Integración de ECE con PCCE en la versión 12.0 y superior

Contenido

Introducción

Este documento describe los pasos para integrar el chat empresarial y el correo electrónico (ECE) con Packaged Contact Center Enterprise (PCCE) en las versiones 12.0 y posteriores

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Chat empresarial y correo electrónico (ECE) 12.x
- Packaged Contact Center Enterprise (PCCE) 12.x

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- CEPE 12.5(1)
- PCCE 12.5(1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

La versión 12.0 de PCCE introdujo una nueva interfaz de gestión conocida como el panel de control único (SPOG). Casi toda la gestión del Contact Center y de las aplicaciones relacionadas se realiza ahora en esta interfaz. Para integrar correctamente tanto la CEPE como la PCCE debe completar varios pasos que son exclusivos de esta integración. Este documento le guiará a través de este proceso.

Terminology

A lo largo de este documento, se utilizan estos términos.

- Conversación empresarial y correo electrónico (ECE): CEPE es un producto que permite que las solicitudes de correo electrónico y chat se enruten a los agentes del Contact Center de la misma manera que las llamadas de voz.
- Panel de vidrio único (SPOG): SPOG es la forma en que se realiza la administración de PCCE en la versión 12.0 y superiores. SPOG es una reescritura completa de la herramienta CCE Administration que se utilizó en versiones anteriores a 12.0.
- Autoridad de certificación (CA): entidad que emite certificados digitales de acuerdo con un modelo de infraestructura de clave pública (PKI). Existen dos tipos de CA que puede encontrar.CA pública: una CA pública que tiene sus certificados raíz e intermedio incluidos en la mayoría de los exploradores y sistemas operativos. Algunas CA públicas comunes incluyen IdenTrust, DigiCert, GoDaddy y GlobalSign.CA privada: una CA privada es aquella que existe dentro de una empresa. Algunas CA privadas están firmadas por CA públicas, pero la mayoría de las veces son CA independientes y los certificados que emiten sólo son de confianza para los equipos de esa organización.Dentro de cualquiera de los dos tipos de CA, hay dos tipos de servidores de CA.Servidor de CA raíz: el servidor de CA raíz firma su propio certificado. En la implementación PKI estándar de varios niveles, la CA raíz está desconectada e inaccesible. La CA raíz en este modelo también emite certificados a otro servidor de la CA conocido como CA intermedia. Algunas empresas eligen utilizar sólo una CA de nivel único. En este modelo, la CA raíz emite certificados destinados a ser utilizados

por una entidad que no sea otro servidor de la CA.Servidor de CA intermedio - El servidor de CA intermedio o emisor emite certificados destinados a ser utilizados por una entidad que no sea otro servidor de CA.
- Microsoft Management Console (MMC): aplicación incluida con Microsoft Windows que permite cargar varios complementos. Puede utilizar los complementos para crear una consola personalizada para la administración del servidor. Con Windows se incluyen muchos complementos diferentes. Una breve lista de ejemplos incluye Certificados, Administrador de dispositivos, Administración de discos, Visor de eventos y Servicios.
- Equilibrador de carga de red (NLB): dispositivo o aplicación que presenta varios recursos físicos a los usuarios finales con un nombre físico común. Los NLB son muy comunes con las aplicaciones y servicios web. Los NLB se pueden implementar de muchas maneras. Cuando se utiliza con ECE, el NLB se debe configurar de manera que garantice que las sesiones de usuario regresen al mismo servidor web de back-end físico mediante el uso de cookie-insert o un método equivalente. Esto se conoce como una sesión fija con cookie-insert. Sesión estática se refiere simplemente a la capacidad de un equilibrador de carga para devolver la sesión de un usuario al mismo servidor back-end físico para todas las interacciones. Paso a través de Secure Sockets Layer (SSL): el paso a través de SSL es un método en el que existe la sesión SSL entre el dispositivo del usuario final y el servidor web físico donde se asignó la sesión del usuario. El paso a través de SSL no permite la inserción de cookies, ya que la sesión HTTP se cifra físicamente en todo momento. La mayoría de los NLB soportan una sesión fija con SSL Passthrough mediante el uso de tablas con stick que monitorean la porción del servidor hello y clienthello de la configuración de la sesión y almacenan los valores únicos en una tabla. Cuando la siguiente solicitud que coincide con estos valores se presenta al NLB, la tabla stick se puede utilizar para devolver la sesión al mismo servidor back-end.Descarga SSL: cuando se configura un NLB para descarga SSL, hay dos sesiones SSL o túneles que existen para cualquier sesión de usuario final dada. El primero se encuentra entre el dispositivo del usuario final y la IP virtual (VIP) configurada en el NLB para el sitio web. La segunda es entre la IP de back-end del NLB y el servidor web físico donde se asigna la sesión del usuario. La descarga SSL admite la inserción de cookies, ya que la secuencia HTTP se descifra completamente mientras se encuentra en el NLB, donde se pueden insertar cookies HTTP adicionales y se puede realizar la inspección de la sesión. La descarga SSL se utiliza a menudo cuando la aplicación web no requiere SSL, sino que se realiza para la seguridad. Las versiones actuales de la CEPE no admiten el acceso a la aplicación en una sesión no SSL.

Pasos previos

Hay varios requisitos previos que se deben completar antes de comenzar a integrar los dos sistemas.

- Nivel mínimo de parche de PCCE Versión 12.0(1) - ES37Versión 12.5(1) - No hay un mínimo actual para la funcionalidad base
  La función del analizador de Webex Experience Management (WXM) requiere ES7
- Nivel mínimo de parche de ECE Se recomienda que la CEPE ejecute el último Engineering Special (ES) disponible.Versión 12.0(1) - ES3 + ES3_ET1aVersión 12.5(1) - No hay un mínimo actual para la funcionalidad base
  La función WXM Analyzer requiere ES1

- Elementos de configuración Asegúrese de asociar los dominios ECE_Email, ECE_Chat y ECE_Outbound Media Routing (MRD) con la instancia de aplicación correcta.Para el modelo de implementación de agente PCCE 2000, la instancia de aplicación es MultiChannel.Para el modelo de implementación de agente PCCE 4000/12000, la instancia de aplicación se presenta en forma de {site}_{perifal_set}_{application_instance}.
  Si instaló PCCE con el nombre del sitio como Main, el periférico como PS1 y la instancia de la aplicación como Multicanal, el nombre de la instancia de la aplicación es Main_PS1_Multichannel.**Nota:** El nombre de instancia de aplicación distingue entre mayúsculas y minúsculas. Asegúrese de escribir el nombre correctamente cuando agregue el servidor Web ECE al inventario.

Pasos de integración

Todos los detalles de todos los pasos de este documento se tratan en la documentación de la CEPE y la CPCE, pero no se muestran en una lista ni están todos en el mismo documento. Consulte los enlaces incluidos al final de este documento para obtener más detalles.

Paso 1. Configurar certificados SSL

Debe generar un certificado para que lo utilice el servidor web de ECE. Puede utilizar un certificado autofirmado, pero a menudo es más fácil utilizar un certificado firmado por CA. Los certificados autofirmados no son menos seguros que los certificados firmados por la CA, hay menos pasos para crear inicialmente el certificado, pero cuando el certificado necesita ser reemplazado, debe recordar cargar el nuevo certificado en los almacenes de claves de Java en todos los servidores de datos de administración de PCCE. Si utiliza un certificado firmado por CA, sólo necesita cargar los certificados raíz y, si los hay, intermedios en los almacenes de claves.

