.
2. Accedere come **pa** e fornire la password per il sistema.
3. Dopo aver eseguito correttamente l'accesso, selezionare il collegamento **Amministrazione** sulla console iniziale.
4. Passare alla cartella **Configurazione SSO** come indicato di seguito, **Amministrazione > Partizione: impostazione predefinita > Protezione > SSO e provisioning**.

5. Nel riquadro superiore a destra, selezionare la voce **Partition Administration Configuration**.
6. Nel riquadro inferiore a destra, immettere i valori per LDAP (Lightweight Directory Access Protocol) e AD. **URL LDAP** - È buona norma utilizzare il nome di un controller di dominio del catalogo globale (GC).
   Se non si utilizza un catalogo globale, è possibile che venga visualizzato un errore nei registri di Application Server come indicato di seguito.
   Eccezione nell'autenticazione LDAP <@>
   javax.naming.PartialResultException: riferimenti di continuazione non elaborati; nome rimanente 'DC=esempio,DC=com' La porta del catalogo globale non protetta è 3268La porta Secure Global Catalog è 3269**Attributo DN** - Deve essere userPrincipalName.**Base**: non è necessario se si utilizza un catalogo globale. In caso contrario, è necessario fornire il formato LDAP corretto della base.**DN per ricerca LDAP** - A meno che il dominio non consenta l'associazione anonima, è necessario fornire il nome distinto di un utente con la possibilità di eseguire l'associazione a LDAP ed eseguire la ricerca nella struttura di directory.
   Suggerimento - Il modo più semplice per trovare il valore corretto per l'utente consiste nell'utilizzare lo strumento Utenti e computer di Active Directory. Attivare **Funzioni avanzate** nel menu **Visualizza**.Passare all'oggetto utente, quindi fare clic con il pulsante destro del mouse e scegliere **Proprietà**.Selezionare la scheda **Attributi**.Selezionare il pulsante **Filtro**, quindi selezionare **Mostra solo attributi con valori**.Individuare **distinquishedName** nell'elenco, quindi fare doppio clic per visualizzare il valore.Evidenziare il valore visualizzato, quindi copiarlo e incollarlo in un editor di testo.Copiare e incollare il valore dal file di testo nel campo di **ricerca DN per LDAP**.
   Il valore deve essere simile a, CN=pcceadmin, CN=Users, DC=esempio, DC=local**Password** - A meno che il dominio non consenta l'autenticazione anonima, è necessario fornire la password per l'utente specificato.**SSL abilitato su LDAP** - Questo campo deve essere considerato obbligatorio per la maggior parte dei clienti.**Percorso keystore** - Indica il percorso del keystore in cui è stato importato il certificato SSL da Active Directory. Nell'esempio, questo valore è c:\ece\pcce\mydomain.jks, come mostrato nell'immagine:



7. Selezionare l'icona del disco floppy per salvare le modifiche.

Passaggio 3. Convalida del file di configurazione

Il completamento di questa sezione è obbligatorio per tutte le installazioni della versione 12.0. Per qualsiasi versione diversa dalla 12.0, è possibile ignorare questa sezione.
Esistono due scenari aggiuntivi con tutte le versioni in cui questo passaggio può essere richiesto. La prima si verifica quando ECE è stato installato in un ambiente ad alta disponibilità. Il secondo caso, più comune, si verifica quando il nome host del server Web non corrisponde al nome utilizzato per accedere a ECE. Ad esempio, se si installa il server Web ECE su un server con il nome host UCSVRECEWEB.example.com, ma gli utenti accedono alle pagine Web ECE con l'URL chat.example.com, è necessario completare questa sezione. Se il nome host del server e l'URL con cui si accede ad ECE sono gli stessi e se è stata installata la versione 12.5 o successiva, è possibile saltare questo passaggio e completare la sezione.

Sostituire {ECE_HOME} con il percorso fisico in cui è installato ECE. Ad esempio, se avete installato ECE in **C:\Cisco**, sostituite {ECE_HOME} con **C:\Cisco** in ciascuna posizione.

> **Suggerimento**: Utilizzare un editor di testo quale Blocco note++ anziché Blocco note o Wordpad in quanto questi non interpretano correttamente le terminazioni della riga.

