

Migración, instalación y configuración de ADOBE® ACROBAT® CONNECT™ PRO SERVER 7.5

© 2009 Adobe Systems Incorporated. All rights reserved.

Migración, instalación y configuración de Adobe® Acrobat® Connect™ Pro Server 7.5 para Windows®

This guide is licensed for use under the terms of the Creative Commons Attribution Non-Commercial 3.0 License. This License allows users to copy, distribute, and transmit the guide for noncommercial purposes only so long as (1) proper attribution to Adobe is given as the owner of the guide; and (2) any reuse or distribution of the guide contains a notice that use of the guide is governed by these terms. The best way to provide notice is to include the following link. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>

Adobe, the Adobe logo, Acrobat, Acrobat Connect, Adobe Connect, Adobe Press, Breeze, Flash, and JRun are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

Contenido

Capítulo 1: Preparación de la migración, instalación y configuración

Novedades de Acrobat Connect Pro Server 7.5	1
Requisitos de instalación	2
Configuraciones admitidas	3
Preparación de la migración	4
Preparación de la instalación	6

Capítulo 2: Instalación de Connect Pro

Instalación de Connect Pro Server y Flash Media Gateway	15
Verificación de la instalación	19
Instalación de Acrobat Connect Pro Edge Server	21
Desinstalación de los servidores	22

Capítulo 3: Implementación y configuración de Connect Pro

Implementación de Acrobat Connect Pro Server	24
Implementación de Acrobat Connect Pro Edge Server	28
Integración con un servicio de directorio	30
Implementación de Voz universal	38
Uso de adaptadores de telefonía integrados	44
Configuración de almacenamiento compartido	46
Configuración de los ajustes de notificación de la cuenta	49
Configuración de PDF para la conversión SWF	51
Integración con Microsoft Live Communications Server 2005 y Microsoft Office Communications Server 2007	52
Configuración de la identificación única (SSO)	57
Configuración de un proxy inverso frente al servidor Connect Pro Server	61
Host del complemento Acrobat Connect	63

Capítulo 4: Seguridad

SSL (capa de conexión segura)	65
PKI (infraestructura de clave pública)	79
Seguridad de la infraestructura	82
Sugerencias y recursos de seguridad	85

Capítulo 5: Administración de Connect Pro Server

Inicio y parada de los servidores	87
Administración y supervisión de registros	90
Mantenimiento del espacio en disco	98
Copia de seguridad de datos	99
Creación de informes personalizados	102

Capítulo 1: Preparación de la migración, instalación y configuración

Revise los requisitos de instalación, las configuraciones admitidas y una descripción general técnica mientras se prepara para diseñar e instalar un sistema Adobe® Acrobat® Connect™ Pro Server 7.5. Si está migrando a Acrobat Connect Pro Server 7.5, siga las instrucciones de copia de seguridad de los archivos.

Novedades de Acrobat Connect Pro Server 7.5

Las siguientes funciones de Acrobat Connect Pro Server 7.5 son nuevas o han cambiado:

VMWare Acrobat Connect Pro Server 7.5 añade asistencia para instalaciones en entorno VMWare. Para obtener más información, consulte el libro blanco [de Configuración de VMWare](#) y los requisitos del sistema [del Connect Pro Server](#).

Universal Voice La solución de Acrobat Connect Pro Server 7.5 Universal Voice le permite retransmitir en directo una audioconferencia para reunirse con los participantes a través de VoIP. También puede grabar la audioconferencia en directo con la reunión Connect Pro.

Para implementar la solución Universal Voice, instale y configure Adobe Flash Media Gateway al instalar Acrobat Connect Pro Server 7.5. Flash Media Gateway está integrado en el instalador de Acrobat Connect Pro Server 7.5. Flash Media Gateway permite la comunicación entre Acrobat Connect Pro Server 7.5 y su infraestructura SIP. Puede instalar Flash Media Gateway en el mismo servidor en el que tenga instalado Acrobat Connect Pro Server o en otro equipo. Consulte [“Implementación de Voz universal”](#) en la página 38.

Nota: Además de Universal Voice, Acrobat Connect Pro 7.5 también admite adaptadores de telefonía totalmente integrados con control de llamada avanzado y función de comentarios de participantes. Para obtener más información, consulta [“Opciones de audioconferencia de Connect Pro”](#) en la página 13.

Compartir archivos PDF Adobe® Comparta archivos PDF en salas de reuniones. Desde una sala de reuniones, seleccione los archivos PDF que desee compartir de la biblioteca de contenido Connect Pro Central de su equipo. En la biblioteca de contenido, los archivos PDF se almacenan como archivos PDF. Para poder visualizarlos en la sala de reuniones, los archivos PDF se convierten a archivos SWF. Para obtener más información, consulte [Compartir un documento](#).

Compatibilidad mejorada de Microsoft® PowerPoint Comparta documentos PPTX en salas de reuniones con alta fidelidad, incluidos los documentos que contengan arte SmartArt, gráficos, texto y efectos de formas. Los presentadores pueden cargar documentos PPTX en salas de reuniones de alta fidelidad desde sus sistemas operativos Windows o Mac.

Adobe Acrobat Connect Pro Add-in para Lotus Notes de IBM Programe y gestione reuniones de Adobe Acrobat Connect desde Lotus Notes. Para obtener más información, consulte [Guía de instalación e implementación de Adobe Acrobat Connect Pro Add-in para IBM Lotus Notes](#) y [Utilización de Adobe Acrobat Connect Pro Add-in para IBM Lotus Notes](#).

Vínculos Asistencia y Estado del menú Ayuda de la sala de reuniones Utilice los parámetros de configuración del archivo custom.ini para añadir los elementos Asistencia y Estado al menú Ayuda de la sala de reuniones. Especifique las direcciones URL que permiten a los usuarios de las reuniones ver información sobre las opciones de asistencia y el estado del sistema. Puede utilizar los servicios web de Acrobat Connect Pro para crear páginas con información dinámica sobre el estado del sistema. Para obtener más información, consulte “[Añadir vínculos Asistencia técnica y Estado al menú Ayuda.](#)” en la página 49.

Requisitos de instalación

Requisitos de hardware, software y usuario

Para ver los requisitos de Adobe Acrobat Connect Pro Server y Adobe Acrobat Connect Pro Edge Server, consulte www.adobe.com/go/connect_sysreqs_es.

Requisitos de puertos

La tabla siguiente describe los puertos con los que los usuarios deben poder establecer conexiones TCP.

Numérica	Dirección bind	Acceso	Protocolo
80	*/Cualquier adaptador	Público	HTTP, RTMP
443	*/Cualquier adaptador	Público	HTTPS, RTMPS
1935	*/Cualquier adaptador	Público	RTMP

Nota: RTMP (protocolo de mensajería en tiempo real) es un protocolo de Adobe.

La tabla siguiente describe los puertos abiertos dentro de un clúster. Cada servidor Acrobat Connect Pro de un clúster debe poder establecer conexiones TCP con el resto de los servidores de ese clúster mediante estos puertos.

Nota: Estos puertos no deberían ser públicos, incluso si no utiliza un clúster.

Numérica	Puerto de origen	Dirección bind	Acceso	Protocolo
8506	Cualquiera	*/Cualquier adaptador	Privado	RTMP
8507	Cualquiera	*/Cualquier adaptador	Privado	HTTP

Cada servidor Acrobat Connect Pro de un clúster debe poder establecer una conexión TCP con el servidor de la base de datos en el puerto siguiente:

Numérica	Puerto de origen	Acceso	Protocolo
1433	Cualquiera	Privado	TSQL

La tabla siguiente describe los puertos de servidor que Acrobat Connect Pro utiliza para comunicarse de forma interna. Estos puertos no deben estar en uso en un servidor que tenga instalado Acrobat Connect Pro o la aplicación podría no iniciarse.

Numérica	Dirección bind	Acceso	Protocolo
1111	127.0.0.1	Interno	RTMP
1434	127.0.0.1 Este puerto sólo está activo cuando utiliza una base de datos incrustada.	Interno	TSQL
2909	127.0.0.1	Interno	RMI
4111	*/Cualquier adaptador	Interno	JMX
8510	127.0.0.1	Interno	HTTP

Para obtener más información sobre los puertos de Flash Media Gateway, consulte [“Puertos y protocolos de Flash Media Gateway”](#) en la página 39.

Configuraciones admitidas

Configuraciones de servidor/base de datos admitidas

Adobe Connect Pro utiliza una base de datos para almacenar información sobre usuarios y contenido. Se admiten las configuraciones de base de datos y Adobe Connect Pro siguientes:

Servidor único con un motor de procesamiento de la base de datos incrustada Instale Adobe Connect Pro en un equipo único e instale el motor de procesamiento de la base de datos incrustada (incluido en el instalador de Adobe Connect Pro) en el mismo equipo. El motor de procesamiento de la base de datos integrada es Microsoft® SQL Server® 2005 Express Edition.

Nota: Esta configuración sólo debería utilizarse en entornos de prueba y no en entornos de producción.

Un solo servidor con la base de datos SQL Server 2005 Standard Edition Instale Adobe Connect Pro en un único equipo e instale Microsoft SQL Server 2005 Standard Edition en el mismo equipo.

Servidor único con una base de datos externa de SQL Server 2005 Standard Edition Instale Adobe Connect Pro en un único equipo e instale SQL Server 2005 Standard Edition en otro equipo.

Servidor único con varias bases de datos externas de SQL Server 2005 Standard Edition Instale Adobe Connect Pro en un único equipo e instale SQL Server 2005 Standard Edition en un clúster de varios equipos externo a Adobe Connect Pro. Adobe Connect Pro admite el reflejo y agrupación de bases de datos de SQL Server.

Varios servidores con una base de datos externa de SQL Server 2005 Standard Edition Instale Adobe Connect Pro en un clúster de varios servidores e instale SQL Server 2005 Standard Edition en otro equipo.

Varios servidores con varias bases de datos externas de SQL Server 2005 Standard Edition Instale Adobe Connect Pro en un clúster de varios servidores e instale SQL Server 2005 Standard Edition en otro clúster. Adobe Connect Pro admite el reflejo y agrupación de bases de datos de SQL Server.

Nota: Microsoft SQL Server 2005 Standard Edition no se incluye con Adobe Connect Pro Server 7.5 y debe adquirirse por separado.

Más temas de ayuda

[“Preparación de la instalación”](#) en la página 6

[“Instalación de Connect Pro Server y Flash Media Gateway”](#) en la página 15

Implementaciones compatibles con Flash Media Gateway

Implemente Flash Media Gateway para activar Voz Universal. Las siguientes implementaciones son compatibles:

Equipo único Instale Connect Pro Server, Flash Media Gateway y SQL Server en el mismo equipo.

Dos equipos Instale Connect Pro Server y Flash Media Gateway en el mismo equipo y SQL Server en un equipo diferente.

Un clúster de equipos Instale cada Connect Pro Server y cada Flash Media Gateway en su propio equipo.

Más temas de ayuda

“[Opciones de audioconferencia de Connect Pro](#)” en la página 13

“[Implementación de Voz universal](#)” en la página 38

Servidores de directorio LDAP admitidos

Puede configurar la autenticación de usuarios con el servicio de directorio LDAP de su organización e importar información de directorio en Acrobat Connect Pro a partir del servidor de directorio LDAP de su organización. Para obtener una lista de servidores de directorio LDAP admitidos, consulte www.adobe.com/go/connect_sysreqs_es.

Nota: Se puede integrar cualquier servidor de directorio LDAP v.3 en Acrobat Connect Pro Server 7.5. Sin embargo, sólo se admiten los servidores de directorio que hayan sido probados por Adobe.

Más temas de ayuda

“[Integración con un servicio de directorio](#)” en la página 30

Dispositivos de almacenamiento de contenido admitidos

Puede configurar el sistema de Acrobat Connect Pro para que almacene contenido en dispositivos NAS (Network Attached Storage) y SAN (Storage Area Network). Para obtener una lista de dispositivos NAS y SAN admitidos, consulte www.adobe.com/go/connect_sysreqs_es.

Más temas de ayuda

“[Configuración de almacenamiento compartido](#)” en la página 46

Preparación de la migración

Rutas de migración

Ejecute el instalador de Adobe Acrobat Connect Pro Server 7.5 para hacer la actualización de Adobe Connect Pro Server 7.x a Acrobat Connect Pro Server 7.5; ésta es la única ruta de actualización. El instalador de Acrobat Connect Pro Server y la consola de gestión de la aplicación proporcionan interfaces gráficas de usuario que le guiarán por el proceso de actualización.

Para obtener más información sobre la actualización, póngase en contacto con el servicio de asistencia técnica de Adobe: www.adobe.com/go/connect_licensed_programs_es.

Migración de Acrobat Connect Pro Server 7.x a Acrobat Connect Pro Server 7.5

Siga este flujo de trabajo para migrar de Acrobat Connect Pro Server 7.x a Acrobat Connect Pro Server 7.5.

1. Probar la migración en un entorno sin producción.

Es recomendable tomar una captura de pantalla del entorno de producción actual y probar la actualización en un entorno sin producción antes de migrar el entorno de producción. Cuando haya migrado la aplicación correctamente en un entorno de prueba, continúe con el paso 2.

2. Informar a los usuarios de la migración.

Consulte [“Informar a los usuarios de la migración”](#) en la página 5.

3. (Opcional) Realice copias de seguridad de los archivos de contenido y configuración.

Consulte [“Copias de seguridad de los archivos”](#) en la página 5.

4. Realice una copia de seguridad de la base de datos.

Consulte [“Realice una copia de seguridad de la base de datos”](#) en la página 101.

5. Ejecución del instalador Adobe Acrobat Connect Pro Server 7.5.

Consulte [“Instalación de Connect Pro Server y Flash Media Gateway”](#) en la página 15. El instalador detiene los servicios de Acrobat Connect Pro Server y realiza una copia de seguridad de los archivos existentes, incluido el archivo custom.ini.

6. Configuración de Acrobat Connect Pro Server 7.5.

Consulte [“Configuración de Acrobat Connect Pro con el Asistente para la consola de administración de la aplicación”](#) en la página 16.

7. Verificación de la instalación.

Consulte [“Verificación de la instalación”](#) en la página 19.

Informar a los usuarios de la migración

Para todas las actualizaciones de software, especialmente las que afectan a un grupo de trabajo, la comunicación y planificación son fundamentales. Antes de iniciar la migración o empezar a agregar módulos a Acrobat Connect Pro, Adobe sugiere que haga lo siguiente:

- Asigne suficiente tiempo para garantizar una migración correcta. La actualización debería adaptarse a su periodo de mantenimiento normal.
- Informe por adelantado a los usuarios de que no podrán utilizar Acrobat Connect Pro durante la migración.
- Informe a los usuarios de los tipos de cambios que se producirán (como nuevas funciones o rendimiento mejorado) tras la migración. Para obtener información sobre las novedades, consulte www.adobe.com/go/learn_cnn_whatnew_es.

Copias de seguridad de los archivos

El asistente de instalación realiza copias de seguridad de los directorios appserv y comserv y del archivo custom.ini, e instala las nuevas versiones. El asistente de instalación no borra ni sobrescribe el contenido del directorio.

Tiene la opción de realizar copias de seguridad de estos directorios y archivos.

Actualización de SQL Server 2005 Express Edition

Siga este flujo de trabajo para migrar una base de datos incrustada a SQL Server 2005 Standard Edition en otro equipo.

Nota: Esta migración se puede efectuar al migrar de Acrobat Connect Pro Server 7.x a Acrobat Connect Pro Server 7.5, pero también en cualquier momento después de instalar Acrobat Connect Pro Server 7.5.

1. Instale SQL Server 2005 Standard Edition en un equipo distinto al equipo en que se aloje Connect Pro Server.

Siga las instrucciones proporcionadas por Microsoft para instalar SQL Server.

2. Realice copias de seguridad del servidor SQL Server 2005 Express Edition.

Consulte [“Realice una copia de seguridad de la base de datos”](#) en la página 101.

3. Copie el archivo .bak del equipo que aloje el servidor Connect Pro en el equipo que aloje SQL Server.

Cuando realiza una copia de seguridad de SQL Server Express Edition, se crea un archivo llamado *breeze.bak* (en el que *breeze* es el nombre de la base de datos).

4. Restaure la base de datos en el equipo que aloja SQL Server 2005 Standard Edition.

Para obtener más información sobre la restauración de SQL Server, consulte Microsoft TechNet.

5. Introduzca la información de la base de datos de SQL Server 2005 Standard Edition en la consola de administración de la aplicación en el servidor que aloja Connect Pro.

Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server > Configuración de Adobe Acrobat Connect Pro Server 7.

Preparación de la instalación

Descripción general de Acrobat Connect Pro desde el punto de vista técnico

La instalación de Acrobat Connect Pro está formada por diversos componentes: Connect Pro Central Application Server, Adobe® Flash® Media Server, Connect Pro Service, Flash Media Gateway y una base de datos.