Si tiene varios servidores web en su implementación, debe revisar estas directrices. Los pasos específicos requeridos para configurar un equilibrador de carga de red están fuera del alcance de este documento. Póngase en contacto con su proveedor de equilibrio de carga para obtener asistencia si es necesario.

Aunque no es necesario, un equilibrador de carga simplifica en gran medida la implementación

El acceso a la aplicación ECE en cada servidor web debe utilizar SSL independientemente del método de equilibrio de carga utilizado

El equilibrador de carga puede configurarse como paso a través de SSL o descarga de SSL

Si se elige el paso a través de SSL, debe hacerse lo siguiente: Debe realizar todas las operaciones de certificados desde un servidor

Una vez configurado correctamente el certificado, debe exportar el certificado y asegurarse de que la clave privada se incluye en un archivo de intercambio de información personal (PFX)

Debe copiar el archivo PFX en todos los demás servidores Web de la implementación y, a continuación, importar el certificado en IIS

Si se elige la descarga SSL, cada servidor web puede configurarse con su propio certificado SSL

individual

> **Nota:** Si tiene varios servidores web y elige el paso a través de SSL en su servidor web, o si desea tener un certificado común en todos los servidores, debe elegir un servidor web para realizar el paso 1 y después importar el certificado a todos los demás servidores web. Si selecciona Descarga SSL, debe realizar estos pasos en todos los servidores web. También debe generar un certificado para utilizarlo en el equilibrador de carga.

Paso 1.1. Generar un certificado

Puede omitir esta sección si ya ha creado u obtenido un certificado; de lo contrario, elija una de las dos opciones.

Opción 1. Utilizar un certificado autofirmado

1. Vaya a IIS Administration (Administración de IIS).
2. Seleccione el nombre del servidor en el árbol Conexiones de la izquierda.
3. Localice **certificados de servidor** en el panel central y haga doble clic para abrirlos.
4. Seleccione **Crear certificado firmado automáticamente...** en el panel Acciones de la derecha.
5. En la ventana **Crear certificado firmado automáticamente**, elija e introduzca un nombre en **Especificar un nombre descriptivo para el certificado:** para abrir el Navegador. Este nombre es el modo en que aparece el certificado en el proceso de selección en el siguiente paso principal. Este nombre no necesita coincidir con el nombre común del certificado y no afecta al modo en que el certificado aparece para el usuario final.
6. Asegúrese de que **Personal** esté seleccionado en **Seleccionar un almacén de certificados para el nuevo certificado:** cuadro desplegable.
7. Seleccione **Aceptar** para crear el certificado.
8. Vaya al siguiente paso importante, **Enlazar certificado a sitio web**.

Opción 2. Utilizar un certificado firmado por CA

Los certificados firmados por CA requieren que genere una solicitud de firma de certificado (CSR). La CSR es un archivo de texto que se envía a la CA donde se firma y luego se devuelve el certificado firmado junto con los certificados de CA requeridos y se cumple el CSR. Puede optar por hacerlo mediante IIS Administration o mediante Microsoft Management Console (MMC). El método de administración de IIS es mucho más sencillo sin necesidad de conocimientos especiales, pero solo permite configurar los campos incluidos en el atributo Subject del certificado y cambiar la longitud del bit. MMC requiere pasos adicionales y dispone de un conocimiento exhaustivo de todos los campos requeridos en una CSR válida. Se recomienda encarecidamente utilizar MMC sólo si tiene experiencia moderada a experta en la creación y administración de certificados. Si la implementación requiere que se tenga acceso a ECE por más de un nombre completo o si se le exige cambiar cualquier parte del certificado excepto el asunto y la longitud del bit, debe utilizar el método MMC.

1. Vía IIS Administration Utilice estos pasos para generar una solicitud de firma de certificado (CSR) a través del Administrador de IIS.Vaya a IIS Administration (Administración de IIS).Seleccione el nombre del servidor en el árbol Conexiones de la izquierda.Localice

certificados de servidor en el panel central y haga doble clic para abrirlos.Seleccione **Crear solicitud de certificado...** en el panel Acciones de la derecha. Aparece el asistente **Solicitar certificado**.En la página **Propiedades del nombre distinguido**, introduzca los valores en el formulario del sistema. Se deben introducir todos los campos. Seleccione **Next** para continuar.En la página **Propiedades del proveedor de servicios criptográficos**, deje la selección predeterminada para **proveedor de servicios criptográficos:**. Cambiar la **longitud de bits:** hasta un mínimo de **2048**. Seleccione **Next** para continuar.En la página **Nombre de archivo**, seleccione el lugar donde desea guardar el archivo CSR.Proporcione el archivo a la CA. Cuando haya recibido el certificado firmado, cópielo en el servidor web y continúe con el siguiente paso.En la misma ubicación en el Administrador de IIS, seleccione **Solicitud de certificado completa** en el **panel Acciones**. Aparecerá el asistente.En la página **Especificar respuesta de autoridad de certificación**, elija el certificado proporcionado por su CA. Escriba un nombre en el cuadro **Nombre descriptivo**. Este nombre es el modo en que aparece el certificado en el proceso de selección en el siguiente paso principal. Asegúrese de que **Seleccione un almacén de certificados para el nuevo certificado:** se establece en **Personal**.Seleccione **Aceptar** para completar la carga del certificado.Vaya al siguiente paso importante, **Enlazar certificado a sitio web**.

2. Mediante Microsoft Management Console (MMC) Utilice estos pasos para generar una CSR a través de MMC. Este método permite personalizar todos los aspectos de la CSR.Haga clic con el botón derecho del ratón en el botón Inicio y seleccione Ejecutar.Escriba **mmc** en el cuadro de ejecución y seleccione **Aceptar**.Agregue el complemento Certificado a la ventana MMC. Seleccione **Archivo**, luego **Agregar/Quitar complemento...**. Aparecerá el cuadro **Agregar o quitar complementos**.En la lista de la izquierda, busque **Certificates** y seleccione **Add >**. Aparece el cuadro de complemento Certificados.Seleccione la opción **Cuenta de equipo** y luego seleccione **Siguiente >**.Asegúrese de que el **equipo local: (el equipo en el que se encuentra esta consola)** está seleccionado en la página **Seleccionar equipo** y, a continuación, seleccione **Finalizar**.Seleccione **Aceptar** para cerrar el cuadro **Agregar o quitar complementos**.Generar CSR En el panel izquierdo, expanda **Certificados (equipo local)** y luego **Personal** y seleccione la carpeta **Certificados**.Haga clic con el botón derecho del ratón en la carpeta **Certificates** y navegue hasta **Todas las tareas > Operaciones avanzadas >** y, a continuación, seleccione **Crear solicitud personalizada...**. Aparece el asistente **Inscripción de certificados**.Seleccione **Next** en la pantalla de introducción.En la página **Select Certificate Enrollment Policy**, seleccione **Proceed without enrollment policy**, que se muestra en **Solicitud personalizada**, y luego seleccione **Next**.En la página **Solicitud personalizada**, asegúrese de que la **plantilla** seleccionada sea la **(Sin plantilla) clave CNG**, y que el **formato de solicitud** sea adecuado para su CA. **PKCS #10** funciona con la CA de Microsoft. Seleccione **Next** para continuar con la página siguiente.En la página **Información del certificado**, seleccione el desplegable junto a la palabra **Detalles** y, a continuación, seleccione el botón **Propiedades**. Aparece el formulario **Propiedades del certificado**.Está fuera del alcance de este documento dar todas las opciones para el formulario **Propiedades del certificado**. Consulte la documentación de Microsoft para obtener más información. A continuación se muestran algunas notas y sugerencias sobre este formulario. Asegúrese de rellenar todos los valores necesarios en el **nombre del asunto:** sección del **Asunto:** fichaAsegúrese de que el valor proporcionado para el **nombre común** también se proporcione en el **nombre alternativo:** secciónEstablecer el **tipo:** a **DNS**, escriba la URL en el **Valor:** y, a continuación, seleccione el botón **Agregar >**Si desea utilizar varias URL para acceder a ECE, proporcione cada nombre alternativo en este mismo campo y seleccione **Agregar >** después de cadaAsegúrese de establecer el **tamaño de clave** en la ficha **Private Key** en un valor mayor que 1024.Si planea