1. Aprire una sessione di desktop remoto in tutti i server Web ECE dell'installazione.
2. Passare al percorso **{ECE_HOME}\eService\templates\finesse\gadget\spog**.
3. Individuare il file **spog_config.**jsfile e creare una copia di backup in un percorso sicuro.
4. Aprite il file **spog_config.**jscorrente in un editor di testo.
5. Individuare queste due righe e aggiornarle in base alla distribuzione.
   Il valore di web_server_protocol deve essere https, aggiornarlo se necessario.
   Aggiornate web_server_name in modo che corrisponda al nome completo che avete allocato per accedere a ECE. Esempio: **ece.example.com** var web_server_protocol = "https";var nome_server_web = "ece.example.com";
6. Salvare le modifiche.
7. Ripetere l'operazione su tutti gli altri server Web della distribuzione.

Passaggio 4. Aggiungere ECE all'inventario PCCE

A partire dalla versione 12.0, PCCE dispone di tre diverse opzioni di implementazione: agente 2000 (agente 2K), agente 4000 (agente 4K) e agente 12000 (agente 12K). Queste tre opzioni di implementazione possono essere suddivise in due gruppi, l'agente 2K e l'agente 4K/12K. Sono separati in questo modo perché ci sono diverse differenze fondamentali nel modo in cui appaiono in SPOG. In questo paragrafo è illustrato un confronto molto approfondito tra i due metodi. In questo documento non vengono fornite istruzioni specifiche per aggiungere un componente al magazzino. Per i dettagli specifici su questo processo, consultare i link alla fine di questo documento. In questa sezione vengono illustrati dettagli specifici che è necessario verificare quando si aggiunge ECE a PCCE. Nel documento si presume inoltre che l'installazione di PCCE sia completa e che sia possibile accedere e configurare altri aspetti della soluzione.

- Installazione agente 2K La configurazione iniziale dei componenti PCCE viene eseguita interamente tramite Amministrazione CCE ed è automatizzataI nuovi componenti vengono aggiunti nella pagina Inventory mediante una casella popup in cui è possibile immettere dettagli quali l'indirizzo IP o il nome host e le credenziali necessarie o la configurazione

specifica del componente
- Installazione di agenti 4K e 12K La maggior parte della configurazione iniziale riflette i passaggi utilizzati per UCCEI componenti vengono aggiunti tramite un file CSV (Comma-Separated Values) scaricato dall'amministrazione CCE, compilato in base all'installazione specifica, quindi caricatoLa distribuzione iniziale richiede l'inclusione di alcuni componenti specifici nel primo file CSVI componenti che non sono stati aggiunti durante la configurazione iniziale del sistema vengono aggiunti tramite file CSV contenenti le informazioni richieste

Passaggio 4.1. Caricamento del certificato server Web ECE nel keystore Java

1. Se vengono utilizzati certificati autofirmati Aprire una connessione desktop remoto al server dati di amministrazione (ADS, Administration Data Server) primario di lato A.Aprire Internet Explorer 11 come amministratore e passare alla partizione aziendale ECE.Selezionare l'icona di un lucchetto sul lato destro della barra dell'URL, quindi scegliere **Visualizza certificati**.Nella casella **Certificato** selezionare la scheda **Dettagli**.Selezionare **Copia su file...** nella parte inferiore della scheda.Nell' **Esportazione guidata certificati** selezionare **Avanti** fino a raggiungere la pagina **Formato file di esportazione**. Accertarsi di selezionare il formato **X.509 (.CER) con codifica Base 64**.Salvare il certificato in un percorso quale **c:\Temp\certificates** sul server ADS per completare l'esportazione.Copiare il certificato in tutti gli altri server ADS.Aprire un prompt dei comandi amministrativo.Passare alla directory home Java, quindi alla directory bin. È possibile accedere alla home directory Java con le seguenti operazioni. **cd %JAVA_HOME%\bin**Eseguire il backup del file **cacerts** corrente. Copiare il file **cacerts** da **%JAVA_HOME%\lib\security** in un'altra posizione.Eseguire questo comando per importare il certificato salvato in precedenza. Se la password del keystore non è "changeit", aggiornare il comando in modo che corrisponda all'installazione.
   keytool -keystore ../lib/security/cacerts -storepass changeit -import -alias <FQDN del server ECE> -file <Percorso in cui è stato salvato il certificato>Riavviare il server ADS.Ripetere i passaggi da 8 a 12 sugli altri server ADS.
2. Se vengono utilizzati certificati firmati dalla CA Ottenere il certificato radice e intermedio in formato DER/PEM e copiarli in un percorso quale **C:\Temp\certificates** su tutti i server ADS.
   Nota: Contattare l'amministratore della CA per ottenere questi certificati. Aprire una connessione desktop remoto all'annuncio pubblicitario principale lato A.Aprire un prompt dei comandi amministrativo.Passare alla directory home Java, quindi alla directory bin. È possibile accedere alla home directory Java con le seguenti operazioni. **cd %JAVA_HOME%\bin**Eseguire il backup del file **cacerts** corrente. Copiare il file **cacerts** da **%JAVA_HOME%\lib\security** in un'altra posizione.Eseguire questo comando per importare il certificato salvato in precedenza. Se la password del keystore non è "changeit", aggiornare il comando in modo che corrisponda all'installazione.
   keytool -keystore ../lib/security/cacerts -storepass changeit -trustcacerts -import -alias <Nome radice CA> -file <Percorso in cui è stato salvato il certificato radice>Ripetere il passaggio 6 e importare il certificato intermedio, se presente.Riavviare il server ADS.Ripetere le fasi da 2 a 12 su tutti gli altri server ADS.