Connect Pro Central Application Server está compilado en J2EE con componentes de Macromedia® JRun™ de Adobe. También denominado el *servidor de aplicaciones*, gestiona usuarios, grupos, contenido bajo demanda y sesiones de cliente. Entre las tareas del servidor de aplicaciones se incluye el control de acceso, seguridad, cuotas, gestión de licencias y funciones de gestión y auditoría como tecnología de clústeres, conmutación por errores y replicación. También transcodifica medios, incluida la conversión de Microsoft® PowerPoint y audio a Adobe® Flash®. El servidor de aplicaciones se encarga de las solicitudes de reuniones y de transferencia de contenido (diapositivas, páginas HTTP, archivos SWF y archivos en el pod Compartir archivos) a través de una conexión HTTP o HTTPS.

Flash Media Server, también denominado el *servidor de reuniones*, se instala con Acrobat Connect Pro para controlar el flujo de audio y vídeo en tiempo real, la sincronización de datos y el contenido rico en medios, incluidas las interacciones de Acrobat Connect Pro. Ciertas tareas de Flash Media Server incluyen la grabación y reproducción, controlar la sincronización de audio y vídeo y transcodificar (convertir y empaquetar datos para interactuar y compartir la pantalla en tiempo real). Flash Media Server también reduce la latencia y la carga del servidor al guardar páginas Web, flujos y datos compartidos a los que se accede con frecuencia. Flash Media Server transfiere audio, vídeo y los datos de reuniones adjuntos a través del protocolo de mensajería en tiempo real de Adobe (RTMP o RTMPS).

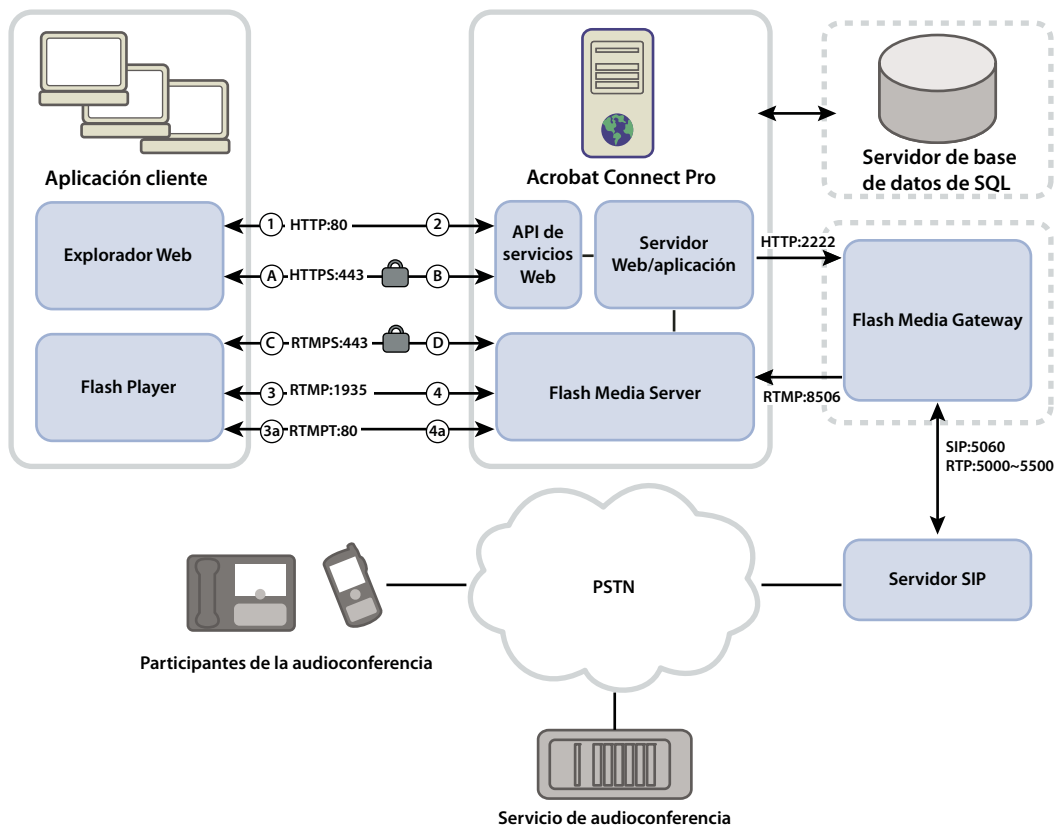
Connect Pro Presence Service integra Acrobat Connect Pro con Microsoft® Live Communication Server 2005 y Microsoft® Office Communication Server para mostrar su presencia de mensajería instantánea en las salas de reunión de Acrobat Connect Pro.

Flash Media Gateway integra Acrobat Connect Pro con su infraestructura SIP/RTP. Flash Media Gateway recibe el audio de un servidor SIP y lo envía a las salas de reunión de Connect Pro. Esta solución se denomina Voz universal.

Acrobat Connect Pro requiere una base de datos para el almacenamiento a largo plazo de metadatos de aplicaciones y transacciones, incluida la información sobre usuarios, grupos, contenido e informes. Puede utilizar el motor de procesamiento de la base de datos integrada (SQL Server 2005 Express Edition) incluida en el instalador de Acrobat Connect Pro Server 7.5, o bien comprar e instalar Microsoft SQL Server 2005 Standard Edition.

Flujo de datos

El diagrama siguiente muestra cómo fluyen los datos entre la aplicación cliente y Acrobat Connect Pro.



Los datos pueden fluir por una conexión cifrada o sin cifrar.

Conexión sin cifrar

Las conexiones sin cifrar se realizan por HTTP y RTMP y siguen las rutas descritas en la tabla. Los números de la tabla corresponden a los números en el diagrama de flujo de datos.

Numérica	Descripción
1	El explorador Web del cliente solicita una reunión o un URL de contenido a través de HTTP:80.

Numérica	Descripción
2	El servidor Web responde y transfiere el contenido o proporciona al cliente la información para que se pueda conectar a la reunión.
3	El cliente Flash Player solicita una conexión a la reunión a través de RTMP:1935.
3a	El cliente Flash Player solicita una conexión a la reunión pero sólo puede conectarse a través de RTMP:80.
4	Flash Media Server responde y abre una conexión a largo plazo para el tráfico de flujo de Acrobat Connect.
4a	Flash Media Server responde y abre una conexión por túnel para el tráfico de flujo de Acrobat Connect.

Conexión cifrada

Las conexiones cifradas se realizan a través de HTTPS y RTMPS y siguen las rutas descritas en la tabla. Las letras de la tabla corresponden a las letras en el diagrama de flujo de datos.

Letra	Descripción
A	El explorador Web del cliente solicita una reunión o un URL de contenido a través de una conexión segura en HTTPS:443.
B	El servidor Web responde y transfiere el contenido a través de una conexión segura o proporciona al cliente la información para que se pueda conectar a la reunión de forma segura.
C	El cliente Flash Player solicita una conexión segura a Flash Media Server a través de RTMPS:443.
D	Flash Media Server responde y abre una conexión segura a largo plazo para el tráfico de flujo de Acrobat Connect Pro.

Flujo de trabajo de instalación

Los pasos siguientes le ayudarán a diseñar, instalar y configurar un sistema de Acrobat Connect Pro. Ciertos pasos requieren que tome una decisión y otros pasos que realice una tarea. Cada paso le proporciona información relacionada con la decisión o tarea.

1. Elija las bases de datos que va a utilizar.

Para obtener más información, consulte [“Selección de una base de datos”](#) en la página 11.

2. Instale Acrobat Connect Pro en un único servidor.

Para obtener más información, consulte [“Instalación de Connect Pro Server y Flash Media Gateway”](#) en la página 15. Si ha seleccionado el motor de procesamiento de la base de datos incrustada en el paso 1, instálelo también. El motor de procesamiento de la base de datos incrustada forma parte del instalador de Acrobat Connect Pro.

3. Si ha seleccionado SQL Server 2005 Standard Edition en el paso 1, instálelo.

Para obtener más información, consulte la documentación de SQL Server.

4. Implemente Acrobat Connect Pro.

Para obtener más información, consulte [“Implementación de Acrobat Connect Pro Server”](#) en la página 24.

5. Verifique que Acrobat Connect Pro se haya instalado correctamente.

Para obtener más información, consulte [“Verificación de la instalación”](#) en la página 19.

6. (Opcional) Integración de Acrobat Connect Pro con su infraestructura.

Hay muchas posibilidades de integración de Acrobat Connect Pro con la infraestructura existente de su organización. Es recomendable verificar que Acrobat Connect Pro funcione tras configurar cada una de estas funciones.

Integración con un proveedor SIP Integre Acrobat Connect Pro con el proveedor SIP de su organización (también llamado *proveedor de VOIP*) para una experiencia de conferencias de audio optimizada. Consulte [“Implementación de Voz universal”](#) en la página 38.

Integración con un directorio LDAP Integre Acrobat Connect Pro con el servidor de directorio LDAP de su organización para que no tenga que gestionar varios directorios de usuarios. Consulte [“Integración con un servicio de directorio”](#) en la página 30.

Configuración de una capa de sockets seguros Lleve a cabo todas las comunicaciones de Acrobat Connect Pro de forma segura. Consulte [“SSL \(capa de conexión segura\)”](#) en la página 65.

Almacene contenido en dispositivos NAS/SAN Utilice dispositivos de red para compartir las tareas de almacenamiento de contenido. Consulte [“Configuración de almacenamiento compartido”](#) en la página 46.

Integración con Live Communication Server y Office Communication Server Integre la aplicación con un servidor de comunicaciones para que los anfitriones de reuniones vean la presencia de mensajería instantánea de los invitados en salas de reuniones. Los anfitriones de reuniones también pueden enviar mensajes a los usuarios de mensajería instantánea desde la sala de reuniones. Consulte [“Integración con Microsoft Live Communications Server 2005 y Microsoft Office Communications Server 2007”](#) en la página 52.

Configuración de una infraestructura de clave pública Si ha integrado Acrobat Connect Pro con un servidor de directorio LDAP, requiera certificados de cliente para agregar otra capa de seguridad. Consulte [“PKI \(infraestructura de clave pública\)”](#) en la página 79

Instale el complemento Adobe Connect Los usuarios pueden descargar con facilidad el complemento Acrobat Connect de los servidores de Adobe. Sin embargo, si la normativa de seguridad de su organización no permite realizar descargas externas, instale el complemento en su propio servidor y la experiencia del usuario aún será fantástica. Consulte [“Host del complemento Acrobat Connect”](#) en la página 63.

7. (Opcional) Seleccione si desea instalar Acrobat Connect Pro Server 7.5 en un clúster.

Para obtener más información, consulte [“Implementación de Acrobat Connect Pro en un clúster”](#) en la página 9 e [“Implementación de un clúster de servidores Acrobat Connect Pro”](#) en la página 24.

8. (Opcional) Seleccione si desea instalar servidores perimetrales.

Para obtener más información, consulte [“Implementación de Acrobat Connect Pro Edge Server”](#) en la página 11 e [“Implementación de Acrobat Connect Pro Edge Server”](#) en la página 28.

Implementación de Acrobat Connect Pro en un clúster

Se pueden instalar todos los componentes de Acrobat Connect Pro Server, incluida la base de datos, en un único servidor, pero este diseño de sistema es más adecuado para realizar pruebas, no para producción.

Un grupo de usuarios conectados, cada uno realizando un trabajo idéntico, normalmente se denomina *clúster*. En un clúster de Acrobat Connect Pro Server, instalará una copia idéntica de Acrobat Connect Pro Server en cada servidor del clúster.

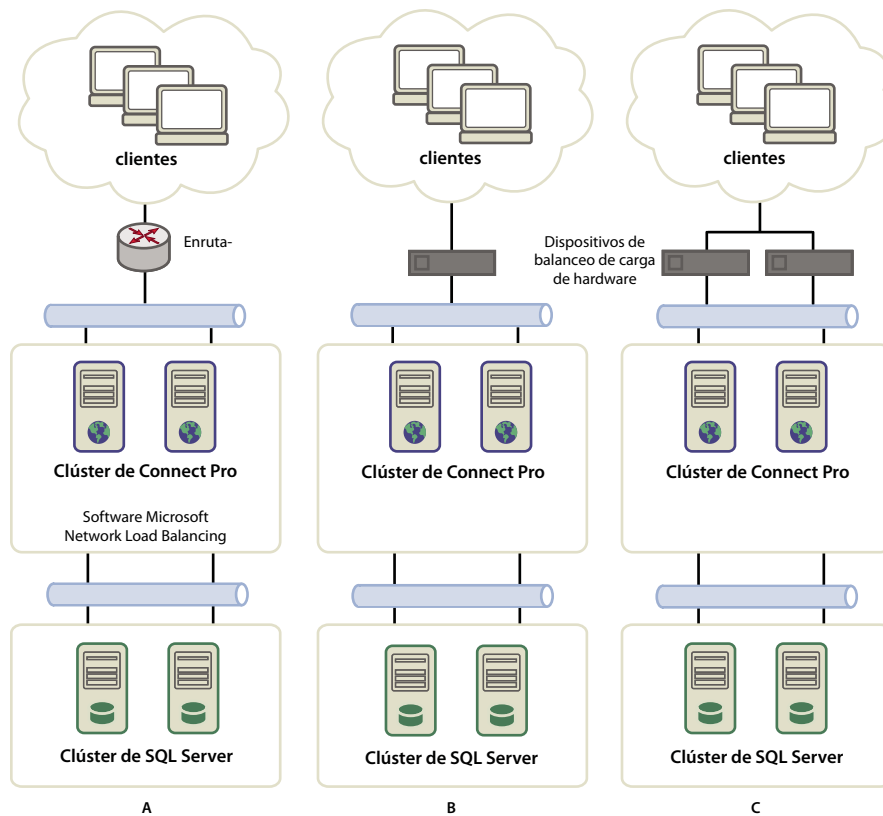
Nota: Cuando instale Acrobat Connect Pro Server en un clúster, debe utilizar SQL Server 2005 Standard Edition e instalarlo en un equipo independiente.

Si un host del clúster falla, otro host del clúster puede hacerse cargo y alojar la reunión. Debe utilizar hardware y software de terceros para proporcionar equilibrio de cargas para el clúster. A menudo, el hardware de equilibrio de cargas también puede funcionar como acelerador SSL.

Nota: En la consola de gestión de la aplicación, puede configurar el almacenamiento compartido para que el contenido se almacene en dispositivos externos y se guarde temporalmente en Acrobat Connect Pro Server.

Los sistemas en red de confianza se diseñan con componentes redundantes; si un componente falla, otro componente idéntico (*redundante*) puede encargarse del mismo trabajo. Cuando un componente falla y su contraparte se hace cargo, se ha producido una *conmutación de errores*.

Sería ideal que cada componente de un sistema fuera redundante, no sólo Acrobat Connect Pro Server. Por ejemplo, podría utilizar varios dispositivos de equilibrio de carga de hardware (como BIG-IP de F5 Networks), un clúster de servidores con Acrobat Connect Pro Server y bases de datos de SQL Server en varios equipos externos. Cree su sistema con el mayor número de redundancias posible y vaya agregándolas a su sistema cuando pueda.



Tres opciones de tecnología de clústeres

A. Un clúster con software de equilibrio de carga en red y dos bases de datos externas **B.** Dispositivos de equilibrio de carga de hardware BIG-IP, un clúster y dos bases de datos externas **C.** Dos dispositivos de equilibrio de carga BIG-IP, un clúster y dos bases de datos externas

Más temas de ayuda

[“Implementación de un clúster de servidores Acrobat Connect Pro”](#) en la página 24

[“Configuración de almacenamiento compartido”](#) en la página 46

Selección de una base de datos

Acrobat Connect Pro Server utiliza una base de datos para almacenar información sobre usuarios, contenido, cursos, reuniones e informes. Puede utilizar el motor de procesamiento de la base de datos incrustada (incluido con el instalador) o puede instalar Microsoft SQL Server 2005 Standard Edition (que deberá adquirirse por separado).

Nota: El motor de procesamiento de la base de datos incrustada es Microsoft SQL Server 2005 Express Edition.

Base de datos incrustada

El motor de procesamiento de la base de datos incrustada se recomienda para pruebas y desarrollo. Utiliza las mismas estructuras de datos que SQL Server 2005 Standard Edition, pero no es tan sólido.

El motor de procesamiento de la base de datos incrustada tiene las limitaciones siguientes:

- A causa de las restricciones de gestión de licencias, debe instalar el motor de procesamiento de la base de datos incrustada en el mismo equipo que Acrobat Connect Pro Server. El equipo debe tener un sólo procesador.
- 2 GB es el tamaño máximo de la base de datos.
- El motor de la base de datos incrustada tiene una interfaz de línea de comandos en vez de una interfaz gráfica de usuario.

Microsoft SQL Server 2005 Standard Edition

Es recomendable utilizar el motor de procesamiento de Microsoft SQL Server 2005 Standard Edition en entornos de producción porque es un sistema de gestión de bases de datos ampliable (DBMS) diseñado para admitir un gran número de usuarios al mismo tiempo. SQL Server 2005 Standard Edition también proporciona interfaces gráficas de usuario para gestionar y consultar la base de datos.

Puede instalar SQL Server 2005 Standard Edition en el mismo equipo que Acrobat Connect Pro Server o en otro equipo. Si los instala en diferentes equipos, sincronice los equipos con la misma fuente horaria. Para obtener más información, consulte la nota técnica siguiente: www.adobe.com/go/2e86ea67.