exportar el certificado para utilizarlo en varios servidores web, como se hace a menudo en una instalación HA, asegúrese de seleccionar **Convertir clave privada en exportable**. Si no se hace esto, no se puede exportar el certificado más tardeLos valores introducidos y las selecciones realizadas no se validan. Debe asegurarse de proporcionar toda la información necesaria o puede que la CA no pueda completar el CSRUna vez que haya seleccionado todas las selecciones, **Aceptar** para volver al asistente. Seleccione **Next** para continuar con la página siguiente.En el **¿Dónde desea guardar la solicitud sin conexión?** seleccione un nombre de archivo en una ubicación a la que pueda acceder. Para la mayoría de las CA, debe seleccionar **Base 64** como formato.Proporcione el archivo a su CA. Cuando lo hayan firmado y le hayan devuelto el certificado, copie el certificado al servidor web y continúe con los últimos pasos.En el complemento Administración de certificados para MMC, navegue hasta **Certificados (equipo local) > Personal**, haga clic con el botón derecho en **Certificados** y elija **Todas las tareas > Importar...**. Aparece el **Asistente para importación de certificados**.Seleccione **Next** en la pantalla de introducción.En la pantalla **Archivo a importar**, seleccione el certificado que ha firmado su CA y, a continuación, seleccione **Siguiente**.Asegúrese de seleccionar **Colocar todos los certificados en el siguiente almacén**.Asegúrese de que **Personal** esté seleccionado en el **almacén de certificados:** y, a continuación, seleccione **Siguiente**.Revise la pantalla final y, a continuación, seleccione **Finalizar** para completar la importación.Ahora puede cerrar la consola MMC. Si se le solicita que guarde la configuración de la consola, puede seleccionar **No**. Esto no afecta a la importación del certificado.Vaya al siguiente paso importante, **Enlazar certificado a sitio web**.

Paso 1.2. Enlazar certificado a sitio web

Precaución: Debe asegurarse de que el campo hostname se deja en blanco y que la opción Require Server Name Indication no está seleccionada en el cuadro Edit Site Binding (Editar enlace de sitio). Si alguno de estos se configura, SPOG falla cuando intenta comunicarse con ECE

1. Abra el Administrador de Internet Information Services (IIS) si no lo ha hecho anteriormente.
2. En el panel **Conexiones** de la izquierda, navegue hasta **Sitios** y seleccione **Sitio Web predeterminado**. Asegúrese de seleccionar el nombre del sitio correcto si decide utilizar un nombre de sitio distinto de Sitio Web predeterminado.
3. Seleccione **Enlaces...** en el panel **Acciones** de la derecha. Aparecerá el cuadro **Enlaces al sitio**. Si no hay una fila con **Type**, **https** y **Port**, **443** , complete lo siguiente. De lo contrario, vaya al siguiente paso importante. Seleccione la opción **Agregar...** , aparece el cuadro **Agregar enlace de sitio**.Seleccione **https** en el **Tipo:** desplegable.Asegúrese de que la **dirección IP:** muestra **Todo sin asignar** y el **puerto:** es **443**.Asegúrese de dejar el **nombre de host:** y la opción **Require Server Name Indication** no está seleccionada.En el **certificado SSL:** seleccione el nombre del certificado que corresponda al que creó anteriormente. Si no está seguro de qué certificado elegir, utilice el comando **Seleccionar...** para ver y buscar los certificados presentes en el servidorUsar la **vista...** para ver el certificado seleccionado y comprobar que los detalles son correctosSeleccione **Aceptar** para guardar la selección.Seleccione la fila que muestra **https** en la columna Tipo y, a continuación, seleccione la **opción Editar...** para abrir el Navegador. Aparece el cuadro **Editar enlace de sitio**. Asegúrese de que la **dirección IP:** muestra **Todo sin asignar** y el **puerto:** es **443**.Asegúrese de que el **nombre de host:** se ha dejado en blanco y la opción **Require**

Server Name Indication no está seleccionada.En el **certificado SSL:** seleccione el nombre del certificado que corresponda al que creó anteriormente. Si no está seguro de qué certificado elegir, utilice el comando **Seleccionar...** para ver y buscar los certificados presentes en el servidorUsar la **vista...** para ver el certificado seleccionado y comprobar que los detalles son correctosSeleccione **Aceptar** para guardar la selección.Seleccione **Cerrar** para volver al Administrador IIS.

4. Ahora puede cerrar el Administrador IIS.

Paso 2. Configuración de SSO del administrador de particiones

La configuración SSO del administrador de particiones permite a ECE crear automáticamente una cuenta de usuario de nivel de partición para cualquier administrador que abra el gadget ECE en SPOG.

> **Nota:** Debe configurar el SSO del administrador de particiones incluso si no tiene pensado habilitar el SSO del agente o del supervisor.

Paso 2.1. Obtenga el certificado de Active Directory (AD) y cree un almacén de claves.

Este paso es necesario para hacer frente a los recientes cambios en la seguridad que ha anunciado Microsoft.