Passaggio 4.2. Aggiunta del server dati ECE all'inventario

- Sebbene il server dati debba essere presente nell'inventario di sistema, non viene effettuata alcuna comunicazione diretta tra PCCE ADS e il server dati

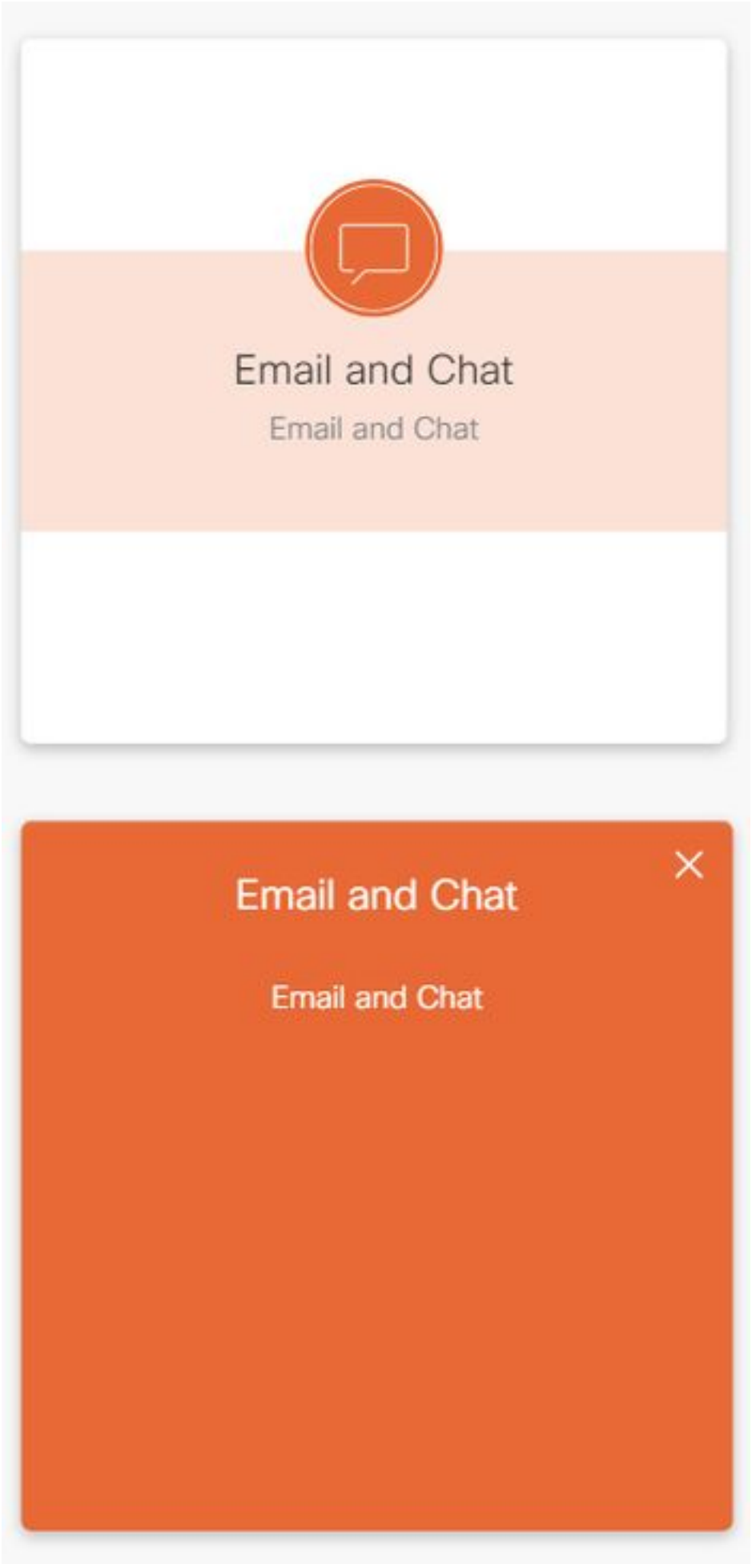
- Quando viene implementato un ECE nell'implementazione con 1500 agenti, il server dati è il server dei servizi
- Quando ECE viene installato in una configurazione HA, è necessario aggiungere entrambi i server dei servizi