Instale SQL Server en un modo de inicio de sesión combinado para poder utilizar la autenticación SQL. Defina la base de datos para que no distinga entre mayúsculas y minúsculas.

Debe utilizar SQL Server en las situaciones de implementación siguientes:

- Si desea instalar la base de datos en un equipo que no tenga Acrobat Connect Pro Server instalado.
- Si Acrobat Connect Pro Server se implementa en un clúster.
- Si Acrobat Connect Pro Server se instala en equipos con multiprocesadores con Hyper-Threading.

Más temas de ayuda

“Configuraciones de servidor/base de datos admitidas” en la página 3

“Instalación de Connect Pro Server y Flash Media Gateway” en la página 15

Implementación de Acrobat Connect Pro Edge Server

Cuando implementa Acrobat Connect Edge Server en su red, los clientes se conectan al servidor Edge y éste se conecta a Acrobat Connect Pro (también denominado el *servidor de origen*). Esta conexión se produce sin interrupciones; los usuarios tienen la sensación de estar conectados directamente al servidor original de la reunión.

Los servidores Edge proporcionan los beneficios siguientes:

Latencia de red reducida Los servidores Edge guardan en una caché el contenido bajo demanda (como reuniones y presentaciones grabadas) y dividen los flujos en directo, lo que produce menos tráfico hacia el origen. Los servidores Edge colocan los recursos más cerca de los clientes.

Seguridad Los servidores Edge son una capa adicional entre la conexión a Internet del cliente y el origen.

Si la licencia se lo permite, puede instalar y configurar un clúster de servidores Edge. La implementación de servidores Edge en un clúster tiene los beneficios siguientes:

Conmutación por error Cuando un servidor Edge falla, los clientes se enrutan a otro servidor Edge.

Compatibilidad con eventos de gran tamaño Si se requieren más de 500 conexiones simultáneas a la misma reunión, con un servidor Edge único los sockets se agotarán. Un clúster permite más conexiones a la misma reunión.

Equilibrio de cargas Si requiere más de 100 reuniones simultáneas, un sólo servidor Edge no tendrá suficiente memoria. Los servidores Edge pueden agruparse tras un equilibrador de carga.

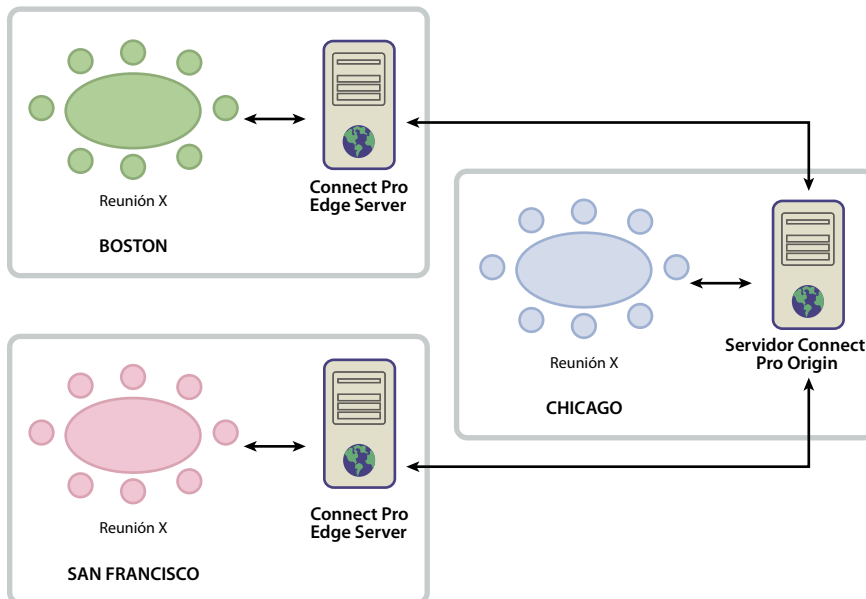
Funcionamiento de los servidores Edge

Los servidores Edge autentican a los usuarios y autorizan sus solicitudes de servicios Web como Acrobat Connect Pro Meeting en vez de utilizar sus recursos para reenviar cada solicitud al servidor de origen. Si los datos solicitados se encuentran en el caché del servidor Edge, devuelve los datos al cliente solicitante sin llamar a Acrobat Connect Pro.

Si los datos solicitados no se encuentran en el caché del servidor Edge, el servidor reenvía la solicitud del cliente al servidor de origen, en el que el usuario se autentica y se autoriza la solicitud de servicios. El servidor de origen devuelve los resultados al servidor Edge solicitante y el servidor Edge proporciona los resultados al cliente solicitante. El servidor Edge también almacena esta información en el caché, desde donde será accesible para otros usuarios autenticados.

Ejemplo de implementación de servidor Edge

Considere el ejemplo siguiente de implementación de servidor Edge:



Los clientes de Chicago utilizan el origen situado en un centro de datos de Chicago. Los servidores Edge en Boston y San Francisco acumulan las solicitudes de cliente locales y las reenvían al origen. Los servidores Edge reciben las respuestas del origen en Chicago y las transmiten a los clientes en sus zonas.

Más temas de ayuda

[“Instalación de Acrobat Connect Pro Edge Server”](#) en la página 21

[“Implementación de Acrobat Connect Pro Edge Server”](#) en la página 28

Creación y optimización de un entorno VMWare

La instalación de Connect Pro Server en VMWare es similar a su instalación en un equipo físico. Para obtener más información sobre los requisitos de hardware, software y de configuración, consulte las [notas del producto](#) sobre la ejecución de Connect Pro Server en un entorno virtual.

Opciones de audioconferencia de Connect Pro

Connect Pro admite dos maneras de conectar proveedores de conferencias de audio: Voz universal y adaptadores de telefonía integrados. Cada solución aporta ventajas diferentes. Puede configurar una solución o ambas soluciones para un único proveedor de conferencias de audio. Puede configurar cualquier número de proveedores de conferencias de audio para una cuenta Connect Pro.

Voz universal habilita a Connect Pro para recibir audio de cualquier proveedor de conferencias de audio. Puede grabar el audio junto con la conferencia Web y transmitirlo sólo a asistentes VoIP.

La solución de Voz universal utiliza un componente llamado Flash Media Gateway que se instala con Connect Pro Server. Flash Media Gateway recibe el audio de un servidor SIP y lo envía a Connect Pro a través de RTMP. Para utilizar la opción Voz universal necesita disponer de su propio servidor SIP o de una cuenta con un proveedor SIP. Para obtener más información sobre la configuración de Flash Media Gateway, consulte [“Implementación de Voz universal”](#) en la página 38.

Una vez que haya implementado la Voz universal, los administradores de la cuenta pueden utilizar la central de Connect Pro para configurar los datos de conferencia de audio. Para obtener más información, consulte www.adobe.com/go/learn_cnn_uvconfig_es.

Los **Adaptadores de telefonía integrados** son extensiones de Java que facilitan la comunicación entre Connect Pro y proveedores de conferencias de audio específicos. Los adaptadores de telefonía integrados proporcionan un mejor control de llamada. Adobe proporciona distintos adaptadores telefónicos integrados en www.adobe.com/go/learn_cnn_adaptors_es.

Además, puede utilizar la API de Java de Connect Pro Telephony para desarrollar un adaptador de telefonía integrado para cualquier proveedor de conferencias de audio. Para obtener más información, consulte [Uso de Telefonía con Adobe Acrobat Connect Pro](#).

Puede configurar la Voz universal para los adaptadores de telefonía integrados. Consulte [“Configuración de la Voz universal para los adaptadores de telefonía integrados”](#) en la página 44.

La siguiente tabla describe las funciones de las dos soluciones:

	Proveedor de audio de Universal Voice	Adaptador de telefonía integrado
Difusión de audio sólo para asistentes VoIP	Sí	No (a menos que el adaptador esté configurado para Voz universal)
Control de llamadas mejorado. Por ejemplo, silenciar, retener, etc.	No	Sí
Grabación de audio con una reunión Connect Pro	Sí	Sí
Requiere Flash Media Gateway (incorporado en el programa de instalación de Connect Pro)	Sí	No (a menos que el adaptador esté configurado para Voz universal)

Capítulo 2: Instalación de Connect Pro

Para instalar Acrobat Connect Pro Server 7.5, Acrobat Connect Pro Edge Server 7.5 y Flash Media Gateway, ejecute el instalador y siga las instrucciones del Asistente para la consola de administración de la aplicación.

Instalación de Connect Pro Server y Flash Media Gateway

Ejecución del instalador

- 1 Inicie sesión como administrador en el equipo.
- 2 Cierre todas las aplicaciones.
- 3 Inserte el DVD de instalación en la unidad de DVD. En la pantalla de inicio, haga clic en el botón de instalación de Adobe Acrobat Connect Pro Server 7.5.

Si la instalación no se inicia automáticamente, haga doble clic en el archivo install.exe ubicado en Connect\7.5\Disk1\InstData\VM\install.exe.

- 4 Seleccione un idioma y haga clic en Aceptar para continuar.
- 5 En la pantalla de introducción, haga clic en Siguiente para continuar.
- 6 Seleccione cualquiera de los siguientes productos que desee instalar y haga clic en Siguiente para continuar:
 - servidor de Connect Pro
 - Flash Media Gateway

Nota: Si no dispone de un proveedor de canal de subida SIP/VOIP, no instale Flash Media Gateway. Para obtener más información, consulta “[Opciones de audioconferencia de Connect Pro](#)” en la página 13.

- 7 En la pantalla de Contrato de licencia, seleccione Acepto los términos del contrato de licencia y haga clic en Siguiente.
- 8 Lleve a cabo una de las siguientes operaciones para seleccionar la ubicación de la instalación de Connect Pro Server y, a continuación, haga clic en Siguiente:
 - Haga clic en Siguiente para aceptar la ubicación de instalación predeterminada de Connect Pro Server (c:\breeze) o haga clic en Elegir para seleccionar una ubicación diferente.
 - Si ha seleccionado una ubicación diferente y decide utilizar la ubicación predeterminada en su lugar, haga clic en Restaurar carpeta predeterminada.
 - Si Acrobat Connect Pro ya está instalado en este equipo, aparece la pantalla Actualizar la instalación existente de Connect Pro. Seleccione la casilla de verificación para confirmar que ha realizado una copia de seguridad de la base de datos y del directorio raíz de Connect Pro.
- 9 Lleve a cabo una de las siguientes acciones para seleccionar la ubicación de la instalación de Flash Media Gateway y, a continuación, haga clic en Siguiente:
 - Haga clic en Siguiente para aceptar la ubicación de instalación predeterminada (C:\Program Files\Adobe\Flash Media Gateway) o haga clic en Elegir para seleccionar una ubicación diferente.

- Si ha seleccionado una ubicación diferente y decide utilizar la ubicación predeterminada en su lugar, haga clic en Restaurar carpeta predeterminada.
- Si Flash Media Gateway ya está instalado en este equipo, aparecerá la pantalla de instalación Actualizar Flash Media Gateway existente.

10 Introduzca el número de serie y haga clic en Siguiente.

Nota: Adobe le ha enviado un correo electrónico con un vínculo al sitio de licencias de Adobe. Siga el vínculo para recuperar su número de serie.

11 Si aparece la pantalla del motor de procesamiento de la base de datos integrada, lleve a cabo una de las siguientes acciones:

- Si tiene intención de instalar una base de datos en un equipo diferente, seleccione No instalar el motor de procesamiento de la base de datos integrada.
- Para instalar la base de datos integrada, seleccione Instalar el motor de procesamiento de la base de datos integrada en la siguiente ubicación. Para llevar a cabo la instalación en la ubicación predeterminada (c:\Program Files\Microsoft SQL Server), haga clic en Siguiente. Para seleccionar una ubicación diferente, haga clic en Elegir.

Nota: Si el instalador detecta que Microsoft SQL Server ya está instalado en este equipo, el instalador no instalará la base de datos. Si está migrando y ya se está utilizando la base de datos integrada, Connect Pro utiliza la base de datos existente. Sin embargo, a veces el instalador detecta una versión antigua de SQL Server que no funciona con Connect Pro. Siga los pasos que se exponen en “[Desinstalación de Acrobat Connect Pro Server](#)” en la página 22 e inicie la instalación de nuevo.

12 Si tiene instalado el motor de procesamiento de la base de datos integrada, introduzca una contraseña segura y haga clic en Siguiente.

13 Revise el resumen previo a la instalación. Haga clic en Anterior para cambiar esta configuración. Haga clic en Instalar para instalar el software.

14 En la pantalla Inicializando el servicio Connect Pro, realice una de las acciones siguientes y haga clic en Siguiente:

- Seleccione Iniciar Connect Pro... (recomendado).
- Seleccione No inicie Connect Pro ahora...

Si elige iniciar Connect Pro después del siguiente reinicio, configure Connect Pro antes de iniciarlo por primera vez. Para abrir la consola de administración de la aplicación con el fin de configurar Connect Pro, seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server > Configurar Connect Pro Enterprise Server.

15 Si ha elegido iniciar Connect Pro, aparecerá un mensaje que le informará de que el servicio se está iniciando.

Acrobat Connect Pro Server se ejecuta como cuatro servicios de Windows: Adobe Connect Enterprise Service, Flash Media Server (FMS), Flash Media Administration Server y Acrobat Connect Pro Presence Server. Flash Media Gateway se ejecuta como el servicio Flash Media Gateway. Consulte “[Inicio y parada de los servidores](#)” en la página 87

16 Haga clic en Hecho para salir del instalador.

Si elige Iniciar Connect Pro, se abre el Asistente para la consola de administración de la aplicación en un explorador para guiarlo por las tareas de configuración.

Configuración de Acrobat Connect Pro con el Asistente para la consola de administración de la aplicación

Después de instalar Acrobat Connect Pro, el instalador iniciará el Asistente de la consola de administración de la aplicación. El asistente le guiará durante la configuración de los ajustes de la base de datos y el servidor, la carga de su archivo de licencia y la creación de un administrador.

Nota: Si se está ejecutando otra aplicación en el puerto 80, no se podrá abrir la consola de administración de la aplicación. Detenga la aplicación que se esté ejecutando en el puerto 80 y vuelva a abrir la consola de administración de la aplicación.

Para acceder a la consola de administración de la aplicación, seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server > Configuración de Connect Pro Enterprise Server o utilice la siguiente URL: <http://localhost:8510/console>.

1. Lea la pantalla de bienvenida.

La pantalla de bienvenida ofrece una descripción general del asistente.

2. Introduzca los ajustes de la base de datos.

Establezca los valores de los parámetros indicados a continuación. Haga clic en Siguiente para conectarse a la base de datos y revisar los ajustes.

Host de la base de datos El nombre host del equipo en el que se ha instalado la base de datos. Si ha instalado una base de datos incrustada, el valor es localhost.

Nombre de la base de datos El nombre de la base de datos. El valor predeterminado es breeze.

Puerto de la base de datos El puerto que la base de datos utiliza para comunicarse con Acrobat Connect Pro. El valor predeterminado es 1433. Si utiliza el motor de la base de datos incrustada, cambie el valor a 1434.

Usuario de la base de datos El nombre del usuario de la base de datos. Si ha instalado una base de datos incrustada, el valor predeterminado es sa.

Contraseña del usuario de la base de datos La contraseña para el usuario de la base de datos. Si ha instalado la base de datos integrada, establezca la contraseña en el instalador.

3. Introduzca los ajustes del servidor.

Nombre de la cuenta Un nombre que identifica la cuenta de Acrobat Connect Pro, como “Cuenta de Acrobat Connect Pro 7”.

Host de Connect Pro Un nombre de dominio completo (FQDN) que los clientes utilizarán para conectarse a Acrobat Connect Pro. Por ejemplo, si el URL de la cuenta es <http://connect.ejemplo.com>, el valor Host de Connect Pro sería connect.ejemplo.com.

Puerto HTTP El puerto que Acrobat Connect Pro utiliza para comunicarse con HTTP. El valor predeterminado es 80. Si introduce un valor que no sea 80, los clientes deberán agregar el número de puerto al nombre de host en la dirección URL cuando accedan a la cuenta de Acrobat Connect Pro.

Asignaciones de host Nombre es el nombre de host del equipo en el que está instalado Acrobat Connect Pro. Nombre externo es el FQDN que los clientes utilizan para conectarse a Acrobat Connect Pro.

Nota: No agregue un puerto al FQDN en el cuadro Nombre externo.

Host SMTP El nombre host del equipo en el que está instalado el servidor de correo SMTP.

Nombre de usuario SMTP el nombre de usuario empleado para autenticarse con el host SMTP. Si este campo se deja en blanco, Connect Pro intentará enviar correos electrónicos sin autenticarse con el servidor SMTP.

Contraseña SMTP La contraseña del nombre de usuario SMTP.

Correo electrónico del sistema La dirección de correo electrónico desde la que se envían mensajes administrativos.

Correo electrónico de asistencia técnica La dirección de correo electrónico de asistencia técnica para los usuarios de Acrobat Connect Pro.

Correo electrónico de CCO Una dirección de correo electrónico de copia oculta a la que también se envían todas las notificaciones de usuario. Esta variable permite el seguimiento administrativo de mensajes de correo electrónico enviados a través de Acrobat Connect Pro sin mostrar una dirección de correo electrónico interna.