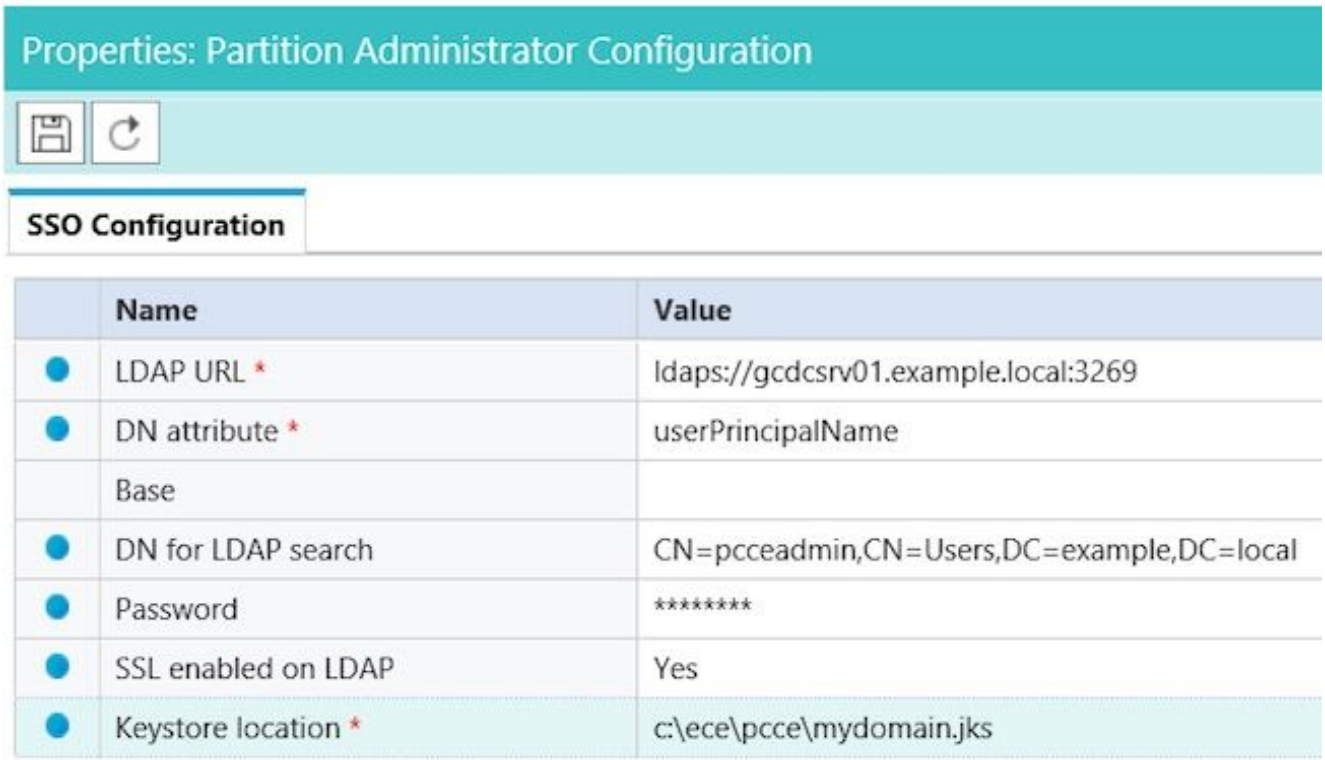
Para más detalles, véase https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows.

1. Obtenga el certificado SSL, en formato Base 64, del servidor AD que proporcione en el formulario Configuración del administrador de particiones.
2. Copie el archivo de certificado en uno de los servidores de la aplicación.
3. Abra una sesión RDP en el servidor de aplicaciones donde copió el certificado.
4. Cree un nuevo almacén de claves Java como se indica a continuación. Abra un símbolo del sistema en el servidor de aplicaciones.Cambie al directorio bin ECE Java Development Kit (JDK).Ejecute este comando. Reemplace los valores según corresponda.
   keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c:\ece\pcce\mydomain.jks -storepass MyP@ssword
5. Copie el almacén de claves a la misma ruta en todos los demás servidores de aplicaciones de su entorno.

Paso 2.2. Configuración de la CEPE con la información de acceso del protocolo ligero de acceso a directorios (LDAP) de AD.

1. Desde una estación de trabajo o un ordenador con **Internet Explorer 11**, navegue hasta la URL de partición empresarial. **Consejo:** La partición Business también se conoce como Partición 1. Para la mayoría de las instalaciones, se puede acceder a la partición Empresarial a través de una URL similar a https://ece.example.com/default.
2. Inicie sesión como **pa** y proporcione la contraseña para su sistema.
3. Después de haber iniciado sesión correctamente, seleccione el enlace **Administration** en la consola inicial.

4. Vaya a la carpeta **Configuración de SSO** de la siguiente manera, **Administración > Partición: default > Security > SSO and Provisioning**.
5. En el panel superior de la derecha, seleccione la entrada **Partition Administration Configuration**.
6. En el panel inferior de la derecha, introduzca los valores de su protocolo ligero de acceso a directorios (LDAP) y AD. **URL LDAP**: como práctica recomendada, utilice el nombre de un controlador de dominio de catálogo global (GC).
   Si no utiliza un GC, es posible que vea un error en los registros de ApplicationServer como se indica a continuación.
   Excepción en la autenticación LDAP <@>
   javax.names.PartialResultException: Referencia(s) de Continuación no Procesada(s); nombre restante 'DC=ejemplo,DC=com' El puerto del catálogo global no seguro es 3268El puerto Secure Global Catalog es 3269**Atributo DN**: debe ser userPrincipalName.**Base** - Esto no es necesario si utiliza un GC, de lo contrario, debe proporcionar el formato LDAP adecuado de base.**DN para la búsqueda LDAP** - A menos que su dominio permita el enlace anónimo, debe proporcionar el nombre distinguido de un usuario con la capacidad de enlazar a LDAP y buscar en el árbol de directorios.
   Sugerencia: la forma más sencilla de encontrar el valor correcto para el usuario es utilizar la herramienta Active Directory Users and Computers. Habilite **Funciones avanzadas** en el **menú Ver**.Navegue hasta el objeto de usuario, luego haga clic con el botón derecho y elija **Propiedades**.Seleccione la pestaña **Atributos**.Seleccione el botón **Filtro** y, a continuación, seleccione **Mostrar sólo atributos con valores**.Busque **distinguishedName** en la lista y, a continuación, haga doble clic para ver el valor.Resalte el valor mostrado y, a continuación, cópielo y péguelo en un editor de texto.Copie y pegue el valor del archivo de texto en el campo **DN para búsqueda LDAP**.
   El valor debe ser similar a, CN=pcceadmin, CN=Users, DC=example, DC=local**Contraseña**: a menos que su dominio permita el enlace anónimo, debe proporcionar la contraseña para el usuario especificado.**SSL habilitado en LDAP** - Este campo debe considerarse obligatorio para la mayoría de los clientes.**Ubicación del almacén de claves**: Debe ser la ubicación del almacén de claves donde se importó el certificado SSL de AD. En el ejemplo, se muestra c:\ece\pcce\mydomain.jks, como se muestra en la imagen:



7. Seleccione el icono del disquete para guardar los cambios.

Paso 3. Validar archivo de configuración

La finalización de esta sección es obligatoria para todas las instalaciones 12.0. Para cualquier versión que no sea 12.0, puede saltarse esta sección.
Existen dos escenarios adicionales con todas las versiones en los que se puede requerir este paso. La primera es cuando se ha instalado ECE en una configuración de alta disponibilidad. La segunda, y más común, es cuando el nombre de host del servidor web no coincide con el nombre que utiliza para acceder a ECE. Por ejemplo, si instala el servidor Web de ECE en un servidor con el nombre de host, UCSVRECEWEB.ejemplo.com, pero los usuarios acceden a las páginas Web de ECE con la dirección URL, chat.ejemplo.com, se debe completar esta sección. Si el nombre de host del servidor y la URL con la que accede a ECE son iguales y si ha instalado la versión 12.5 o superior, puede omitir este paso y completar la sección.