Passaggio 4.3. Aggiunta del server Web ECE all'inventario

- Accertarsi di aggiungere il server Web con il nome completo Questo nome deve corrispondere al nome comune nel certificato ECE o deve essere elencato come uno dei nomi alternativi del soggetto (SAN)Non è necessario utilizzare solo il nome host o l'indirizzo IP
- Il nome utente e la password per ECE devono essere le credenziali di accesso PA
- Verificare che l'istanza dell'applicazione sia corretta Il nome dell'istanza dell'applicazione fa distinzione tra maiuscole e minuscolePer le distribuzioni PCCE dell'agente 2000, l'istanza dell'applicazione è MultiChannelPer le distribuzioni PCCE dell'agente 4000/12000, l'istanza dell'applicazione contiene il sito e il set di periferiche come parte del nome
- Quando ECE viene installato con più server Web, ad esempio nella distribuzione dell'agente 1500 o in una distribuzione di 400 Agent HA, è possibile utilizzare l'URL che punta al bilanciamento del carico o l'URL che punta a ogni singolo server Web come nome completo del server Web.
- Se si dispone di più di un'installazione ECE o se si sceglie di aggiungere ogni singolo server Web all'installazione con più di un'installazione, è consigliabile scegliere il server Web corretto quando si apre il gadget ECE in SPOG.

Passaggio 5. Integrare ECE con PCCE

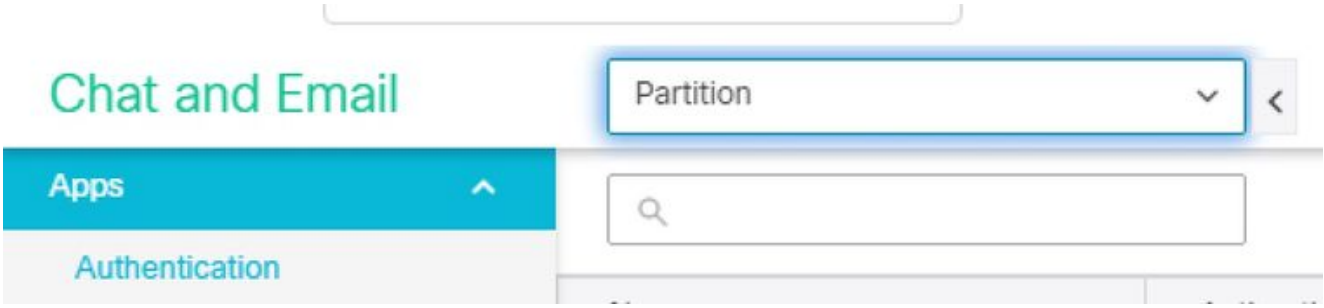
1. Accedere ad Amministrazione CCE come amministratore.
2. Selezionare la scheda **Email e Chat**, quindi il collegamento **Email e Chat** come mostrato nell'immagine.



3. Controllare il server selezionato nell'elenco a discesa Nome dispositivo. Se sono stati aggiunti entrambi i server Web in un'installazione HA, è possibile scegliere uno dei due

server Web. Se si aggiunge una seconda distribuzione ECE al sistema in un secondo momento, assicurarsi di selezionare il server appropriato prima di continuare.