Almacenamiento compartido Un volumen y directorio en un servidor externo en el que se almacena contenido, por ejemplo, \\volumen\directorio. Si desea almacenar contenido en varios volúmenes, sepárelos con punto y coma (;). Antes de configurar esta función, consulte “[Configuración de almacenamiento compartido](#)” en la página 46.

Tamaño de caché de contenido Un número entero entre 1 y 100 que especifica el porcentaje de espacio libre en el disco que puede utilizarse para almacenar contenido en Acrobat Connect Pro. La caché puede superar el porcentaje especificado, por lo que es recomendable mantener el valor entre 15 y 50. Si deja el cuadro en blanco o introduce 0, no se utiliza la caché y el contenido se refleja en Acrobat Connect Pro y los volúmenes externos. Antes de configurar esta función, consulte “[Configuración de almacenamiento compartido](#)” en la página 46.

4. Introduzca la configuración de Flash Media Gateway.

Introduzca los nombres de los equipos y los nombres externos de los servidores Flash Media Gateway. Los ajustes no surtirán efecto de forma inmediata. Cuando haga clic en Aceptar para confirmar los ajustes, es posible que Connect Pro reinicie todos los servidores Flash Media Gateway. Los ajustes se insertan en todos los servidores Flash Media Gateway de un clúster.

Haga clic en Añadir para añadir servidores de Flash Media Gateway. Introduzca los siguientes parámetros:

Nombre El nombre del equipo en el que se aloje Flash Media Gateway, por ejemplo, jperez-pc.

Nombre externo El FQDN del servidor en el que se aloje Flash Media Gateway, por ejemplo, jperez-pc.ejemplo.com.

Nota: No agregue un puerto al FQDN en el cuadro Nombre externo.

El Estado indica si Connect Pro Server puede o no conectarse al servidor Flash Media Gateway. Es posible que el servidor Flash Media Gateway tarde unos segundos en activarse. Un estado "Activo" no implica que la configuración SIP se haya insertado en el servidor de Flash Media Gateway. Si no se puede conectar Connect Pro Server a Flash Media Gateway, el estado será "Inactivo".

Haga clic en Siguiente e introduzca los siguientes parámetros:

Nombre de usuario el nombre de usuario del perfil SIP que utiliza el servidor Flash Media Gateway para crear las sesiones SIP, por ejemplo sipUN1.

Contraseña La contraseña del perfil SIP que utiliza el servidor Flash Media Gateway para crear sesiones SIP.

Dirección SIP La dirección del servidor SIP para el perfil SIP que utiliza Flash Media Gateway para crear sesiones SIP, por ejemplo, 10.12.13.14:12345.

Host predeterminado El host predeterminado para el perfil SIP. Este parámetro es la dirección del servidor SIP que se debe utilizar si falla el registro con el servidor SIP. Este parámetro se configura normalmente con la misma dirección que la dirección IP

Registro Seleccione si debe registrarse un servidor de Flash Media Gateway en un servidor SIP.

Puerto SIP El puerto en el que el servidor Flash Media Gateway escucha las solicitudes SIP, por ejemplo, 5060.

Límite inferior del puerto El número de puerto inferior que se puede utilizar para los datos de audio RTP. El valor predeterminado es 5000.

Límite superior del puerto El número más alto del puerto que se puede utilizar para los datos de audio. El valor predeterminado es 6000.

Caducidad del registro El intervalo, en segundos, en el que Flash Media Gateway renueva su registro con el servidor SIP. El valor predeterminado es 2400 segundos.

5. Cargue el archivo de licencia.

Acrobat Connect Pro no se habilitará hasta que descargue un archivo de licencia de Adobe y lo instale en el equipo en el que esté instalado Acrobat Connect Pro. Haga clic en el vínculo para descargar el archivo de licencia de Adobe. A continuación, examine el archivo de licencia descargado para copiarlo en su instalación de Acrobat Connect Pro.

6. Cree un administrador de cuentas.

Cada cuenta de Acrobat Connect Pro precisa al menos un administrador para realizar tareas en la aplicación Web Connect Pro Central. Las cuentas actualizadas ya dispondrán de un administrador de cuenta como mínimo, pero aquí podrá agregar otro.

7. Continúe utilizando Acrobat Connect Pro.

Desde esta pantalla, podrá iniciar sesión en Connect Pro Central (la aplicación Web que le permite gestionar su cuenta, crear reuniones, eventos, etc. y gestionar contenido en el equipo en el que esté instalado Acrobat Connect Pro), volver a la consola de administración de la aplicación (para cambiar o revisar los ajustes) o consultar la documentación para obtener más información sobre Acrobat Connect Pro.

Verificación de la instalación

Verifique la conectividad de la base de datos

Si puede iniciar sesión en Connect Pro Central (una aplicación Web de Acrobat Connect Pro), la base de datos y Acrobat Connect Pro son compatibles.

1 Vaya al URL siguiente: `http://[hostname]`.

Nota: En este URL, `[hostname]` es el valor configurado para el Host de Connect Pro en la consola de gestión de la aplicación.

2 Introduzca el Id. de inicio de sesión y la contraseña establecidos en la consola de gestión de la aplicación.

Si puede iniciar la sesión correctamente, aparecerá la ficha de inicio de Connect Pro Central.

Comprobar que puede enviar notificaciones por correo electrónico

Si no ha introducido ningún valor en el campo Host SMTP de la consola de administración de la aplicación, Acrobat Connect Pro no podrá enviar notificaciones por correo electrónico. Si ha introducido un Host SMTP, lleve a cabo la siguiente operación para comprobar que Connect Pro puede enviar notificaciones por correo electrónico:

1 Haga clic en la ficha Administración en la ficha de inicio de Connect Pro Central.

2 Haga clic en la ficha Usuarios y grupos.

3 Haga clic en Nuevo usuario.

4 En la página Información de nuevo usuario, introduzca la información requerida. A continuación se muestra una lista parcial de opciones:

Correo electrónico Utilice la dirección de correo electrónico del nuevo usuario. Asegúrese de seleccionar la opción Enviar un correo electrónico con los datos de la cuenta de usuario, inicio de sesión y contraseña.

Nueva contraseña Cree una contraseña de 4 a 16 caracteres.

5 Haga clic en Siguiente para continuar.

6 En el encabezado Editar pertenencia al grupo, seleccione un grupo, asigne el usuario al grupo y haga clic en Finalizar.

7 Deje suficiente tiempo para que el usuario vea su notificación por correo electrónico.

Si el usuario recibe la notificación, Acrobat Connect Pro funciona y puede enviar mensajes a través de su servidor de correo electrónico.

8 Si el correo electrónico no llega, haga lo siguiente:

a Compruebe que la dirección de correo electrónico sea válida.

b Compruebe que el correo electrónico no se haya filtrado como correo no deseado.

c Compruebe que haya configurado Acrobat Connect Pro con un host SMTP válido y que el servicio SMTP funcione fuera de Acrobat Connect Pro.

d Póngase en contacto con el servicio de asistencia técnica de Adobe en www.adobe.com/go/connect_licensed_programs_es.

Verificar que puede utilizar Adobe Presenter

Para verificar que puede utilizar Adobe Presenter, envíe una presentación de Microsoft PowerPoint a Acrobat Connect Pro para compilarla en una presentación de Flash y visualícela.

Para poder enviar una presentación de PowerPoint a Acrobat Connect Pro, instale Adobe Presenter en un equipo que ya disponga de PowerPoint.

1 Inicie un navegador y abra Connect Pro Central (<http://localhost:8510>, o el FQDN de su Connect Pro Server).

2 Haga clic en Recursos > Introducción.

3 En la página Introducción, haga clic en Publicar presentaciones > Instalar Adobe Presenter.

4 Inicie la ejecución del instalador.

5 Si no dispone de una presentación Power Point, cree y guarde una presentación de una o dos diapositivas.

6 Seleccione Publicar en el menú de Adobe Presenter en PowerPoint para abrir el Asistente para la publicación de Connect Pro.

7 Seleccione Connect Pro e introduzca la información de su servidor.

8 Inicie una sesión con su dirección de correo electrónico y contraseña y siga los pasos siguientes en el Asistente para la publicación. Compruebe que esté matriculado en el grupo Autores (Administración > Usuarios y grupos en Connect Pro Central).

Cuando complete los pasos en el asistente para la publicación, Adobe Presenter carga su presentación de PowerPoint a Connect Pro, que la compila en una presentación de Flash.

9 Cuando se haya completado la compilación, vaya a la ficha Contenido en Connect Pro Central y busque la presentación.

10 Abra la presentación para verla.

Verifique que puede utilizar Training

Nota: Adobe Acrobat Connect Pro Training es una función opcional que debe habilitarse en su licencia.

❖ Vaya a la ficha Formación en Connect Pro Central.

Si la ficha Formación está visible y es accesible, Training funciona. Compruebe que esté matriculado en el grupo Administradores de formación (Administración > Usuarios y grupos).

Verificar que puede utilizar Meeting

Nota: Adobe Acrobat Connect Pro Meeting es una función opcional que debe habilitarse en su licencia.

Para verificar que Acrobat Connect Pro Meeting funciona, debe estar matriculado en el grupo Anfitriones de reunión o Administradores.

- 1 Inicie una sesión en Connect Pro Central como usuario matriculado en el grupo Anfitriones de reunión o Administradores.
- 2 Haga clic en la ficha Reuniones y seleccione Nueva reunión.
- 3 En la página Introducir información de la reunión, introduzca la información requerida. Para la opción Acceso a la reunión, seleccione la opción Sólo los usuarios registrados y los invitados admitidos pueden entrar en la sala. Haga clic en Finalizar para crear la reunión.
- 4 Haga clic en el botón Entrar en la sala de reuniones.
- 5 Inicie una sesión para entrar en la reunión como Usuario registrado.
- 6 Si aparece la ventana del complemento Acrobat Connect, siga las instrucciones para instalarlo.

Si se abre la sala de la reunión, Acrobat Connect Pro Meeting funciona.

Verificar que puede utilizar Events

Nota: Adobe Acrobat Connect Pro Events es una función opcional que debe habilitarse en su licencia.

- 1 Inicie una sesión en Connect Pro Central como usuario matriculado en el grupo Responsables de eventos o Administradores.
- 2 Vaya a la ficha Gestión de eventos de Connect Pro Central.

Si esta ficha está visible y es accesible, Connect Pro Events funciona.

Instalación de Acrobat Connect Pro Edge Server

Ejecución del instalador

- 1 Cierre todas las demás aplicaciones.
- 2 Inserte el DVD de instalación en la unidad de DVD. En la pantalla de inicio, haga clic en el botón de instalación de Adobe Acrobat Connect Pro Edge Server

Si el instalador no se inicia automáticamente, haga doble clic en el archivo edgsetup.exe de la carpeta raíz de instalación del DVD.

- 3 Seleccione un idioma del cuadro de diálogo Seleccionar idioma de configuración. Haga clic en Aceptar para continuar.
- 4 En la pantalla de configuración, haga clic en Siguiente para continuar.
- 5 En la pantalla de Acuerdo de licencia, seleccione Acepto el acuerdo y haga clic en Siguiente.

6 Realice una de las siguientes acciones:

- Haga clic en Siguiente para aceptar la ubicación de instalación predeterminada (c:\breeze) o haga clic en Examinar para seleccionar una ubicación diferente y haga clic en Siguiente.
- Si Adobe Acrobat Connect Edge Server ya está instalado en este equipo, aparece la pantalla Actualizando la Instalación de Adobe Acrobat Connect Pro Edge Server existente. Haga clic en Siguiente.

7 En la pantalla Seleccionar carpeta del menú inicio, realice una de las acciones siguientes:

- Haga clic en Siguiente para aceptar la ubicación predeterminada de los accesos directos del menú Inicio.
- Haga clic en Examinar para seleccionar una ubicación diferente.

8 En el cuadro de diálogo Listo para instalar, compruebe la ubicación en la que se instalarán Adobe Acrobat Connect Pro Edge Server y la carpeta Menú Inicio. Haga clic en Atrás para comprobar o cambiar estos ajustes o haga clic en Instalar.

9 Haga clic en Finalizar para salir de la instalación de Adobe Acrobat Connect Pro Edge Server 7.

Más temas de ayuda

[“Implementación de Acrobat Connect Pro Edge Server”](#) en la página 28

Desinstalación de los servidores

Desinstalación de Acrobat Connect Pro Server

Nota: La desinstalación de Acrobat Connect Pro Server no desinstala SQL Server.

- 1 Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server > Desinstalar Connect Pro Server.
- 2 Elimine la carpeta raíz Acrobat Connect Pro. La ubicación predeterminada es c:\breeze.

Cuando se desinstala Acrobat Connect Pro, los archivos custom.ini, config.ini y los archivos de contenido no se eliminan. Si elimina la carpeta raíz, se eliminarán estos archivos.

Importante: La carpeta raíz contiene la carpeta de contenidos. Si desea conservar el contenido, cópiela en otra ubicación.

- 3 Seleccione Inicio > Ejecutar. Introduzca **regedit** y haga clic en Aceptar para abrir el Editor del registro.
 - a Navegue a Mi PC -> HKEY_LOCAL_MACHINE -> SOFTWARE -> MICROSOFT -> WINDOWS -> CurrentVersion -> Desinstalar.
 - b Seleccione y elimine todas las claves de Adobe Acrobat Connect Pro (los títulos pueden contener una cadena de versión).
- 4 (Opcional) Si el motor de procesamiento de la base de datos estaba instalado, elimine las siguientes claves de registro:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLSERVER

Desinstalación de Acrobat Connect Pro Edge Server

- 1 Seleccione Inicio > Configuración > Panel de control > Agregar o quitar programas > Adobe Acrobat Connect Pro Edge Server > Quitar.
- 2 Elimine la carpeta raíz Acrobat Connect Pro. La ubicación predeterminada es c:\breeze.

Desinstalación de Flash Media Gateway

Flash Media Gateway se desinstala cuando desinstala Acrobat Connect Pro Server. También puede ejecutar el siguiente programa para desinstalar Flash Media Gateway: Program Files\Adobe\Flash Media Gateway\Uninstall_Flash Media Gateway\ Uninstall Flash Media Gateway.exe.

Capítulo 3: Implementación y configuración de Connect Pro

Tras instalar Adobe Acrobat Connect Pro Server, Flash Media Gateway o Adobe Acrobat Connect Pro Edge Server y completar la primera fase de configuración con la consola de administración de la aplicación, configure cualquiera de las características opcionales e implemente el servidor.

Implementación de Acrobat Connect Pro Server

Implementación de Acrobat Connect Pro Server

1 En su servidor DNS, defina un nombre de dominio completo (FQDN) para Acrobat Connect Pro (como connect.miempresa.com). Asigne el nombre de dominio a la dirección IP estática del equipo en el que esté instalado Acrobat Connect Pro.

2 Si desea que Acrobat Connect Pro esté disponible fuera de la red, configure los puertos siguientes en un servidor de seguridad:

80 El puerto predeterminado para el servidor de la aplicación Acrobat Connect Pro. El puerto terciario para el servidor de reuniones (Flash Media Server).

1935 El puerto predeterminado para el servidor de reuniones (Flash Media Server).

443 El puerto predeterminado para SSL. El puerto secundario para el servidor de reuniones (Flash Media Server).

Nota: Si el tráfico de Acrobat Connect Pro se enruta a través de una puerta de enlace (con una dirección IP diferente), compruebe que el servidor de seguridad esté configurado para aceptar solicitudes de la dirección IP de la puerta de enlace.

Para obtener ayuda para la implementación de Acrobat Connect Pro, póngase en contacto con el servicio de asistencia técnica de Adobe en www.adobe.com/go/connect_licensed_programs_es.

Más temas de ayuda

[“Requisitos de puertos”](#) en la página 2

Implementación de un clúster de servidores Acrobat Connect Pro

Antes de implementar un clúster, necesitará lo siguiente:

- Una licencia que admita el número de nodos de su clúster. Para obtener más información, póngase en contacto con su representante de Adobe.
- Cada equipo del clúster debe disponer de una dirección IP estática y una entrada DNS.
- Un servidor de correo electrónico.
- Una instalación de servidor SQL Server 2005 Standard Edition en un equipo específico con una dirección IP estática. Si instala Acrobat Connect Pro en un clúster, no puede utilizar el motor de procesamiento de bases de datos incrustadas. Todos los servidores con Acrobat Connect Pro se conectan a la base de datos, pero las restricciones de licencia sólo permiten que un servidor se conecte al motor de procesamiento de la base de datos incrustada.

- Una solución de equilibrio de carga de hardware o software. Los dispositivos de equilibrio de carga requieren un equipo independiente con una dirección IP estática y una entrada DNS. El software se puede instalar en uno de los nodos del clúster.
- Un volumen de almacenamiento compartido o más. Esta configuración no es obligatoria pero se recomienda.

Antes de implementar Acrobat Connect Pro en un clúster, realice una instalación correcta en un solo equipo. Configure las funciones adicionales (por ejemplo, SSL, una integración de servicios de directorio, identificación única, almacenamiento de contenido compartido, etc.) y compruebe que funcionen correctamente en un solo servidor.