Reemplace {ECE_HOME} por la ubicación física en la que ha instalado ECE. Por ejemplo, si ha instalado ECE en **C:\Cisco**, reemplace {ECE_HOME} por **C:\Cisco** en cada ubicación.

> **Consejo:** Utilice un editor de texto como Notepad++ en lugar de notepad o Wordpad, ya que no interpretan correctamente los extremos de línea.

1. Abra una sesión de escritorio remoto a todos los servidores web de la CEPE en su implementación.
2. Vaya a esta ruta, **{ECE_HOME}\eService\templates\finesse\gadget\spog**.
3. Busque el archivo **spog_config.**jsfile y haga una copia de seguridad en una ubicación segura.
4. Abra el **spog_config.**jsfile actual en un editor de texto.
5. Busque estas dos líneas y actualícelas para que coincidan con su implementación.
   El web_server_protocol debe ser https, actualizar si es necesario.
   Actualice el nombre_de_servidor_web para que coincida con el nombre completo que ha

asignado para utilizar para acceder a ECE. Ejemplo: **ece.example.com** var web_server_protocol = "https";var web_server_name = "ece.example.com";

6. Guarde los cambios.
7. Repita este procedimiento en todos los demás servidores web de la implementación.

Paso 4. Agregar CEPE al inventario PCCE

Desde la versión 12.0, PCCE cuenta con 3 opciones de implementación diferentes: 2000 Agent (2K Agent), 4000 Agent (4K Agent) y 12000 Agent (12K Agent). Estas tres opciones de implementación se pueden separar en dos grupos: 2K Agent y 4K/12K Agent. Se separan de esta manera ya que hay varias diferencias fundamentales en su aspecto en SPOG. A continuación de este párrafo se hace una comparación de muy alto nivel de los dos métodos. Este documento no da pasos específicos para agregar un componente al inventario. Consulte los enlaces al final de este documento para obtener detalles específicos sobre este proceso. Esta sección cubre detalles específicos que deben verificarse al agregar ECE a PCCE. En este documento también se asume que la instalación de PCCE ha finalizado y que usted puede acceder y configurar otros aspectos de la solución.

- Implementación de agentes de 2000 La configuración inicial de los componentes PCCE se realiza completamente a través de CCE Administration y está automatizadaLos nuevos componentes se agregan en la página de inventario a través de un cuadro emergente en el que se especifican los detalles, como la IP o el nombre de host, así como las credenciales necesarias o la configuración específica del componente
- Implementación de agentes de 4000 y 12 000 Gran parte de la configuración inicial refleja los pasos utilizados para UCCELos componentes se agregan a través de un archivo de valores separados por comas (CSV) que se descarga de CCE Administration, se rellenan según la instalación específica y, a continuación, se carganLa implementación inicial requiere que algunos componentes específicos se incluyan en el primer archivo CSVLos componentes que no se agregaron cuando se configuró inicialmente el sistema se agregan a través de archivos CSV que contienen la información requerida

Paso 4.1. Cargar certificado de servidor Web de ECE en el almacén de claves de Java

1. Si se utilizan certificados autofirmados Abra una conexión de escritorio remoto al servidor de datos de administración (ADS) primario, lateral A.Abra Internet Explorer 11 como administrador y desplácese a la partición empresarial de ECE.Seleccione el icono de un candado en el lado derecho de la barra de URL y luego elija **Ver certificados**.En el cuadro **Certificado**, seleccione la **ficha Detalles**.Seleccione **Copiar a archivo...** cerca de la parte inferior de la pestaña.En el **Asistente para exportación de certificados**, seleccione **Siguiente** hasta que llegue a la página **Exportar formato de archivo**. Asegúrese de seleccionar el formato **X.509 (.CER)** codificado **Base-64**.Guarde el certificado en una ubicación como **c:\Temp\certificates** en el servidor ADS para completar la exportación.Copie el certificado a todos los demás servidores ADS.Abra un símbolo del sistema administrativo.Cambie al directorio de inicio de Java y, a continuación, al directorio bin. Se puede acceder al directorio de inicio de Java de la siguiente manera. **cd %JAVA_HOME%\bin**Realice una copia de seguridad del archivo **cacerts** actual. Copie el archivo **cacerts** de **%JAVA_HOME%\lib\security** a otra ubicación.Ejecute este comando para importar el certificado que guardó anteriormente. Si la contraseña del almacén de claves no es 'changeit', actualice el comando para que coincida con la instalación.

keytool -keystore ../lib/security/cacerts -storepass changeit -import -alias <FQDN del servidor ECE> -file <Ubicación donde guardó el certificado>Reinicie el servidor ADS.Repita los pasos 8-12 en los otros servidores ADS.

2. Si se utilizan certificados firmados por CA Obtenga el certificado raíz e intermedio en formato DER/PEM y cópielo en una ubicación como **C:\Temp\certificates** en todos los servidores ADS. **Nota:** Póngase en contacto con el administrador de la CA para obtener estos certificados. Abra una conexión de escritorio remoto al ADS lateral principal.Abra un símbolo del sistema administrativo.Cambie al directorio de inicio de Java y, a continuación, al directorio bin. Se puede acceder al directorio de inicio de Java de la siguiente manera. **cd %JAVA_HOME%\bin**Realice una copia de seguridad del archivo **cacerts** actual. Copie el archivo **cacerts** de **%JAVA_HOME%\lib\security** a otra ubicación.Ejecute este comando para importar el certificado que guardó anteriormente. Si la contraseña del almacén de claves no es 'changeit', actualice el comando para que coincida con la instalación.
keytool -keystore ../lib/security/cacerts -storepass changeit -trustcacerts -import -alias <Nombre de la raíz de la CA> -file <Ubicación donde guardó el certificado raíz>Repita el paso 6. e importar el certificado intermedio si está presente.Reinicie el servidor ADS.Repita los pasos 2-12 en todos los demás servidores ADS.