4. Nell'elenco a discesa accanto a **Chat ed e-mail**, selezionare **Partition** (Partizione) o **Global** (Globale), come mostrato nell'immagine.



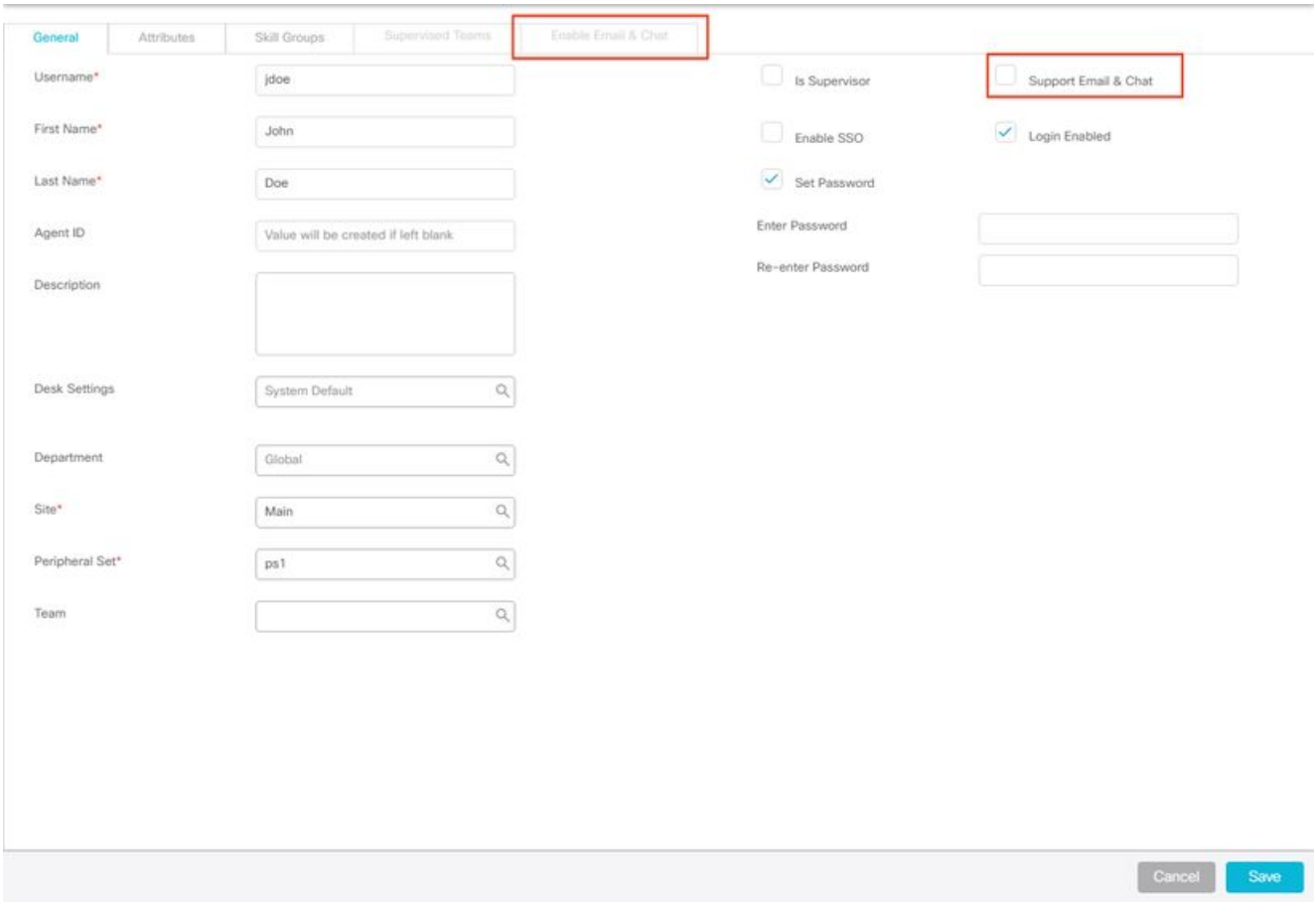
5. Nel menu superiore, selezionare **Integration**, quindi fare clic sulla freccia accanto a **Unified CCE** e selezionare il secondo **Unified CCE** come mostrato nell'immagine.