Paso 4.2. Agregar el servidor de datos ECE al inventario

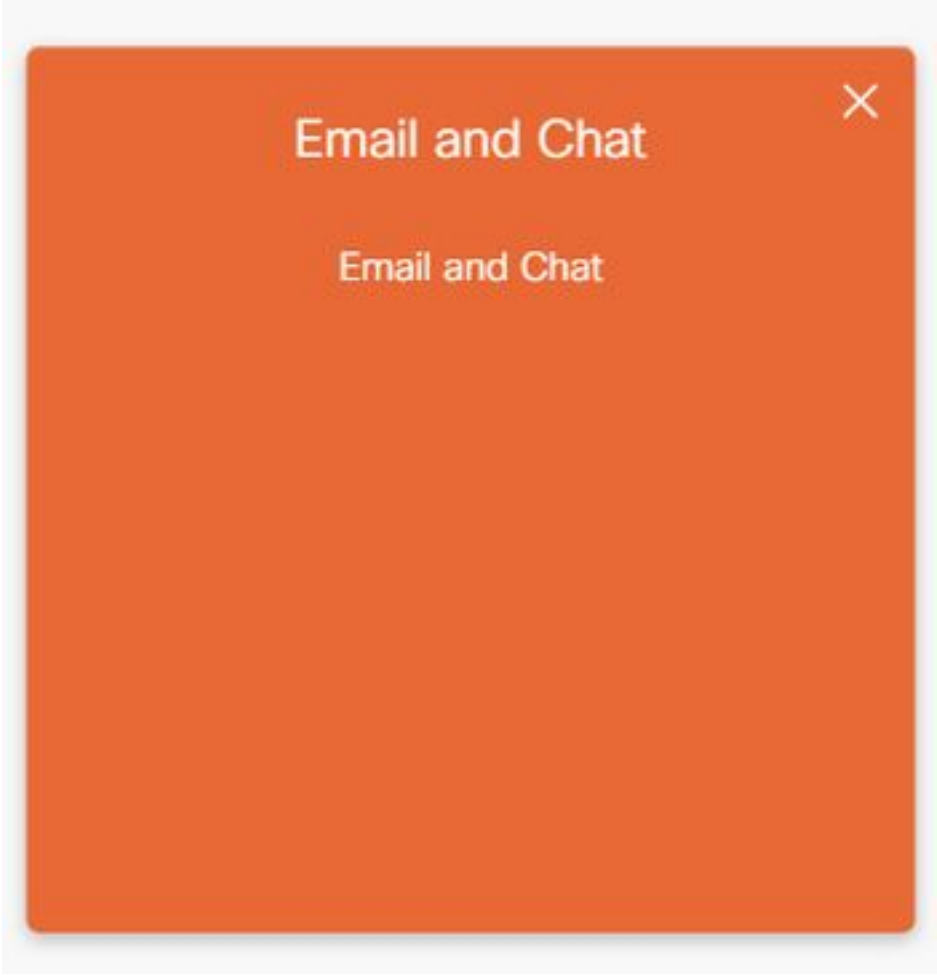
- Aunque el servidor de datos debe existir en el inventario del sistema, no se realiza ninguna comunicación directa entre el ADS PCCE y el servidor de datos
- Cuando se implementa ECE en la implementación de 1500 agentes, el servidor de datos es el servidor de servicios
- Cuando ECE se instala en una configuración HA, se deben agregar ambos servidores de servicios

Paso 4.3. Agregar el servidor Web ECE al inventario

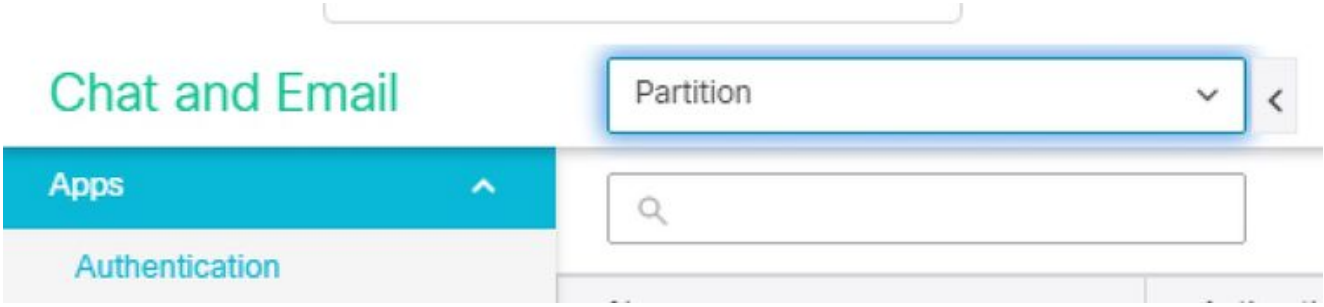
- Asegúrese de agregar el servidor web con el nombre completo Este nombre debe coincidir con el nombre común del certificado de la CEPE o debe aparecer como uno de los nombres alternativos de asunto (SAN)sNo debe utilizar sólo el nombre de host o la dirección IP
- El nombre de usuario y la contraseña de ECE deben ser las credenciales de inicio de sesión de PA
- Asegúrese de que la instancia de aplicación es correcta El nombre de la instancia de aplicación distingue entre mayúsculas y minúsculasPara las implementaciones de Agent PCCE de 2000, la instancia de aplicación es multicanalPara las implementaciones de 4000/12000 de Agent PCCE, la instancia de aplicación contiene el sitio y el conjunto de periféricos como parte del nombre
- Cuando ECE se instala con más de un servidor web, por ejemplo en la implementación del agente 1500 o en una implementación de HA del agente 400, puede utilizar la URL que apunta al equilibrador de carga o la URL que apunta a cada servidor web individual como nombre completo del servidor web.
- Si tiene más de una implementación ECE o si decide agregar cada servidor Web individual en implementación con más de uno, puede elegir el servidor Web correcto cuando abra el gadget ECE en SPOG.

Paso 5. Integración de CEPE con PCCE

1. Inicie sesión en CCE Administration como administrador.
2. Seleccione la tarjeta **Email and Chat y, a continuación, el** enlace **Email and Chat** como se muestra en la imagen.



3. Revise el servidor seleccionado actual en el menú desplegable Device Name (Nombre de dispositivo). Si agregó ambos servidores web en una instalación de HA, puede elegir uno de ellos. Si agrega una segunda implementación de ECE a su sistema más adelante, asegúrese de seleccionar el servidor adecuado antes de continuar.
4. En el menú desplegable junto a **Chat y correo electrónico**, seleccione **Partition** o **Global** como se muestra en la imagen.