6. Inserire i valori nella scheda **Dettagli AWDB** per l'installazione, quindi selezionare il pulsante **Salva**.
7. Selezionare la scheda **Configuration** (Configurazione) e completare l'operazione come indicato di seguito. Selezionare l'elenco a discesa accanto a **Istanza applicazione** e selezionare l'Istanza applicazione creata per ECE. **Nota:** Non deve essere l'istanza dell'applicazione che inizia con UQ.Selezionare il cerchio verde con il pulsante del segno più bianco selezionare Agent PG. Selezionare l'agente PG (o l'agente PG se ne esistono più di uno).Selezionare **Save** (Salva) dopo aver aggiunto tutte le pagine PG dell'agente. **Avviso:** Una volta selezionato **Save**, il sistema è connesso in modo permanente al PCCE e non può essere annullato. Se si verificano errori in questa sezione, è necessario disinstallare completamente ECE ed eliminare tutti i database, quindi installare ECE come se si trattasse di una nuova installazione.

Passaggio 6. Convalida integrazione ECE

1. In Amministrazione CCE, verificare che nella barra di stato superiore non siano visualizzati avvisi. Se sono presenti avvisi, selezionare la parola **Avvisi** ed esaminare la pagina Inventario per verificare che non siano presenti avvisi per i server ECE.
2. Selezionare **Utenti**, quindi **Agenti** nella barra di navigazione a sinistra.
3. Selezionare un agente dall'elenco e verificarlo. A questo punto dovrebbe essere visualizzata una nuova casella di controllo per **Supporto e-mail e chat** nella scheda **Generale**.A questo punto dovrebbe essere visualizzata una nuova scheda con l'etichetta **Abilita e-mail e chat** ,

come mostrato nell'immagine.



4. Attivare un agente di prova per ECE. Selezionare la casella di controllo **Supporto e-mail e chat** e notare che è possibile selezionare la scheda **Abilita e-mail e chat**.Selezionare la scheda **Abilita e-mail e chat** e specificare il valore nel campo **Nome schermata**.Selezionare **Salva** per aggiornare l'utente.Dovresti ricevere un messaggio di operazione riuscita.
5. Verificare che ECE sia stato aggiornato. Selezionare il pulsante di navigazione **Panoramica**, quindi selezionare la scheda **E-mail e chat** e il collegamento.Nell'elenco a discesa accanto a **Chat ed e-mail**, selezionare il nome che corrisponde al reparto dell'agente. **Nota:** Il reparto Assistenza in ECE contiene tutti gli oggetti appartenenti al reparto Globale in PCCE. Il nome di reparto Servizio è pertanto un valore riservato.Nel menu superiore, selezionare **Gestione utenti**, quindi selezionare **Utenti** nel menu sotto **Chat ed Email**.Verificare che il nuovo agente sia presente nell'elenco.

Risoluzione dei problemi

Si consiglia di scaricare diversi strumenti e di conservarli sui server ECE. Ciò semplifica notevolmente la risoluzione dei problemi e la manutenzione della soluzione nel tempo.

- Un editor di testo come Blocco note++
- Uno strumento di archiviazione come 7-Zip
- Uno dei numerosi programmi Tail per Windows
  Alcuni esempi sono: Baretail -https://www.baremetalsoft.com/baretail/Tail per Win32 - http://tailforwin32.sourceforge.net/

Per risolvere i problemi relativi all'integrazione, è innanzitutto necessario conoscere alcuni file di log delle chiavi e la posizione di ciascuno di essi.

1. ## Nomi file e posizioni su ECE

   Ci sono molti log sul sistema ECE, questi sono solo quelli che sono più utili quando si cerca di risolvere un problema con l'integrazione.

   Chiave server:C = server collocatoA = Server applicazioniS = Server dei serviziM = Server di messaggisticaLa maggior parte dei file di log dispone inoltre di altri due log associati.eg_log_{SERVERNAME}_{PROCESS}.log - Registro processo primarioeg_log_dal_connpool_{SERVERNAME}_{PROCESS}.log - Utilizzo del connection pooleg_log_query_timeout_{SERVERNAME}_{PROCESS}.log - Aggiornato quando una query ha esito negativo a causa di un timeout
2. ## Nomi file e percorsi su PCCE

   I registri PCCE per i problemi di integrazione si trovano tutti sul lato A di ADS. Di seguito sono elencati i registri più importanti per la risoluzione dei problemi di integrazione. Ognuna di queste si trova in, **C:\icm\tomcat\logs**.