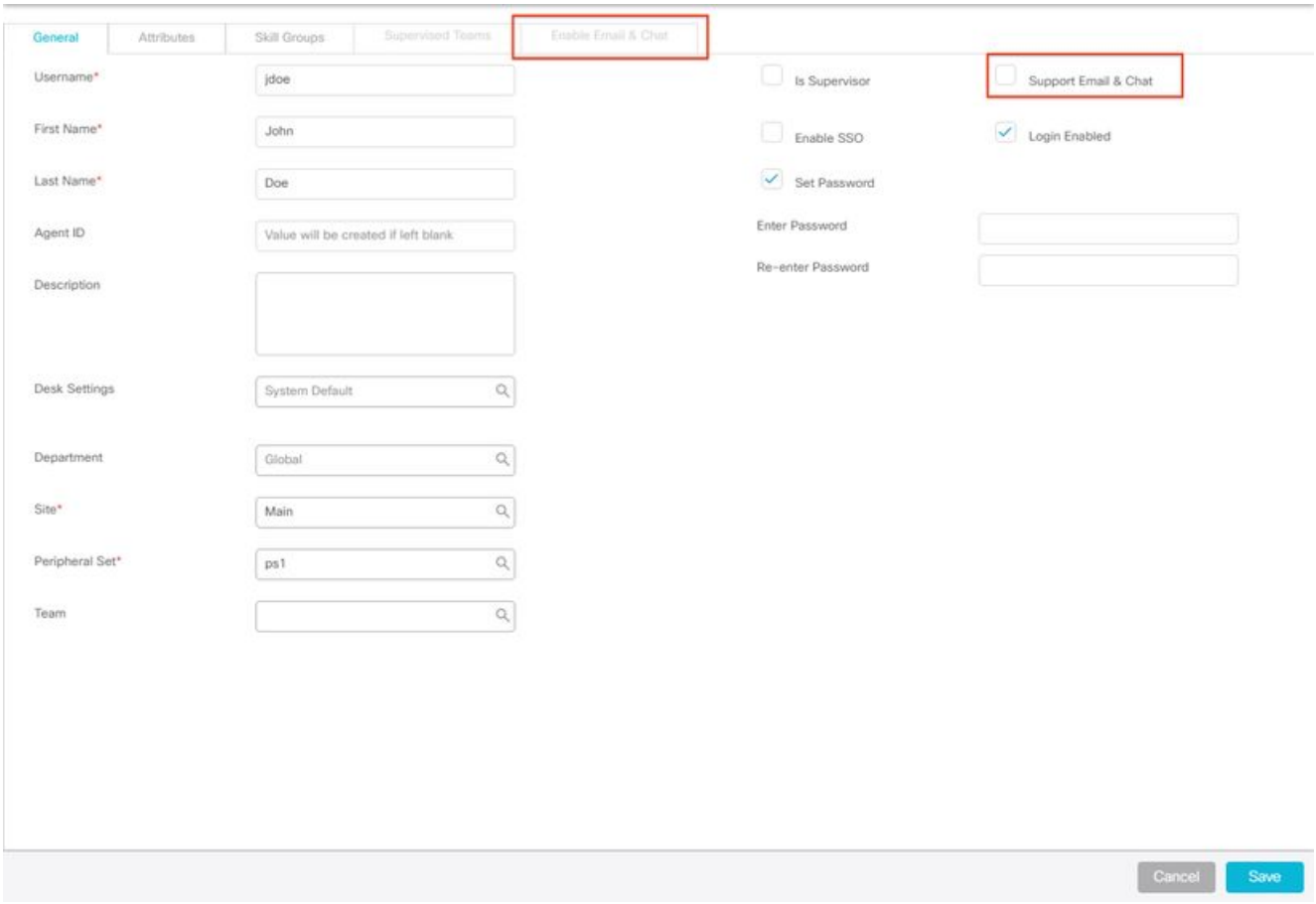


5. En el menú superior, seleccione **Integración** y, a continuación, seleccione la flecha situada junto a **Unified CCE** y seleccione el segundo **Unified CCE** como se muestra en la imagen.

6. Rellene los valores de la ficha **Detalles de AWDB** para su instalación y, a continuación, seleccione el **botón Guardar**.
7. Seleccione la pestaña **Configuración** y complete esto de la siguiente manera. Seleccione la lista desplegable junto a **Application Instance** y seleccione Application Instance creada para ECE. **Nota:** Esta no debe ser la instancia de aplicación que comienza con UQ.Seleccione el círculo verde con el botón blanco más el signo  seleccione el PG de agente. Seleccione el PG de agente (o PG de agente si hay más de uno).Seleccione **Guardar** una vez que haya agregado todos los PG de agente. **Advertencia:** Una vez que seleccione **Guardar** el sistema está conectado permanentemente a PCCE y no se puede deshacer. Si se producen errores en esta sección, debe desinstalar completamente CEPE y eliminar todas las bases de datos, luego instalar la CEPE como si fuera una instalación nueva.

Paso 6. Validar integración CEPE

1. En CCE Administration, verifique que no se muestre ninguna alerta en la barra de estado superior. Si hay alertas, seleccione la palabra **Alertas** y revise la página Inventario para asegurarse de que ninguna de las alertas son para los servidores CEPE.
2. Seleccione **Usuarios** y **Agentes** en la barra de navegación de la izquierda.
3. Seleccione un agente de la lista y verifique esto. Ahora debería ver una nueva casilla de verificación para **Support Email & Chat** en la pestaña **General**.Ahora debería ver una nueva pestaña etiquetada como **Habilitar correo electrónico y chat** como se muestra en la imagen.



4. Habilite un agente de prueba para ECE. Seleccione la casilla de verificación **Support Email & Chat** y observe que la pestaña **Enable Email & Chat** ahora puede estar seleccionada.Seleccione la pestaña **Habilitar correo electrónico y chat** y proporcione valor en el **campo Nombre de pantalla**.Seleccione **Guardar** para actualizar al usuario.Debería recibir un mensaje de confirmación.
5. Verifique que se haya actualizado la CEPE. Seleccione el botón de navegación **Descripción general** y, a continuación, seleccione la tarjeta **Correo electrónico y chat** y el enlace.En la lista desplegable junto a **Chat y correo electrónico**, seleccione el nombre que corresponda al departamento del agente. **Nota:** El departamento de servicios de la CEPE contiene todos los objetos que pertenecen al departamento mundial de la CPE. Por lo tanto, el nombre del departamento Service es un valor reservado.En el menú superior, seleccione **User Management** y luego **Users** en el menú bajo **Chat y correo electrónico**.Valide que vea el nuevo agente en la lista.

Troubleshoot

Se recomienda descargar varias herramientas y guardarlas en los servidores ECE. Esto facilita en gran medida la resolución de problemas y el mantenimiento de la solución con el tiempo.

- Un editor de texto como Notepad++
- Herramienta de archivo como 7-Zip
- Uno de los muchos programas de cola para Windows
  Algunos ejemplos son: Baretail -https://www.baremetalsoft.com/baretail/Correo para Win32 - http://tailforwin32.sourceforge.net/

Para resolver problemas con la integración, primero debe tener en cuenta algunos archivos de registro de claves y la ubicación de cada uno.

1. ## Nombres y ubicaciones de archivos en ECE

   Hay muchos registros en el sistema ECE, estos son sólo los que son más útiles cuando se intenta resolver un problema con la integración.

   Clave de servidor:C = Servidor compartidoA = Servidor de aplicacionesS = Servidor de serviciosM = Servidor de mensajeríaLa mayoría de los archivos de registro también tienen otros dos registros asociados.eg_log_{SERVERNAME}_{PROCESS}.log - Registro de procesos principaleg_log_dal_connpool_{SERVERNAME}_{PROCESS}.log - Uso del conjunto de conexioneseg_log_query_timeout_{SERVERNAME}_{PROCESS}.log - Actualizado cuando una consulta falla debido al tiempo de espera
2. ## Nombres y ubicaciones de archivos en PCCE

   Todos los registros de PCCE para problemas de integración se encuentran en el ADS del lado A. Estos son los registros que son más importantes a la hora de resolver problemas de integración. Cada una de ellas se encuentra en **C:\icm\tomcat\logs**.