   Di questi registri, i primi tre sono i più richiesti e rivisti.Utilizzare la procedura seguente per impostare i livelli di traccia e raccogliere i registri necessari.
3. **Configurazione livello traccia**La presente sezione si applica solo all'ECE. Il livello di traccia dei log richiesti da PCCE è impostato da Cisco e non può essere modificato. Da una workstation o da un computer con **Internet Explorer 11**, passare all'URL della partizione di sistema. **Suggerimento**: La partizione di sistema è nota anche come partizione 0. Per la maggior parte delle installazioni, è possibile accedere alla partizione di sistema tramite un URL simile a https://ece.example.com/systemAccedere come **sa** e fornire la password per il sistema.Dopo aver eseguito correttamente il login, selezionare il collegamento **System** sulla console iniziale.Nella pagina Sistema, espandere **Sistema > Risorse condivise > Logger > Processi**.Nel riquadro superiore destro individuare il processo che si desidera modificare il livello di traccia e selezionarlo.
   Nota: In un sistema HA e in un sistema con più di un server applicazioni, i processi sono elencati più di una volta. Per assicurarsi di acquisire i dati, impostare il livello di traccia per tutti i server che contengono il processo.Nel riquadro inferiore destro selezionare l'elenco a discesa **Livello di traccia massimo** e quindi il valore appropriato.
   In ECE sono definiti 8 livelli di traccia. I 4 in questo elenco sono quelli utilizzati più di frequente. 2 - Errore - Livello di traccia predefinito per i processi4 - Informazioni - Livello di traccia generalmente utilizzato per la risoluzione dei problemi6 - Dbquery - Spesso utile per diagnosticare i problemi all'inizio della configurazione o problemi più complessi7 - Debug - Output molto dettagliato, richiesto solo nei problemi più complessi**Nota:** Nessun processo deve essere mantenuto al livello di 6 - Dbquery per un periodo di tempo prolungato e in

genere solo con la guida del TAC.La maggior parte dei processi deve rimanere a livello di traccia, 2-Error. Se si seleziona il livello 7 o 8, è necessario selezionare anche una durata massima. Quando viene raggiunta la durata massima, il livello di traccia torna all'ultimo livello impostato.
Una volta configurato il sistema, modificare questi quattro processi in trace level 4.Processo EAASEAMS-processprocesso dxrx-processSelezionare l'icona Salva per impostare il nuovo livello di traccia.

4. Raccolta file di log

Aprire una sessione di Desktop remoto nel server in cui sono necessari i registri del processo.Passare al percorso del file di log. Server ECE I log vengono scritti come segue.Per impostazione predefinita, i registri sono file scritti con una dimensione massima di 5 MBQuando un file di log raggiunge il valore massimo configurato, viene rinominato nel formato {LOGNAME}.log.{#}L'ECE conserva i 49 file di log precedenti più il file correnteIl registro corrente termina sempre con.log e senza numero dopoI registri non sono né archiviati né compressiLa maggior parte dei registri ha una struttura comuneI file di log utilizzano <@> per separare le sezioniI registri vengono sempre scritti nel tempo GMT+0000I registri ECE si trovano in posizioni diverse in base all'installazione specifica.400 distribuzioni di agenti Su un lato Server: Server collocatoPercorso: **{ECE_HOME}\eService_RT\logs**Alta disponibilità Server: Entrambi i server collocatiPercorso: **{ECE_HOME}\eServizio\log**La directory creata per la condivisione DFS contiene solo i registri per l'installazione e gli aggiornamenti.Solo il server proprietario del ruolo DSM (Distributed Systems Manager) scrive i log per i componenti che fanno parte del ruolo Servizi Il proprietario del ruolo DSM è disponibile nella scheda Processi di Gestione attività Windows. Su questo server sono presenti 10-15 processi Java che non si trovano sul server secondario.I componenti di DSM includono EAS, EAMS, Retriever, Dispatcher, Workflow, ecc.1500 Agent Deployment Registri nel server che ospita il ruoloPercorso: **{ECE_HOME}\eServizio\log**Ad eccezione del server dei servizi, tutti i server funzionano e scrivono i log per tutti i processi associati al componenteIn un'implementazione ad alta disponibilità, il server dei servizi opera in una configurazione attiva/standbyI registri vengono scritti solo dal server proprietario del ruolo DSM (Distributed Systems Manager)Il proprietario del ruolo DSM può essere identificato dal numero di processi visualizzati in Gestione attività Windows. Sul server principale sono in esecuzione da 10 a 15 processi Java, mentre sul server secondario sono in esecuzione solo 4 processi JavaServer PCCE I log richiesti da PCCE si trovano in, **C:\icm\tomcat\logs**I log Tomcat non vengono riportati né archiviatiI registri vengono scritti all'ora del server localeRaccogliere tutti i log creati o modificati dopo l'analisi del problema.
Una spiegazione completa dei registri e dei problemi riscontrati esula tuttavia dalle finalità del presente documento. Di seguito sono riportati alcuni problemi comuni, gli elementi da esaminare e alcune possibili soluzioni. Problemi correlati ai certificati Certificato non importato Comportamento: Quando si tenta di aprire il gadget ECE in SPOG, viene visualizzato l'errore "Si è verificato un errore durante il caricamento della pagina. Contattare

l'amministratore."Verifica: Catalina esegue l'accesso a PCCE per errori simili a questi javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: Compilazione del percorso PKIX non riuscita: sun.security.provider.certpath.SunCertPathBuilderException: impossibile trovare un percorso di certificazione valido per la destinazione richiestaRisoluzione: Verificare di aver importato il certificato server Web ECE o i certificati CA appropriati nel keystore di ADSCertificato non corrispondente Comportamento: Quando si tenta di aprire il gadget ECE in SPOG, viene visualizzato un errore che indica che il nome comune del certificato o il nome alternativo del soggetto non corrisponde al nome configurato.Verifica: Convalida il certificato SSLRisoluzione: Verificare che il campo Nome comune nell'oggetto o uno dei campi DNS nel campo Nome soggetto alternativo contenga il nome completo immesso in SPOG come nome del server Web.Problemi del sistema Servizio non avviato Comportamento: Quando si tenta di aprire il gadget ECE in SPOG, viene visualizzato l'errore "La pagina Web all'indirizzo https://{url} potrebbe essere temporaneamente inattiva o potrebbe essere stata spostata in modo permanente in un nuovo indirizzo".Verifica: Verificare che il servizio Windows - Cisco sia stato avviato su tutti i server ECE ad eccezione del server Web. Esaminare i registri radice nel server applicazioni per individuare eventuali erroriRisoluzione: Avviare il servizio Cisco su tutti i servizi ECE.Problema di configurazione Configurazione LDAP Comportamento: Quando si tenta di aprire il gadget ECE in SPOG, viene visualizzato l'errore "Si è verificato un errore durante il caricamento della pagina. Contattare l'amministratore."Verifica: Aumentare il livello di traccia dell'Application Server portandolo al livello 7- Debug, quindi tentare di nuovo l'accesso ed esaminare il log dell'Application Server. Cercare la parola LDAP.Risoluzione: Convalidare la configurazione LDAP per l'SSO dell'amministratore delle partizioni per assicurarsi che sia corretta.

Informazioni correlate

Questi sono i documenti chiave che è necessario esaminare attentamente prima di iniziare qualsiasi installazione o integrazione ECE. Non si tratta di un elenco esaustivo di documenti ECE.

> **Attenzione:** La maggior parte dei documenti ECE ha due versioni. Accertarsi di scaricare e utilizzare le versioni di PCCE. Il titolo del documento è **per Packaged Contact Center Enterprise** o **(Per PCCE)** o **(Per UCCE e PCCE)** dopo il numero di versione.

Prima di procedere all'installazione, all'aggiornamento o all'integrazione, controllare la pagina iniziale della documentazione di Cisco Enterprise Chat and Email.

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

- 12.0 Guida all'installazione e alla configurazione di Enterprise Chat and EmailGuida all'aggiornamento di Enterprise Chat and EmailGuida per l'amministratore di Enterprise Chat

and Email

- 12.5 Guida all'installazione e alla configurazione di Enterprise Chat and EmailGuida all'aggiornamento di Enterprise Chat and EmailGuida per l'amministratore di Enterprise Chat and Email