   De estos registros, los tres primeros son los más solicitados y revisados.Utilice estos pasos para establecer niveles de seguimiento y recopilar los registros necesarios.
3. **Configuración de nivel de seguimiento**Esta sección sólo se aplica a la CEPE. Los registros que se requieren de PCCE tienen su nivel de seguimiento establecido por Cisco y no se pueden cambiar. Desde una estación de trabajo o equipo con **Internet Explorer 11**, navegue hasta la URL de partición del sistema. **Consejo:** La partición del sistema también se conoce como Partición 0. Para la mayoría de las instalaciones, se puede acceder a la partición System a través de una URL similar a, https://ece.example.com/systemInicie sesión como **sa** y proporcione la contraseña para su sistema.Después de haber iniciado sesión correctamente, seleccione el enlace **System** en la consola inicial.En la página Sistema, expanda **System > Shared Resources > Logger > Procesos**.En el panel superior derecho, busque el proceso que desea cambiar el nivel de seguimiento y selecciónelo.
   Nota: En un sistema HA y en un sistema con más de un servidor de aplicaciones, los procesos se enumeran más de una vez. Para asegurarse de capturar los datos, establezca el nivel de seguimiento para todos los servidores que contienen el proceso.En el panel inferior derecho, seleccione el desplegable **Nivel máximo de seguimiento** y seleccione el valor adecuado.
   Hay 8 niveles de seguimiento definidos en la CEPE. Los 4 de esta lista son los que se utilizan con más frecuencia. 2 - Error - Nivel de seguimiento predeterminado para los procesos4 - Información - Nivel de seguimiento generalmente utilizado para la resolución de problemas6 - Dbquery: a menudo es útil para diagnosticar problemas al principio de la configuración o problemas más complejos7 - Depuración - Resultado muy detallado, solo

necesario en los problemas más complejos**Nota:** No se debe mantener ningún proceso en 6 - Dbquery durante un periodo de tiempo prolongado, y generalmente sólo con la guía del TAC.La mayoría de los procesos deben permanecer en el nivel de seguimiento, 2-Error. Si selecciona el nivel 7 u 8, también debe seleccionar una duración máxima. Cuando se alcanza el tiempo máximo de duración, el nivel de seguimiento vuelve al último nivel establecido.
Después de configurar el sistema, cambie estos cuatro procesos para seguir el nivel 4.proceso EAASproceso EAMSdx-processrx-processSeleccione el icono Guardar para establecer el nuevo nivel de seguimiento.

4. ## Recopilación de archivos de registro

Abra una sesión de Escritorio remoto en el servidor donde se necesitan los registros de proceso.Navegue hasta la ubicación del archivo de registro. Servidores ECE Los registros se escriben de la siguiente manera.De forma predeterminada, los registros son archivos escritos con un tamaño máximo de 5 MBCuando un archivo de registro alcanza el máximo configurado, se le cambia el nombre en el formato {LOGNAME}.log.{#}ECE mantiene los 49 archivos de registro anteriores más el archivo actualEl registro actual siempre finaliza con.log y sin número despuésLos registros no se archivan ni se comprimenLa mayoría de los registros tienen una estructura comúnLos archivos de registro utilizan <@> para separar las seccionesLos registros siempre se escriben en GMT+0000Los registros de la CEPE se encuentran en diferentes lugares según la instalación específica.400 implementaciones de agente De un solo lado Servidor: Servidor ubicadoUbicación: **{ECE_HOME}\eService_RT\logs**Alta disponibilidad Servidores: Ambos servidores ubicados en comúnUbicación: **{ECE_HOME}\eService\logs**El directorio creado para el recurso compartido Sistema de archivos distribuidos (DFS) sólo contiene registros de instalación y actualizaciones.Sólo el servidor que posee la función de administrador de sistemas distribuidos (DSM) escribe registros de los componentes que forman parte de la función de servicios El propietario de la función DSM se puede encontrar en la ficha Procesos del Administrador de tareas de Windows. Hay 10-15 procesos Java en este servidor que no están en el servidor secundario.Los componentes de DSM incluyen: EAAS, EAMS, Recovery, Dispatcher, Workflow, etc.Implementaciones de 1500 agentes Registros ubicados en el servidor que aloja la funciónUbicación: **{ECE_HOME}\eService\logs**Con la excepción del servidor de servicios, todos los servidores funcionan y escriben registros para todos los procesos asociados con el componenteEn una implementación de alta disponibilidad, el servidor de servicios funciona en la configuración Activo/En esperaSólo el servidor que posee la función de administrador de sistemas distribuidos (DSM) escribe registrosEl propietario del rol DSM se puede identificar por el número de procesos que se ven en el Administrador de tareas de Windows. Hay 10-15 procesos Java que se ejecutan en el servidor primario y sólo 4 procesos Java en el servidor secundarioServidores PCCE Los registros requeridos de PCCE se encuentran en, **C:\icm\tomcat\logs**Los registros de Tomcat no se traspasan ni se archivanLos registros se escriben en la hora del servidor localRecopile

todos los registros que se crearon o modificaron después de observar el problema. Una explicación completa de los registros y los problemas que se ven está fuera del alcance de este documento. A continuación se exponen algunos problemas comunes, qué revisar y algunas posibles soluciones. Problemas relacionados con el certificado Certificado no importado Comportamiento: Cuando intenta abrir el gadget ECE en SPOG, aparece el error "Error al cargar la página. Póngase en contacto con el administrador".Comprobar: El Catalina inicia sesión en PCCE por errores similares a estos javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: Fallo al construir la ruta PKIX: sun.security.Provider.certpath.SunCertPathBuilderExcepción: no se puede encontrar una ruta de certificación válida para el destino solicitadoResolución: Asegúrese de que ha importado el certificado de servidor Web de ECE o los certificados de CA adecuados en el almacén de claves en el ADSDiscordancia de certificado Comportamiento: Cuando intenta abrir el gadget ECE en SPOG, aparece un error que indica que el nombre común del certificado o el nombre alternativo del asunto no coinciden con el nombre configurado.Comprobar: Validar el certificado SSLResolución: Asegúrese de que el campo Nombre común del asunto o uno de los campos DNS del nombre alternativo del asunto contenga el nombre completo que ha introducido en SPOG como nombre de servidor Web.Problemas del sistema Servicio no iniciado Comportamiento: Cuando intenta abrir el gadget ECE en SPOG, aparece el error "La página web en https://{url} puede estar temporalmente inactiva o puede que se haya desplazado permanentemente a una nueva dirección".Comprobar: Valide que el servicio de Windows - Cisco Service se haya iniciado en todos los servidores CEPE, con la excepción del servidor Web. Revise los registros raíz en el servidor de aplicaciones para ver si hay erroresResolución: Inicie el servicio Cisco en todos los servicios de la CEPE.Problema de configuración Configuración LDAP Comportamiento: Cuando intenta abrir el gadget ECE en SPOG, aparece el error "Error al cargar la página. Póngase en contacto con el administrador".Comprobar: Aumente el nivel de seguimiento del servidor de aplicaciones al nivel 7 - Depurar, intente de nuevo el inicio de sesión y revise el registro del servidor de aplicaciones. Busque la palabra LDAP.Resolución: Valide la configuración LDAP para el SSO del administrador de particiones para asegurarse de que sea correcta.

Información Relacionada

Estos son los documentos clave que debe revisar a fondo antes de iniciar cualquier instalación o integración de la CEPE. No se trata de una lista completa de los documentos de la CEPE.

> **Precaución:** La mayoría de los documentos de la CEPE tienen dos versiones. Asegúrese de descargar y utilizar las versiones de PCCE. El título del documento es **para Packaged Contact Center Enterprise** o **(para PCCE)** o **(para UCCE y PCCE)** después del número de versión.

Asegúrese de consultar la página de inicio de la documentación de Cisco Enterprise Chat y Email

para ver si hay alguna actualización antes de realizar cualquier instalación, actualización o integración.

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

- 12.0 Guía de instalación y configuración de chat empresarial y correo electrónicoGuía de actualización de correo electrónico y chat empresarialGuía del administrador de correo electrónico y chat empresarial
- 12.5 Guía de instalación y configuración de chat empresarial y correo electrónicoGuía de actualización de correo electrónico y chat empresarialGuía del administrador de correo electrónico y chat empresarial