1 Instale y configure Acrobat Connect Pro en un servidor dedicado.

Utilice el mismo número de serie y archivo de licencia cada vez que instale Acrobat Connect Pro. No instale el motor de procesamiento de la base de datos incrustada y, si el almacenamiento compartido precisa un nombre de usuario y una contraseña, no inicie Acrobat Connect Pro desde el instalador.

2 Si el almacenamiento compartido precisa un nombre de usuario y una contraseña, haga lo siguiente para agregarlos a Adobe Connect Enterprise Service:

- a Abra el panel de control Servicios.
- b Haga doble clic en el servicio Adobe Connect Enterprise.
- c Haga clic en la ficha Iniciar sesión.
- d Haga clic en el botón de selección Esta cuenta e introduzca el nombre de usuario del almacenamiento compartido en el cuadro. La sintaxis del nombre de usuario es [subdominio\]nombre de usuario.
- e Introduzca y confirme la contraseña del almacenamiento compartido.
- f Haga clic en Aplicar y, a continuación, en Aceptar.

3 Para iniciar Acrobat Connect Pro, haga lo siguiente:

- a En el panel de control Servicios, seleccione Flash Media Server (FMS) y haga clic en Iniciar el servicio.
- b En el panel de control Servicios, seleccione el servicio Adobe Connect Enterprise y haga clic en Iniciar el servicio.

4 Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Configuración de Connect Pro Server 7 para abrir el Asistente para la consola de gestión de la aplicación. Haga clic en Siguiente.

5 Introduzca la información de la base de datos de SQL Server en la pantalla Ajustes de la base de datos y haga clic en Siguiente.

Si Acrobat Connect Pro conecta correctamente con la base de datos, verá una confirmación y los ajustes de la base de datos. Haga clic en Siguiente.

6 En la ventana Ajustes del servidor, haga lo siguiente y haga clic en Siguiente:

- a Introduzca un nombre de cuenta.
- b En el cuadro Host de Connect Pro, introduzca el nombre del equipo que ejecuta el equilibrador de carga.
- c Introduzca un número de puerto HTTP. Este número podría ser 80 o 8080 según el equilibrador de carga.
- d Introduzca el nombre externo del nodo de clúster.
- e Introduzca el nombre de dominio del host SMTP y las direcciones de correo electrónico del sistema y de asistencia.
- f Si está utilizando almacenamiento compartido, introduzca la ruta del volumen o los volúmenes (separe volúmenes múltiples con punto y coma).
- g Introduzca el porcentaje del servidor Acrobat Connect Pro que desea utilizar como caché local.

Nota: El contenido se escribe en la caché local y el volumen de almacenamiento compartido. El contenido permanece en la caché local durante 24 horas desde la última vez que se utilizó. Tras 24 horas, si se ha superado el porcentaje de la caché, el contenido se depura.

- 7 Cargue el archivo de licencia y haga clic en Siguiente.
- 8 Cree un administrador y haga clic en Finalizar.
- 9 Repita los pasos del 1 al 8 para cada servidor del clúster.
- 10 Para configurar el equilibrador de carga, haga lo siguiente:
 - a Configure el equilibrador de carga para que escuche al puerto 80.
 - b Agregue todos los nombres de clúster al archivo de configuración del equilibrador de carga.

Nota: Para obtener información detallada sobre la configuración del equilibrador de carga, consulte la documentación del distribuidor.

- 11 Abra un explorador Web e introduzca el nombre de dominio del equilibrador de cargas, por ejemplo, `http://connect.ejemplo.com`.

Para obtener ayuda con la implementación de clústeres, póngase en contacto con el servicio de asistencia técnica de Adobe en www.adobe.com/go/connect_licensed_programs_es.

Más temas de ayuda

“Instalación de Connect Pro Server y Flash Media Gateway” en la página 15

“Configuración de almacenamiento compartido” en la página 46

Verificación de operaciones en un clúster

Si un equipo en un clúster se cierra, el equilibrador de carga enruta todas las solicitudes de HTTP a un equipo activo del clúster.

Cuando se inicia una reunión, el servidor de la aplicación asigna un host primario y de respaldo a la sala de reuniones según la carga. Cuando el host primario se cierra, el cliente se reconecta al host de respaldo.

También es recomendable verificar que el contenido cargado en un servidor de un clúster se replique en los otros equipos del clúster.

Los procedimientos siguientes asumen que el clúster contiene dos equipos, el Equipo1 y el Equipo2.

Verificación del equilibrio de cargas y conmutación de error de reuniones

- 1 Inicie Acrobat Connect Pro en ambos equipos.
 - a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Meeting Server.
 - b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

- 2 Inicie una sesión en Connect Pro Central desde el URL siguiente:

`http://[nombredehost]`

Para *nombredehost*, utilice el valor Host de Connect Pro introducido en la consola de gestión de la aplicación.

- 3 Seleccione la ficha Reuniones y haga clic en un vínculo de reunión para entrar en una sala de reuniones.

Cree una nueva reunión si es necesario.

4 Detenga Acrobat Connect Pro en el Equipo2.

- a** Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
- b** Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Meeting Server.

Si la conmutación de errores de la reunión funcionó correctamente, la reunión debería continuar mostrando una luz de conexión verde.

5 En Connect Pro Central, haga clic en cualquier ficha o vínculo.

Si el equilibrador de carga funciona, debería ser capaz de enviar solicitudes a Connect Pro Central correctamente y recibir respuestas.

Si el clúster contiene más de dos equipos, aplique este procedimiento de iniciar/detener a cada equipo del clúster.

Verificación de la replicación de contenido**1 Inicie Acrobat Connect Pro en el Equipo1.**

- a** Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Meeting Server.
- b** Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

2 Detenga Acrobat Connect Pro en el Equipo2.

- a** Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
- b** Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Meeting Server.

3 Inicie una sesión en Connect Pro Central desde el URL siguiente:

`http://[nombredehost]`

Para *nombredehost*, introduzca el valor Host de Connect Pro introducido en la consola de gestión de la aplicación.

4 Cargue una imagen JPEG u otro contenido en Acrobat Connect Pro en el Equipo1:

- Compruebe que sea miembro del grupo Autores. Si es un administrador de cuentas, puede agregarse al grupo Autores en Connect Pro Central.
- Haga clic en la ficha Contenido.
- Haga clic en Nuevo contenido y siga los pasos que se muestran en el explorador para agregar contenido.

Tras haber cargado el contenido de la prueba, se abre la página Contenido del usuario y se muestra una lista del contenido que le pertenezca.

5 Haga clic en el vínculo del contenido actualizado de prueba.

Se abre una página de Datos sobre el contenido con un URL para ver el contenido de prueba.

6 Anote el URL; lo utilizará en el paso 10.**7 Haga clic en el URL.****8 Inicie el Equipo2, espere hasta que Acrobat Connect Pro se haya iniciado completamente y detenga el Equipo1.**

Si ha configurado un dispositivo de almacenamiento externo, no tiene que esperar a que el Equipo2 se detenga; el contenido requerido se copia desde el dispositivo externo.

9 Cierre la ventana del explorador en la que estaba visualizando el contenido de prueba.**10 Abra una nueva ventana del explorador y vaya al URL para ver el contenido de prueba.**

Si se muestra el contenido de prueba, la replicación en el Equipo2 se realizó correctamente. Una ventana en blanco o un mensaje de error significan que la replicación ha fallado.

Implementación de Acrobat Connect Pro Edge Server

Flujo de trabajo de instalación de Acrobat Connect Pro Edge Server

1. Diseñe las zonas del servidor Edge.

Puede configurar servidores Edge o clústeres de servidores Edge en ubicaciones diferentes o *zonas* para asignar y equilibrar el acceso a Acrobat Connect Pro. Por ejemplo, puede configurar un servidor Edge en San Francisco para los usuarios de la costa occidental de Estados Unidos y un servidor Edge en Boston para los de su costa oriental.

2. Instale Acrobat Connect Pro Edge Server.

Instale Acrobat Connect Pro Edge Server en cada equipo de cada zona. Por ejemplo, si tiene un clúster de servidores Edge en una zona, instale Acrobat Connect Pro Edge Server en cada equipo en el clúster. Consulte [“Instalación de Acrobat Connect Pro Edge Server”](#) en la página 21

3. Modifique el servidor DNS para cada zona.

Asigne el FQDN del servidor de origen de Acrobat Connect Pro a la dirección IP estática de Acrobat Connect Pro Edge Server en cada zona. Consulte [“Implementación de Acrobat Connect Pro Edge Server”](#) en la página 28.

4. Configure el servidor Edge.

Debe agregar parámetros de configuración al archivo custom.ini de cada servidor de Acrobat Connect Pro Edge Server. Consulte [“Implementación de Acrobat Connect Pro Edge Server”](#) en la página 28.

5. Configure el servidor de origen.

Debe agregar parámetros de configuración al archivo custom.ini de cada servidor de Acrobat Connect Pro. Asimismo, debe ajustar el Nombre externo de cada servidor Edge en la consola de gestión de la aplicación en el servidor de origen. Consulte [“Implementación de Acrobat Connect Pro Edge Server”](#) en la página 28.

6. Configure un equilibrador de carga.

Si configura varios servidores Edge en una zona, debe utilizar un equilibrador de carga para equilibrar la carga entre servidores Edge y configurarlo para que escuche al puerto 80. Los servidores Edge escuchan al puerto 8080. Para obtener más información, consulte la documentación proporcionada por el proveedor del equilibrador de carga.

Implementación de Acrobat Connect Pro Edge Server

Antes de implementar los servidores Edge, verifique si Acrobat Connect Pro y las funciones adicionales (por ejemplo, SSL, una integración de servicio de directorios, identificación única o almacenamiento de contenido compartido) se ejecutan correctamente.

- 1 En el servidor DNS, asigne el FQDN del servidor de origen a la dirección IP estática del servidor Edge. Si instala servidores Edge en varias zonas, repita este paso para cada zona.

Nota: Si lo prefiere, puede utilizar un archivo de host; en ese caso, cada cliente debe tener un archivo host que dirija la dirección IP estática del servidor Edge al FQDN del servidor de origen.

- 2 En Acrobat Connect Edge Server, abra el archivo `[dir_instal_raíz]\edgeserver\win32\conf\HttpCache.xml` y sustituya el nombre del equipo en la etiqueta `HostName` con el FQDN del equipo del servidor Edge, por ejemplo `edge1.ejemplo.com`.

```
<!-- The real name of this host. -->  
<HostName>edge1.yourcompany.com</HostName>
```

- 3 En Acrobat Connect Pro Edge Server, cree un archivo nuevo `[dir_instal_raíz]\edgeserver\custom.ini` e introduzca los siguientes parámetros y valores:

FCS_EDGE_HOST El FQDN del servidor Edge, por ejemplo, `FCS_EDGE_HOST=edge1.yourcompany.com`.

FCS_EDGE_REGISTER_HOST El FQDN del servidor de origen de Acrobat Connect Pro, por ejemplo,
`FCS_EDGE_REGISTER_HOST=connect.yourcompany.com`.

FCS_EDGE_CLUSTER_ID El nombre del clúster. Cada clúster de servidor Edge debe tener un id. único. Cada equipo dentro del clúster debe tener el mismo id. El formato recomendado es *nombredeempresa-nombredelclúster*, por ejemplo, `FCS_EDGE_CLUSTER_ID=yourcompany-es`.

Nota: Debe configurar este parámetro incluso si sólo implementa un servidor Acrobat Connect Pro Edge Server.

FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT La dirección IP o el nombre de dominio y número de puerto del equipo en el que está instalado Acrobat Connect Pro, por ejemplo,

`FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80`. Acrobat Connect Pro Edge Server se conecta al servidor de origen de Acrobat Connect Pro en esta ubicación.

FCS_EDGE_PASSWORD (Optativo) Una contraseña para el servidor Edge. Si establece un valor para este parámetro, debe ajustar el mismo valor para cada servidor Edge y servidor de origen.

FCS_EDGE_EXPIRY_TIME (Optativo) El número de milisegundos que cada servidor Edge debe registrarse en el servidor de origen antes de que caduque del clúster y el sistema cambie a otro servidor Edge. Empiece con el valor predeterminado, `FCS_EDGE_EXPIRY_TIME=60000`.

FCS_EDGE_REG_INTERVAL (Opcional) El intervalo, en milisegundos, en que el servidor Edge intenta registrarse con el servidor de origen. Este parámetro determina la frecuencia con la que el servidor Edge se pone a disposición del servidor de origen. Empiece con el valor predeterminado, `FCS_EDGE_REG_INTERVAL=30000`.

DEFAULT_FCS_HOSTPORT (Opcional) Para configurar los puertos del servidor Edge, agregue la línea siguiente:
`DEFAULT_FCS_HOSTPORT=:1935,80,-443`.

El signo menos (-) delante de 443 indica que el puerto 443 es un puerto seguro que recibe sólo conexiones RTMPS. Si intenta solicitar una conexión RTMPS al puerto 1935 o 80, la conexión fallará. Asimismo, una conexión RTMP no segura al puerto 443 fallará.

Nota: Si el servidor Edge utiliza un acelerador de hardware externo, no hace falta configurar el puerto 443 como puerto seguro.

A continuación encontrará los valores de ejemplo del archivo `config.ini`:

```
FCS_EDGE_HOST=edge.yourcompany.com  
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com  
FCS_EDGE_CLUSTER_ID=yourcompany-us  
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

- 4 Reinicie el servidor Edge.

- 5 En el servidor de origen de Acrobat Connect Pro, abra el archivo `[dir_instal_raíz]\custom.ini` en un editor de textos y asigne el valor del parámetro `FCS_EDGE_CLUSTER_ID` a un id. de zona; la sintaxis es `edge.FCS_EDGE_CLUSTER_ID = id-zona`. Debe asignar el nombre de id. de clúster a un id. de zona incluso si implementa sólo un servidor Edge.

Cada clúster de servidor Edge debería tener un id. de zona. El id. de zona puede ser cualquier número entero mayor que 0. Por ejemplo, puede tener tres clústeres asignados a las zonas de la 1 a la 3:

```
edge.yourcompany-us=1
edge.yourcompany-apac=2
edge.yourcompany-emea=3
```

A continuación se muestra un archivo custom.ini de ejemplo para el servidor de origen:

```
DB_HOST=localhost
DB_PORT=1433
DB_NAME=breeze
DB_USER=sa
DB_PASSWORD=#V1#4cUsRJ6oeFwZLnQPpS4f0w==
# DEBUG LOGGING SETTINGS
HTTP_TRACE=yes
DB_LOG_ALL_QUERIES=yes
# EDGE SERVER SETTINGS
edge.yourcompany-us=1
```

Nota: Si define un parámetro `FCS_EDGE_PASSWORD` en el archivo `config.ini` del servidor Edge, defina la misma contraseña en el archivo `custom.ini` del servidor de origen.

- 6 Reinicie el servidor de origen.
- 7 En el servidor de origen, abra la consola de gestión de la aplicación (Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Configuración de Connect Pro Server 7). Seleccione la ficha Ajustes de la aplicación, a continuación seleccione Ajustes del Servidor y, en la sección Asignaciones de host, introduzca el Nombre externo del servidor Edge. El Nombre externo debe ser idéntico al valor establecido para el parámetro `FCS_EDGE_HOST` en el servidor Edge.
- 8 En el servidor de origen, configure el servidor de seguridad de Windows para que los servidores Edge puedan acceder al puerto 8506.
- 9 Repita los pasos del 2 al 4 para cada servidor Edge en cada zona.
- 10 Repita los pasos del 5 al 7 para cada servidor de origen en cada zona.

Para obtener asistencia con la implementación de los servidores Edge, póngase en contacto con el servicio de asistencia técnica de Adobe en www.adobe.com/go/connect_licensed_programs_es.

Más temas de ayuda

“Implementación de Acrobat Connect Pro Edge Server” en la página 11

Integración con un servicio de directorio

Descripción general de la integración del servicio de directorio

Puede integrar Acrobat Connect Pro con un servicio de directorio para autenticar usuarios con un directorio LDAP y no tener que agregar los usuarios y grupos individuales de forma manual. En Acrobat Connect Pro, las cuentas de usuario se crean automáticamente por medio de sincronizaciones manuales o programadas con el directorio de su organización.

Para integrarlo con Acrobat Connect Pro, el servidor del directorio debe utilizar un protocolo de acceso ligero a directorio (LDAP) o un protocolo de acceso ligero a directorio seguro (LDAPS). LDAP es un protocolo de Internet cliente-servidor para buscar información de contacto de usuario a partir de un servidor de directorio compatible con LDAP.

Acrobat Connect Pro se conecta a un directorio LDAP como cliente LDAP. Acrobat Connect Pro importa usuarios y grupos y sincroniza su información con el directorio LDAP. También puede configurar Acrobat Connect Pro para que autentique usuarios con el directorio LDAP.

Acrobat Connect Pro puede integrarse con cualquier servicio de directorio compatible con LDAP. Para obtener una lista de directorios LDAP, consulte www.adobe.com/go/connect_sysreqs_es.

Acerca de la estructura de directorio LDAP

Los directorios LDAP organizan la información según la normativa X.500.

Un usuario o grupo en un directorio LDAP se denomina una *entrada*. Una entrada es una colección de atributos. Un atributo consiste en un tipo y uno o más valores. Los tipos utilizan cadenas mnemónicas, como `ou` para unidad organizativa (organizational unit) o `cn` para nombre común (common name). Los valores de atributo consisten en información como el número de teléfono, dirección de correo electrónico y foto. Para averiguar la estructura de directorio LDAP de su organización, póngase en contacto con su administrador de LDAP.

Cada entrada tiene un *nombre de reconocimiento* (DN) que describe una ruta hasta la entrada a través de una estructura de árbol desde la entrada a la raíz. El DN de una entrada en el directorio LDAP es una combinación del nombre de la entrada (denominado *nombre de reconocimiento relativo*, RDN) y los nombres de sus entradas antecesoras en la estructura de árbol.

Una estructura de árbol puede reflejar ubicaciones geográficas o límites departamentales en una empresa. Por ejemplo, si Alicia Solis es una usuaria en el departamento de QA de Acme, Inc. en Francia, el DN para esta usuaria podría ser el siguiente:

```
cn=Alicia Solis, ou=QA, c=Francia, dc=Acme, dc=com
```

Importación de las ramificaciones de directorios

Al importar usuarios y grupos de un directorio LDAP en Acrobat Connect Pro, especificará una ruta a una sección del árbol LDAP mediante el DN de la sección. Esto especifica el alcance de la búsqueda. Por ejemplo, puede ser que desee importar sólo los usuarios de un grupo particular en su organización. Para ello, debe saber donde están ubicadas las entradas de este grupo en la estructura de árbol del directorio.

Una técnica usual es utilizar el dominio de Internet de la organización como raíz para la estructura de árbol. Por ejemplo, Acme, Inc. podría utilizar `dc=com` para especificar el elemento raíz del árbol. Un DN que especifica la oficina de ventas de Singapur de Acme, Inc. podría ser `ou=Singapur, ou=Marketing, ou=Empleados, dc=Acme, dc=com`. En este ejemplo, `ou` es una abreviatura de unidad organizativa y `dc` es una abreviatura de componente de dominio (domain component).

Nota: Todos los directorios LDAP no tienen una única raíz. En este caso, puede importar ramificaciones independientes.

Importación de usuarios y grupos

Hay dos formas de estructurar las entradas de usuario y grupo en un directorio LDAP: bajo el mismo nodo de una ramificación o bajo ramificaciones diferentes.

Si los usuarios y grupos están bajo el mismo nodo en una ramificación LDAP, los ajustes de usuario y grupo para importar entradas contienen el mismo DN de ramificación. Esto quiere decir que, cuando importe usuarios, debe utilizar un filtro para seleccionar sólo usuarios y, cuando importe grupos, debe utilizar un filtro para seleccionar sólo grupos.

Si usuarios y grupos están bajo ramificaciones diferentes en el árbol, utilice un DN de ramificación que seleccione la ramificación de usuario cuando importe los usuarios y la ramificación de grupo cuando importe los grupos.

También puede importar subramificaciones para importar usuarios de todas las ramificaciones por debajo de un cierto nivel. Por ejemplo, si deseara importar todos los empleados del departamento de ventas, podría utilizar el DN de ramificación siguiente:

```
ou=Sales, dc=Acme, dc=com
```

Sin embargo, los representantes de ventas pueden estar en subramificaciones. En ese caso, en la pantalla Asignación del perfil de usuario, ajuste el parámetro Búsqueda de subárbol a `true` para garantizar que se importen usuarios de las subramificaciones por debajo de dicho nivel en el árbol.

Filtrado de entradas seleccionadas

Un filtro especifica una condición que una entrada debe cumplir para ser seleccionada. Esto limita la selección a entradas dentro de una parte del árbol. Por ejemplo, si el filtro especifica `(objectClass=organizationalPerson)`, sólo las entradas que tengan el atributo `organizationalPerson` se seleccionarán para importarse.

***Nota:** El atributo `objectClass` debe estar presente en cada entrada en el directorio LDAP.*

Grupos y usuarios internos y externos

Los usuarios y grupos que cree directamente en Acrobat Connect Pro en vez de importarlos desde un directorio LDAP se denominan usuarios y grupos *internos*. Los usuarios y grupos importados en la base de datos de Acrobat Connect Pro desde un directorio LDAP se denominan usuarios y grupos *externos*.

Para garantizar que los grupos importados se mantengan sincronizados con el directorio LDAP externo, no puede agregar usuarios y grupos internos a grupos externos. Sin embargo, puede agregar usuarios y grupos externos a grupos internos.

Si el valor del inicio de sesión o el nombre de una entrada de usuario o grupo importada coincide con el inicio de sesión de un grupo o usuario interno existente, si sincroniza los directorios cambiará el grupo o usuario importado de interno a externo y pondrá una advertencia en el registro de sincronización.

Integración de Acrobat Connect Pro con un directorio LDAP

La integración del servicio de directorio se produce en la ficha Ajustes del servicio de directorio de la consola de administración de la aplicación. Utilice una cuenta de administrador.

Puede configurar un servidor de directorio para la autenticación de usuarios y sincronización con LDAP. La configuración puede apuntar a una o varias bifurcaciones de un servicio de directorio.

1. Abrir la consola de gestión de la aplicación.

Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Configuración de Connect Pro Server 7.

2. Introduzca los ajustes de conexión del servidor LDAP.

Seleccione la ficha Ajustes del servicio de directorio. Introduzca valores en la pantalla Ajustes LDAP > Ajustes de conexión y haga clic en Guardar.

Cuando haga clic en Guardar, Acrobat Connect Pro prueba la conexión a LDAP. Si el resultado de la prueba es negativo, verá el mensaje siguiente: Los ajustes se guardaron correctamente, pero no se pudo comprobar la conexión con LDAP. Compruebe el puerto y URL de LDAP.

Campo	Valor predeterminado	Descripción
URL del servidor LDAP	Sin valor predeterminado.	La forma usual es <code>ldap://[servername:portnumber]</code> . Si su organización utiliza un servidor LDAP seguro, utilice <code>ldaps://</code> . Si no especifica un puerto, Acrobat Connect Pro utiliza el puerto LDAP estándar (389) o el puerto LDAPS (636). LDAPS requiere certificados SSL. Si configura Acrobat Connect Pro para que funcione con un bosque de Microsoft Active Directory cuando se habilita Global Catalog, utilice Global Catalog (puerto estándar: 3268).
Método de autenticación por conexión LDAP	Sin valor predeterminado.	El mecanismo para autenticar las credenciales (nombre de usuario LDAP, contraseña de LDAP) de la cuenta del servicio LDAP para Acrobat Connect Pro (derechos de administración). Simple (configuración estándar; recomendada). Anónimo (sin contraseña; el servidor LDAP debe estar configurado para permitir los inicios de sesión anónimos). Digest MD5 (configure el servidor LDAP para permitir la autenticación por resumen).
Nombre de usuario de conexión de LDAP	Sin valor predeterminado.	Inicio de sesión administrativo en el servidor LDAP.
Contraseña de conexión de LDAP	Sin valor predeterminado.	Contraseña administrativa en el servidor LDAP.
Tiempo de espera de consulta LDAP	Sin valor predeterminado.	El tiempo que puede pasar hasta que se cancele la consulta, en segundos. Si deja el campo vacío, no hay tiempo de espera. Establezca el valor en 120.
Límite de tamaño de página de consulta de entrada LDAP	Sin valor predeterminado.	El tamaño de página de los resultados devueltos por el servidor LDAP. Si este cuadro está en blanco o es 0, no se utiliza un tamaño de página. Utilice este campo para los servidores LDAP que tienen configurado un tamaño máximo de resultados. Establezca el tamaño de página a un valor inferior al tamaño de resultados máximo de forma que todos los resultados se recuperen del servidor en varias páginas. Por ejemplo, si intenta integrar un directorio LDAP de gran tamaño que sólo puede mostrar 1.000 usuarios y quiere importar 2.000 usuarios, la integración no se realizará correctamente. Si establece el Tamaño de página de consulta en 100, los resultados se devolverán en 20 páginas y se importarán todos los usuarios.

A continuación se muestra un ejemplo de sintaxis LDAP para ajustes de conexión:

```
URL:ldap://ldapservidor.mycompany.com
UserName:MYCOMPANY\jdoe
Password:password123
Query timeout:120
Authentication mechanism:Simple
Query page size:100
```

3. Asignación de los perfiles de usuario de Acrobat Connect Pro y directorio LDAP.

Seleccione la ficha Asignación de perfil de usuario, introduzca los valores y haga clic en Guardar.

Campo	Valor predeterminado	Descripción
Iniciar sesión	Sin valor predeterminado.	El atributo de inicio de sesión del servicio del directorio.
Nombre	Sin valor predeterminado.	El atributo de nombre del servicio de directorio.
Apellido	Sin valor predeterminado.	El atributo de apellido del servicio de directorio.
Correo electrónico	Sin valor predeterminado.	El atributo de correo electrónico del servicio de directorio.

Si ha definido campos personalizados, se agregarán a la pantalla Asignación de perfil de usuario. Este ejemplo asigna un perfil de usuario de Acrobat Connect Pro a un perfil de usuario de LDAP Active Directory; Inicio de sesión de red es un campo personalizado.

```
Login:mail
FirstName:givenName
LastName:sn
Email:userPrincipalName
NetworkLogin:mail
```

4. (Opcional) Agregue una ramificación de usuario.

Haga clic en Agregar para agregar información de usuario de una ramificación concreta de su empresa. Introduzca valores en los campos Ramificación y Filtro y haga clic en Guardar.

Si desea importar usuarios de subramificaciones, seleccione True en el menú Búsqueda de subárbol; en el caso contrario, seleccione False.

Para obtener más información, consulte “[Acerca de la estructura de directorio LDAP](#)” en la página 31.

Campo	Valor predeterminado	Atributo/notas LDAP
DN de ramificación	Sin valor predeterminado.	DN (nombre de reconocimiento) del nodo raíz de la ramificación. Se muestra un vínculo a la ramificación seleccionada.
Filtro	Sin valor predeterminado.	La cadena del filtro de consulta.
Búsqueda de subárbol	True	True o False. Un valor True inicia una búsqueda recursiva de todos los subárboles de la ramificación.

5. Asignación de los perfiles de grupo de Acrobat Connect Pro y directorio LDAP.

Seleccione la ficha Asignación de perfil de grupo, introduzca los valores y haga clic en Guardar.

Nota: Los perfiles de grupo de Acrobat Connect Pro no admiten campos personalizados.

Campo	Valor predeterminado	Atributo/notas LDAP
Nombre de grupo	Sin valor predeterminado.	El atributo de nombre de grupo del servicio de directorio.
Miembro del grupo	Sin valor predeterminado.	El atributo de miembro del grupo del servicio de directorio.

A continuación verá una asignación entre los atributos de entrada de grupo LDAP y un perfil de grupo de Acrobat Connect Pro:

```
Name:cn
Membership:member
```

6. (Opcional) Agregue una ramificación de grupo.

Haga clic en **Agregar** para agregar información de usuario de una ramificación concreta de su organización. Introduzca valores en los campos **Ramificación** y **Filtro** y haga clic en **Guardar**.

Si desea importar grupos de subramificaciones, seleccione **True** en el menú **Búsqueda de subárbol**; en el caso contrario, seleccione **False**.

Para obtener más información, consulte [“Acerca de la estructura de directorio LDAP”](#) en la página 31.

Campo	Valor predeterminado	Atributo/notas LDAP
DN de ramificación	Sin valor predeterminado.	DN (nombre de reconocimiento) del nodo raíz de la ramificación. Cada ramificación de la organización tiene su propio atributo DN de LDAP. Se muestra un vínculo a la ramificación seleccionada.
Filtro	Sin valor predeterminado.	La cadena del filtro de consulta.
Búsqueda de subárbol	True	Un valor booleano de <code>true</code> o <code>false</code> . Un valor <code>true</code> inicia una búsqueda recursiva de todos los subárboles de la ramificación.

El ejemplo siguiente muestra una sintaxis de LDAP para agregar una ramificación de la organización y definir sus grupos:

```
DN: cn=USERS,DC=myteam,DC=mycompany,DC=com
Filter: (objectClass=group)
Subtree search:True
```

7. Introducción de los ajustes de autenticación.

Seleccione la ficha **Ajustes de autenticación**. Si desea autenticar usuarios de Acrobat Connect Pro con el servicio de directorio de su organización, seleccione **“Habilitar la autenticación por directorio LDAP”**. Si no selecciona esta opción, Acrobat Connect Pro utiliza la autenticación nativa (las credenciales de usuario almacenadas en la base de datos de Acrobat Connect Pro).

Si selecciona, **“Habilitar una alternativa para Connect Pro si la autenticación del directorio LDAP no tiene éxito”**, Acrobat Connect Pro utiliza la autenticación nativa.

Nota: Esta opción es útil en caso de un error de conexión LDAP temporal en la red. No obstante, las credenciales LDAP pueden diferir de las de la base de datos de Acrobat Connect Pro.

Seleccione **“Crear una cuenta de usuario de Connect Pro tras autenticar correctamente con el directorio LDAP”** para aceptar a los usuarios que se conecten al servidor de Acrobat Connect Pro por primera vez si se autentican correctamente en LDAP. Si todos los usuarios de su servicio de directorio pueden utilizar Acrobat Connect Pro, deje seleccionada esta opción y seleccione **“Interno”** como tipo de cuenta de usuario. Para obtener más información, consulte [“Grupos y usuarios internos y externos”](#) en la página 32.

Seleccione **“Habilitar la matriculación en grupo sólo en el primer inicio de sesión”** para crear un id. de inicio de sesión en Acrobat Connect Pro y colocar los usuarios en grupos especificados cuando inicien sesión en Acrobat Connect Pro por primera vez. Introduzca los grupos en el cuadro **Nombres de grupo**.

8. Programe una sincronización.

Seleccione la ficha **Ajustes de sincronización**. En la pantalla **Ajustes de programación**, seleccione la casilla de verificación **Habilitar sincronización programada** para programar sincronizaciones regulares una vez al día, a la semana o al mes a una hora determinada. Para obtener más información, consulte [“Prácticas recomendadas de sincronización”](#) en la página 36.

También puede realizar una sincronización manual en la pantalla **Acciones de sincronización**.

9. Establezca una normativa de contraseñas y una normativa de eliminación.

Seleccione la ficha Ajustes de normativa, seleccione una Normativa de configuración de contraseñas y una Normativa de eliminación y haga clic en Guardar. Para obtener más información sobre la normativa de contraseñas, consulte “[Gestión de contraseñas](#)” en la página 36.

Nota: Si selecciona la opción Eliminar usuarios y grupos... durante una sincronización, todos los usuarios externos que se hayan eliminado del servidor LDAP también se eliminarán del servidor Acrobat Connect Pro.

10. Previsualice la sincronización.

Seleccione la ficha Acciones de sincronización. En la sección Previsualizar la sincronización de directorio, haga clic en Previsualizar. Para obtener más información, consulte “[Prácticas recomendadas de sincronización](#)” en la página 36.

Gestión de contraseñas

Si no habilita la autenticación LDAP, debe escoger cómo autenticará Acrobat Connect Pro a los usuarios.

Cuando Acrobat Connect Pro importa la información de usuario de un directorio externo, no importará las contraseñas de red. Por lo tanto, implemente otro método de gestión de contraseñas para los usuarios importados en el directorio de Acrobat Connect Pro.

Notificación a los usuarios de la necesidad de establecer una contraseña

En la pantalla Ajustes de normativa de la ficha Ajustes de Sincronización, puede elegir enviar un correo electrónico a los usuarios importados con un vínculo que les permite establecer una contraseña.

Establecer un atributo LDAP como contraseña

Puede elegir que la contraseña inicial de un usuario importado sea el valor de un atributo en la entrada de directorio de dicho usuario. Por ejemplo, si el directorio LDAP contiene un campo de número de id. de empleado, podría establecer este número como contraseña inicial para los usuarios. Cuando los usuarios inician la sesión con esta contraseña, pueden cambiar sus contraseñas.

Prácticas recomendadas de sincronización

Como administrador, puede sincronizar Acrobat Connect Pro con el directorio LDAP externo de dos formas:

- Puede programar la sincronización de forma que se produzca a intervalos regulares.
- Puede realizar una sincronización manual que sincronice inmediatamente el directorio Acrobat Connect Pro con el directorio LDAP de la organización.

Antes de importar usuarios y grupos en una sincronización inicial, es recomendable utilizar un explorador LDAP para verificar los parámetros de conexión. Los exploradores siguientes están disponibles en línea: LDAP Browser/Editor y LDAP Administrator.

Importante: No reinicie el servidor LDAP ni ejecute otras tareas durante la sincronización. Si lo hiciera, usuarios o grupos podrían eliminarse de Acrobat Connect Pro.

Sincronizaciones programadas

Se recomienda realizar sincronizaciones programadas porque garantizan que Acrobat Connect Pro tiene una imagen actualizada de los usuarios y grupos importados del directorio LDAP de la organización.

Si está importando un gran número de usuarios y grupos, la sincronización inicial puede utilizar un número importante de recursos. En este caso, se recomienda programar la sincronización inicial en una hora de poco tráfico, como por la noche. Si lo prefiere, puede realizar la sincronización inicial de forma manual.

Para configurar una sincronización programada, utilice la pantalla Ajustes de sincronización > Ajustes de programación en la consola de administración de la aplicación.

Cuando se produce una sincronización, Acrobat Connect Pro compara las entradas de directorio LDAP con las entradas de directorio Acrobat Connect Pro e importa sólo las que contengan al menos un campo modificado.

Previsualización de la sincronización

Antes de importar usuarios y grupos en una sincronización inicial, Adobe recomienda que previsualice la sincronización para probar las asignaciones. En una previsualización, los usuarios y grupos no llegan a importarse, pero se registran errores; puede examinar estos errores para diagnosticar problemas en la sincronización.

Para acceder a los registros de sincronización, utilice la pantalla Registros de sincronización. Cada línea del registro muestra un evento de sincronización; la sincronización produce al menos un evento para cada (usuario o grupo) principal procesado. Si se generan advertencias o errores durante la previsualización, se indican en un segundo registro de advertencia.

Valores del archivo de registro

Los registros de sincronización almacenan valores en un formato separado por comas. En las tablas siguientes, *principal* se refiere a las entradas de usuario y grupo. Los valores siguientes se incluyen en las entradas de registro:

Campo	Descripción
Fecha	El valor de hora-fecha formateado, hasta milisegundos. El formato es <i>aaaaMMddT'HHmms.SSS</i> .
Id. principal	El inicio de sesión o nombre de grupo.
Tipo de principal	Un carácter único: U para usuario, G para grupo.
Evento	La acción tomada o condición que se ha producido.
Detalle	Información detallada sobre el evento.

La tabla siguiente describe los diferentes tipos de evento que pueden aparecer en los archivos del registro de sincronización:

Evento	Descripción	Detalle
sumar	El principal se agregó a Acrobat Connect Enterprise.	Un paquete XML abreviado que describe los campos actualizados mediante una serie de pares de etiquetas en el formato <code><fieldname>valor</fieldname></code> (por ejemplo, <code><first-name>José</first-name></code>). El nodo principal y los campos sin actualizar se omiten.
actualizar	El principal es un usuario externo y ciertos campos se actualizaron.	
actualizar-miembros	El principal es un grupo externo y los principales se agregaron o quitaron del grupo.	Un paquete XML abreviado describe los miembros agregados y eliminados. El nodo principal se omite: <code><add>ID list</add></code> <code><remove>ID list</remove></code> La lista id. es una serie de paquetes <code><id>Id.principal</id></code> en los que Id. principal es un id. que se indicaría en la columna Id. principal, como un inicio de sesión de usuario o un nombre de grupo. Si no hay miembros en una lista de id., el nodo principal se define como <code><add/></code> o <code><remove/></code> .
eliminar	El principal se eliminó de Acrobat Connect Pro.	

Evento	Descripción	Detalle
actualizado	El principal es un principal externo en Acrobat Connect Pro y ya está sincronizado con el directorio externo. No se realizaron cambios.	Un usuario o grupo creado en Acrobat Connect Pro se considera un principal interno. Un usuario o grupo creado por el proceso de sincronización se considera un principal externo.
hacer-externo	El principal es un principal interno en Acrobat Connect Pro y se convirtió a un principal externo.	Este evento permite que la sincronización modifique o elimine el principal y normalmente va seguido por otro evento que modifica o elimina. Este evento se registra en el registro de advertencias.
advertencia	Se produjo un evento de nivel advertencia.	Un mensaje de advertencia.
error	Ha ocurrido un error.	Mensaje de excepción de Java.

Acerca de LDAPS

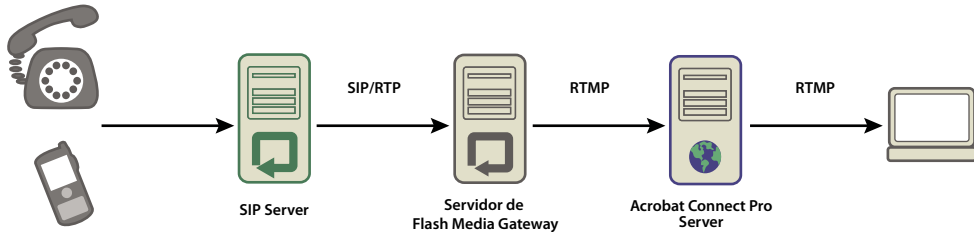
Acrobat Connect Pro admite el protocolo LDAP seguro, LDAPS. El servidor del directorio LDAP debe ofrecer conectividad SSL. Para realizar una conexión segura a un servidor del directorio LDAP, use el protocolo LDAPS en el URL de conexión de la siguiente forma: `ldaps://ejemploServidorDirectorio:numeroPuerto`.

Implementación de Voz universal

Flujo de trabajo para implementar la Voz universal

Nota: Para ver un cuadro comparativo de la Voz universal y los adaptadores de telefonía integrados, consulte “Opciones de audioconferencia de Connect Pro” en la página 13.

El sistema de Voz universal de Connect Pro utiliza un componente llamado Flash Media Gateway para recibir el audio de un servidor SIP. El audio sale en una dirección, de un servidor SIP a una sala de reuniones de Connect Pro. Instale Flash Media Gateway y configúrelo para comunicarse con un servidor SIP. El servidor SIP puede alojarse en una infraestructura de otro fabricante o de su propia empresa. (También se llama a los proveedores de SIP *proveedores de VoIP*).



El audio se transmite desde un teléfono, a través de un servidor de conferencia de audio (no representado), a través de un servidor SIP, y a través de Flash Media Gateway hacia una sala de reunión de Connect Pro.

Siga este flujo de trabajo para implementar la solución de Voz universal:

- 1 Para instalar y configurar la Voz universal, debe llevar a cabo las siguientes operaciones:
 - Connect Pro Server 7.5
 - Credenciales del proveedor SIP
- 2 Instale Flash Media Gateway.

Puede instalar Flash Media Gateway en el mismo equipo en el que tenga instalado Connect Pro Server o en otro equipo específico. Puede implementar Flash Media Gateway en un solo equipo o en un clúster de servidores. El instalador de Flash Media Gateway forma parte del instalador de Connect Pro Server. Consulte [“Ejecución del instalador”](#) en la página 15.

3 Configure Flash Media Gateway para conectarse a un servidor SIP.

Cuando se haya completado la instalación, se iniciará la consola de administración de la aplicación. (Además, puede acceder a la consola de administración de la aplicación en <http://localhost:8510/console>). Utilice la consola para configurar Flash Media Gateway para conectarse a un servidor SIP. Consulte [“Configuración de Acrobat Connect Pro con el Asistente para la consola de administración de la aplicación”](#) en la página 16.

4 Abra los puertos. Consulte [“Puertos y protocolos de Flash Media Gateway”](#) en la página 39

Si un servidor de seguridad utiliza NAT, consulte [“Configuración de Flash Media Gateway para la comunicación detrás de un cortafuegos que utiliza NAT”](#) en la página 40.

5 Para instalar Flash Media Gateway en un clúster de equipos, consulte [“Implementación de Flash Media Gateway en un clúster de servidores”](#) en la página 43.

6 Para crear una secuencia de marcación y probar la conexión de audio, consulte www.adobe.com/go/learn_cnn_uvconfig_es.

7 Si no puede oír el audio en una reunión de Connect Pro, consulte [“Resolución de problemas de Voz universal”](#) en la página 44.

Puertos y protocolos de Flash Media Gateway

Nota: Para ver un diagrama que muestre cómo fluyen los datos entre un proveedor SIP, Flash Media Gateway y Connect Pro Server, consulte [“Flujo de datos”](#) en la página 7.

Flash Media Gateway escucha las solicitudes del servidor de aplicaciones Connect Pro Central en el siguiente puerto:

Número de puerto	Dirección de enlace	Protocolo
2222	*/Cualquier adaptador	HTTP

Flash Media Gateway inicia una conexión con Flash Media Server como un cliente RTMP habitual. Flash Media Server escucha Flash Media Gateway en el siguiente puerto:

Número de puerto	Dirección de enlace	Protocolo
8506	*/Cualquier adaptador	RTMP

Flash Media Gateway se comunica con el proveedor de conferencias de audio mediante los protocolos SIP y RTP de los siguientes puertos:

Dirección	Norma
Flash Media Gateway a Internet	SRC-IP=<Server-IP>, SRC-PORT=5060, DST-IP=ANY, DST-PORT=5060
Internet a Flash Media Gateway	SRC-IP=ANY, SRC-PORT=5060, DST-IP=<Server-IP>, DST-PORT=5060
Flash Media Gateway a Internet	SRC-IP=<Server-IP>, SRC-PORT=5000_TO_6000, DST-IP=ANY, DST-PORT=ANY_HIGH_END
Internet a Flash Media Gateway	SRC-IP=ANY, SRC-PORT=ANY_HIGH_END, DST-IP=<Server-IP>, DST-PORT=5000_TO_6000

Nota: ANY_HIGH_END significa cualquier puerto por encima de 1024. El intervalo de puertos predeterminado es 5000-6000. Puede modificar estos valores en la consola de administración de la aplicación.

Configuración de Flash Media Gateway para la comunicación detrás de un cortafuegos que utiliza NAT

Nota: Puede que no sea necesario completar esta tarea si su cortafuegos es compatible o está preparado para funcionar con SIP. Además, en algunos casos la ALG (puerta de enlace de capa de aplicación) para SIP en un cortafuegos puede causar problemas. Si no consigue una comunicación exitosa a través de ALG, deshabilite la ALG para SIP en el cortafuegos y utilice la técnica descrita en esta sección.

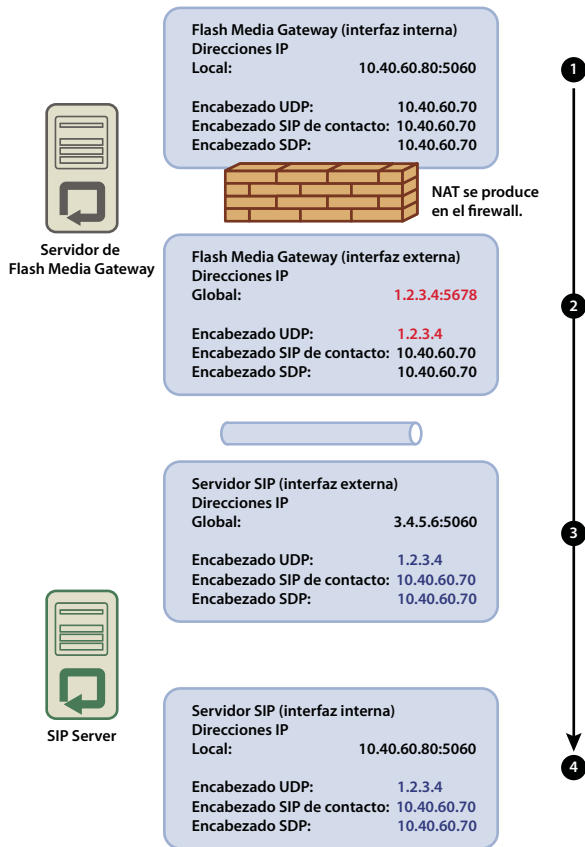
La traducción de direcciones de red (NAT) es un proceso que permite que las redes utilicen menos direcciones IP externas, así como ocultar las direcciones IP internas. NAT cambia las direcciones IP y el número de puerto de los paquetes que fluyen fuera de una red. Las direcciones IP internas se han cambiado a direcciones IP externas. Asimismo, NAT intenta remitir las respuestas enviadas a la dirección IP externa a las direcciones IP internas correctas.

Cuando Flash Media Gateway esté al otro lado del servidor de seguridad que utiliza NAT, es posible que no pueda recibir paquetes del servidor SIP. NAT cambia la dirección IP local y la dirección IP con encabezado UDP (origen del paquete) de forma que coincidan con la dirección IP externa.

La dirección IP del encabezado UDP es la misma que la dirección IP externa de Flash Media Gateway. Por tanto, si el servidor SIP utiliza la dirección IP con encabezado UDP para enviar una respuesta, la respuesta buscará Flash Media Gateway.

La dirección IP del encabezado de contacto es la misma que la dirección IP local de Flash Media Gateway. Por tanto, si el servidor SIP utiliza la dirección IP con encabezado de contacto SIP para enviar una respuesta, la respuesta no podrá buscar Flash Media Gateway. La dirección IP local se oculta al otro lado del servidor de seguridad y no está visible para el servidor SIP.

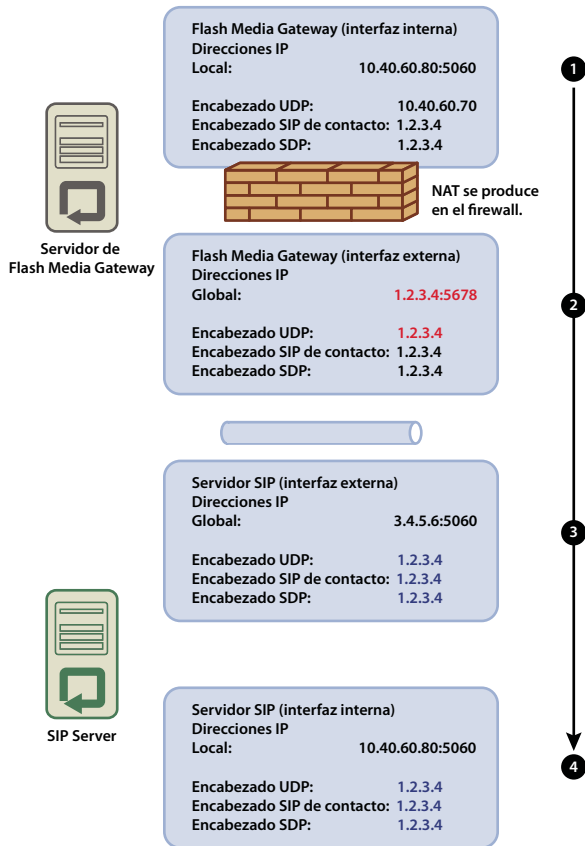
La siguiente imagen muestra cómo NAT cambia las direcciones IP del servidor de seguridad:



NAT cambia la dirección IP

- 1 Flash Media Gateway (interfaz interna). El encabezado UDP (dirección IP del origen del paquete) y la dirección IP con encabezado de contacto SIP coinciden con las direcciones IP locales.
- 2 Flash Media Gateway (interfaz externa). NAT cambia la dirección IP con encabezado UDP a la dirección IP general.
- 3 Servidor SIP (interfaz externa). El paquete alcanza la interfaz global del servidor SIP. Para alcanzar la interfaz interna, avance directamente al puerto. Si no se envía el puerto, se pierde el paquete y se rompe la comunicación.
- 4 Servidor SIP (interfaz interna). El paquete se procesa cuando alcanza esta interfaz. Si el servidor SIP utiliza la dirección IP con encabezado UDP para enviar la respuesta, ésta alcanza Flash Media Gateway correctamente. Si el servidor SIP utiliza la dirección IP con encabezado de contacto, la respuesta no podrá alcanzar Flash Media Gateway.

La siguiente imagen muestra una configuración correcta en la que la dirección IP con encabezado de contacto SIP coincide con la dirección IP externa de Flash Media Gateway. Este cambio permite que los paquetes se asignen de nuevo a Flash Media Gateway desde el servidor SIP.



Una configuración que permite una comunicación satisfactoria

Para garantizar que Flash Media Gateway pueda recibir los paquetes satisfactoriamente desde un servidor SIP, lleve a cabo las siguientes operaciones:

- 1 En Flash Media Gateway, abra el archivo `RootInstallationFolder/conf/sip.xml` en un editor de texto. (La carpeta de instalación raíz predeterminada es `C:\Program Files\Adobe\Flash Media Gateway`).
 - a Cree una etiqueta `<globalAddress>` bajo la etiqueta `<Profile>`. Introduzca la dirección IP externa de Flash Media Gateway como se indica a continuación:

```

...
<Profiles>
  <Profile>
    <profileID> sipGateway </profileID>
    <userName>141583220 00 </userName>
    <password></password>
    <displayName> sipGateway </displayName>
    <registrarAddress>8.15.247.100:5060</registrarAddress>
    <doRegister>0</doRegister>
    <defaultHost>8.15.247.100:5060</defaultHost>
    <hostPort> 0 </hostPort>
    <context> sipGatewayContext </context>
    <globalAddress>8.15.247.49</globalAddress>
    <supportedCodecs><codecID> G711u </codecID><codecID> speex </codecID>
  </supportedCodecs>
</Profile>
</Profiles>
...

```

En un clúster, cada servidor Flash Media Gateway debe tener una única dirección IP externa.

Importante: Si la dirección IP externa es dinámica, debe volver a configurar Flash Media Gateway cada vez que la dirección IP externa cambie.

- b** Reinicie el servicio Flash Media Gateway. Consulte [“Inicio y parada de Flash Media Gateway”](#) en la página 89
- 2** En el cortafuegos entre el servidor Flash Media Gateway y el servidor SIP reenvíe directamente el puerto SIP (5060 de forma predeterminada) y todos los puertos de voz RTP (5000-6000 de forma predeterminada) al servidor Flash Media Gateway. Los puertos abiertos en el cortafuegos deben ser los mismos que los puertos abiertos en el servidor Flash Media Gateway.

Nota: Los servidores se pueden comunicar sin reenvío de puertos. Sin embargo, sin reenvío de puertos las llamadas se pueden desconectar de forma inesperada, especialmente después de una larga duración.

Implementación de Flash Media Gateway en un clúster de servidores

Para implementar un clúster de servidores, instale Flash Media Gateway en sus propios equipos e instale Connect Pro Server en sus propios equipos. No instale Connect Pro Server y Flash Media Gateway en los mismos equipos.

Cuando implemente Flash Media Gateway en un clúster de servidores, Connect Pro Server administrará el equilibrio de carga y la conmutación por error. Connect Pro Edge Server no requiere ninguna configuración adicional.

- 1** Ejecute el instalador en todos los servidores del clúster y elija instalar Flash Media Gateway. Consulte [“Ejecución del instalador”](#) en la página 15.

Nota: Para obtener información sobre la implementación de Connect Pro Server en un clúster, consulte [“Implementación de un clúster de servidores Acrobat Connect Pro”](#) en la página 24.

- 2** En un servidor Connect Pro, abra la consola de administración de la aplicación en <http://localhost:8510/console>.
- 3** Seleccione la configuración de Flash Media Gateway > Configuración del host FMG y haga clic en Añadir para añadir y configurar servidores adicionales de Flash Media Gateway. Consulte [“Configuración de Acrobat Connect Pro con el Asistente para la consola de administración de la aplicación”](#) en la página 16.

Nota: Utilice la consola de administración de la aplicación en un servidor para introducir los parámetros de configuración de todos los servidores del clúster. La consola de administración de la aplicación inserta los ajustes de configuración en todos los servidores del clúster.

Opciones de configuración avanzadas de Flash Media Gateway

Para obtener información acerca de las opciones avanzadas de configuración, consulte [documentación de Flash Media Gateway](#).

Resolución de problemas de Voz universal

Si no puede escuchar el audio de una conferencia de audio de Voz Universal en una sala de reunión, realice lo siguiente:

- 1 Asegúrese de que el volumen de su equipo está alto. Si está usando auriculares, asegúrese de que están conectados a la clavija de salida.
- 2 Compruebe la secuencia de marcado. Consulte [Prueba de la secuencia de marcado](#).
- 3 Verifique que Flash Media Gateway esté configurado correctamente.
 - a Abra la consola de administración de la aplicación (<http://localhost:8510/console>) en Connect Pro Server y haga clic en Configuración de Flash Media Gateway > Configuración del host FMG. El estado de cada Flash Media Gateway debe ser "Activo".
 - b Si no está activo, abra el archivo `RootInstallationFolder/custom.ini`. Asegúrese de ver las siguientes entradas:

```
FMG_ADMIN_USER=sa
FMG_ADMIN_PASSWORD=breeze
```

Si no ve las entradas, introdúzcalas y reinicie Connect Pro Central Application Server.
- 4 Póngase en contacto con el servicio de asistencia técnica de Adobe en www.adobe.com/go/connect_licensed_programs_es.

Uso de adaptadores de telefonía integrados

Instalación de adaptadores de telefonía integrados

Los adaptadores de telefonía integrados cuentan con extensiones de Java que permiten a Connect Pro conectar con un puente de audio. Puede instalar cualquier número de adaptadores de telefonía integrados. La guía de instalación está disponible en [Centro de ayuda y soporte técnico de Connect Pro](#). Los adaptadores de telefonía pueden obtenerse en adobe.com.

Configuración de la Voz universal para los adaptadores de telefonía integrados

Puede configurar la Voz universal para cualquiera de los adaptadores de telefonía integrados instalados en Connect Pro Server. Cuando un adaptador de telefonía integrado se configura para la opción de Voz universal, puede difundir la conferencia de audio sólo para asistentes VoIP en una sala de reuniones.

- 1 Abra el archivo `RootInstallationFolder\appserv\conf\telephony-settings.xml` en un editor de texto.
- 2 En el archivo XML, defina la secuencia de marcación del proveedor de conferencias de audio. El siguiente ejemplo utiliza la secuencia de marcado para el adaptador Premiere:

Nota: Usted proporciona los valores para los parámetros entre corchetes ([]). El adaptador proporciona los valores para los parámetros entre llaves ({}).

```
<telephony-adaptor id="premiere-adaptor" class-name="com.macromedia.breeze_
xt.premiere.gateway.PTekGateway" enabled="true" name="{premiere-adaptor}" disable-
profiles-on-edit="false" disable-profiles-on-disable="false" default-recording-
source="adaptor">
  <setting id="PREMIERE_HOST">CSAXIS.PREMCONF .C OM </ se tt in g>
  <setting id="PREMIERE_PORT">443</setting>
  <setting id="PREMIERE_WEB_ID">[123456]</setting>
  <setting id="PREMIERE_PASSWORD">[aVerySecurePassword]</setting>
  <setting id="PREMIERE_MAX_DOWNLOAD_TRIES">120</setting>
  <setting id="PREMIERE_DOWNLOAD_LOGIN">[login]</setting>
  <setting id="PREMIERE_DOWNLOAD_PASSWORD">[aVerySecurePassword]</setting>
  <setting id="PREMIERE_REPORT_INTERVAL">60</setting>
  <setting id="PREMIERE_DOWNLOAD_URL">https://ww7.premconf.com/audio/</setting>
  <dial-in-sequence>
    <conf-num>{x-tel-premiere-conference-number}</conf-num>
    <delay>6000</delay>
    <dtmf>{x-tel-premiere-participant-code}</dtmf>
    <dtmf>#</dtmf>
    <delay>2000</delay>
    <dtmf>*#</dtmf>
    <delay>5000</delay>
  </dial-in-sequence>
</telephony-adaptor>
```

El siguiente ejemplo utiliza la secuencia de marcado para el adaptador InterCall:

```
<telephony-adaptor id="intercall-adaptor" class-
name="com.macromedia.breeze_ext.telephony.Intercall.IntercallTelephonyAdaptor"
enabled="true" name="{intercall-adaptor}" disable-profiles-on-edit="false" disable-
profiles-on-disable="false" default-recording-source="audio-bridge">
  <setting
id="INTERCALL_CCAPI_HOST">https://iccapr.audiocontrols.net:8443/axis2/services/CCAPI</sett
ing>
  <setting
id="INTERCALL_CCAPI_AUTH_HOST">https://iccapr.audiocontrols.net:8443/axis2/services/Author
ization</setting>
  <setting id="INTERCALL_CLIENT_CALLBACK_URL">https://[external-
hostname]:8443/services/CCAPICallbackSOAP</setting>
  <setting id="INTERCALL_APP_TOKEN">[appTokenProvidedByIntercall]</setting>
  <setting id="INTERCALL_BREEZE_INSTALL">C:\breeze</setting>
  <dial-in-sequence><conf-num>{x-tel-intercall-conference-number}</conf-num>
<delay>6000</delay><dtmf>{x-tel-intercall-participant-code}</dtmf><dtmf>#</dtmf>
<delay>4000</delay><dtmf>#</dtmf><delay>8000</delay><dtmf>#</dtmf> </dial-in-
sequence></telephony-adaptor>
```

Elemento XML	Descripción
conf-num	El número de teléfono para la audioconferencia. Este elemento debe ser el primero en la secuencia de marcado. Sólo puede tener un elemento <conf-num>. El adaptador proporciona el valor entre llaves {}.
demora	Un retraso en la secuencia de marcación, en milisegundos.
dtmf	Un tono de DTMF (multi-frecuencia de tono dual). Un valor DTMF puede ser cualquier número o letra de un teclado telefónico, incluyendo los símbolos * y #.

- 3 Valide y guarde el archivo XML.
- 4 Reinicie Connect Pro Central Application Server.

Para obtener más información sobre la configuración de adaptadores de telefonía, consulte *Uso de adaptadores de telefonía* en el [Centro de ayuda y soporte técnico de Connect Pro](#).

Ocultar el usuario Flash Media Gateway en la lista Asistentes

Nota: Esta sección hace referencia sólo a los adaptadores de telefonía integrados que se han configurado para Voz Universal.

Cuando se conecte una sala de reuniones a Flash Media Gateway, la conexión aparece como un usuario en la lista Asistentes. Para ocultar el usuario Flash Media Gateway en la lista Asistentes, configure el número de conferencia de audio en el archivo custom.ini. Utilice el mismo número para todos los equipos de un clúster. Puede obtener el número de conferencia de audio de su proveedor SIP. O bien, si el administrador de cuenta ha configurado un proveedor de audio en Connect Pro Central, podrá buscar el número en la sala de reuniones.

1 Abra el archivo `\breeze\custom.ini` en un editor de texto.

2 Añada el siguiente parámetro:

```
UV_NUMBER={audio_conference_telephone_number}
```

```
// Example:
```

```
UV_NUMBER=415551212
```

3 Guarde y cierre el archivo custom.ini.

4 Lleve a cabo la siguiente operación para reiniciar el servidor:

- a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server > Detener Connect Pro Central Application Server.
- b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server > Iniciar Connect Pro Central Application Server.

Configuración de almacenamiento compartido

Acerca del almacenamiento compartido

Puede utilizar la consola de gestión de la aplicación para configurar Acrobat Connect Pro de forma que utilice dispositivos NAS y SAN para gestionar el almacenamiento de contenido. Contenido es cualquier archivo publicado en Acrobat Connect Pro, como cursos, archivos SWF, PPT o PDF y grabaciones archivadas.

A continuación verá configuraciones posibles de almacenamiento compartido:

- El contenido se copia en el dispositivo primario de almacenamiento externo y se traslada a la carpeta de contenido de cada servidor de Acrobat Connect Pro tal como sea necesario. El contenido antiguo se elimina de la carpeta de contenido de cada servidor para dejar espacio para el nuevo contenido tal como sea necesario. Esta configuración libera recursos en el servidor de la aplicación, lo cual es particularmente útil en un clúster de gran tamaño. Introduzca un valor en el cuadro Almacenamiento compartido y en el cuadro Tamaño de caché de contenido.
- El contenido se copia en todos los servidores y el dispositivo primario de almacenamiento externo. Se recomienda esta configuración para clústeres pequeños a menos que tenga una gran cantidad de contenido al que se accede de forma aleatoria. Introduzca un valor en el cuadro Almacenamiento compartido y deje el cuadro Tamaño de caché de contenido en blanco.

Nota: Si dispone de un clúster de Acrobat Connect Pro y no configura los dispositivos de almacenamiento compartido, el clúster funciona en modo de reflejo completo (el contenido publicado en Acrobat Connect Pro se copia en todos los servidores) y el contenido nunca se elimina de forma automática de ninguno de los servidores.

Configuración de almacenamiento compartido

Si está configurando almacenamiento compartido para un servidor Acrobat Connect Pro, siga las instrucciones de la primera tarea. Si está configurando almacenamiento compartido para un clúster, siga las instrucciones de la primera tarea para un equipo en el clúster y a continuación siga las instrucciones de la segunda tarea para el resto de equipos del clúster.

Más temas de ayuda

“Dispositivos de almacenamiento de contenido admitidos” en la página 4

“Implementación de un clúster de servidores Acrobat Connect Pro” en la página 24

Configuración de almacenamiento compartido

Acrobat Connect Pro debería configurarse sin almacenamiento compartido y ejecutarse en un servidor antes de continuar.


1 Configure un volumen compartido en un dispositivo de almacenamiento externo.

Si un volumen compartido tiene un nombre de usuario y una contraseña, todos los volúmenes compartidos deben utilizar el mismo nombre de usuario y contraseña.

2 (Opcional) Si está actualizando un servidor Acrobat Connect Pro existente para utilizar volúmenes de almacenamiento compartido, debe copiar el contenido de uno de los servidores existentes en el volumen compartido.

a Detenga el servidor (Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server y Detener Connect Pro Meeting Server).

b Copie la carpeta `[root_install_dir]\content\7` en el volumen compartido creado en el paso 1.

 *Ciertos equipos en un clúster pueden tener contenido adicional. Acrobat Connect Pro no puede utilizar estos archivos pero si desea copiarlos en el volumen compartido para archivarlos, puede escribir y ejecutar una secuencia de comandos que compare el contenido de cada equipo con el contenido del volumen compartido.*

c Inicie Acrobat Connect Pro (Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Meeting Server e Iniciar Connect Pro Central Application Server).

3 En Acrobat Connect Pro, seleccione Inicio > Panel de control > Herramientas administrativas > Servicios para abrir la ventana Servicios, seleccione Adobe Connect Enterprise Service y haga lo siguiente:

a Haga clic con el botón secundario del mouse y seleccione Propiedades.

b Seleccione la ficha Iniciar sesión.

c Seleccione Esta cuenta y, si el volumen compartido tiene un nombre de usuario y una contraseña, introdúzcalos y haga clic en Aplicar.

4 Reinicie Acrobat Connect Pro (sólo el servidor de aplicaciones).

a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.

b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

- 5 Abra la consola de gestión de la aplicación (Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Configuración de Connect Pro Server 7).
- 6 En la ficha Ajustes de la aplicación, seleccione la ficha Ajustes del servidor, desplácese hasta la sección Ajustes de almacenamiento compartido e introduzca una ruta de carpeta en el cuadro Almacenamiento compartido (por ejemplo, \\almacenamiento).

Si el dispositivo de almacenamiento primario se llena, puede agregar otro dispositivo a la posición primaria. Separe las rutas con punto y coma (;): \\nuevo-almacenamiento;\\almacenamiento.

Nota: Sólo se escribe (se copia en la carpeta de almacenamiento) en la primera carpeta. Se lee (se copia de la carpeta de almacenamiento) en secuencia, desde la primera carpeta, hasta que se encuentra el archivo.

- 7 (Opcional) Para configurar la carpeta de contenido en Acrobat Connect Pro para que funcione como caché (los elementos se eliminan de forma automática cuando se necesita espacio y se restauran bajo demanda), introduzca un valor en el cuadro Tamaño de caché de contenido.

El tamaño de caché de contenido es un porcentaje del espacio de disco que se utiliza como caché. Adobe recomienda que establezca el valor entre 15 y 50 porque la caché puede superar el tamaño establecido. La caché sólo se limpia cuando el contenido visualizado ha caducado (24 horas después de visualizarse).

- 8 Haga clic en Guardar y cierre la aplicación de consola de administración de la aplicación.
- 9 Reinicie Acrobat Connect Pro (sólo el servidor de aplicaciones).
 - a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
 - b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

Configuración de almacenamiento compartido para servidores adicionales en un clúster

- 1 Instale Acrobat Connect Pro pero no lo inicie. Si Acrobat Connect Pro está instalado y activo, deténgalo.
- 2 En Acrobat Connect Pro, seleccione Inicio > Panel de control > Herramientas administrativas > Servicios para abrir la ventana Servicios, seleccione Adobe Connect Enterprise Service y haga lo siguiente:
 - a Haga clic con el botón secundario del mouse y seleccione Propiedades.
 - b Seleccione la ficha Iniciar sesión.
 - c Seleccione Esta cuenta y, si el volumen compartido tiene un nombre de usuario y una contraseña, introdúzcalos y haga clic en Aplicar.
- 3 Inicie Acrobat Connect Pro.
 - a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Adobe Connect Meeting Server.
 - b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.
- 4 (Opcional) Si está instalando Acrobat Connect Pro por primera vez, siga los pasos que se enumeran en [“Implementación de un clúster de servidores Acrobat Connect Pro”](#) en la página 24.
- 5 Haga clic en Guardar y cierre la consola de gestión de la aplicación.

Configuración de los ajustes de notificación de la cuenta

Añadir vínculos Asistencia técnica y Estado al menú Ayuda.

Los administradores de cuentas pueden añadir un vínculo a la página Estado y un vínculo a la página Asistencia técnica en el menú Ayuda de las salas de reuniones. Estos vínculos son para acceder a las páginas HTML que se diseñen. La página Estado podría proporcionar información sobre el estado actual del sistema Acrobat Connect Pro. La página Soporte técnico podría proporcionar información sobre cómo obtener asistencia técnica con Acrobat Connect Pro. Si no define estos vínculos, no estarán disponibles en el menú Ayuda.

- 1 Abra el archivo `RootInstallationFolder\custom.ini` en un editor de texto.
- 2 Para editar el vínculo a la página Estado, configure `STATUS_PAGE = "http://connect.mycompany.com/status.html"`.
- 3 Para editar el vínculo a la página Asistencia técnica, configure `SUPPORT_PAGE="http://connect.mycompany.com/support.html"`.

Las direcciones URL pueden ser absolutas o relativas al dominio del servidor de reuniones. Inicie la dirección URL absoluta con "http://" o "https://". Inicie la dirección URL relativa con "/".

- 4 Para reiniciar Acrobat Connect Pro, haga lo siguiente:
 - a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
 - b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

Definición de cuándo se envían los informes mensuales

Acrobat Connect Pro envía un correo electrónico cada mes con información de la capacidad de su cuenta. De forma predeterminada, los informes mensuales de capacidad de la cuenta se envían a las 3:00 a.m. GMT. Si quiere que Acrobat Connect Pro envíe el correo electrónico en otro momento, puede agregar parámetros al archivo `custom.ini` y definir los valores deseados.

Para obtener más información sobre la configuración de las notificaciones de cuenta en Connect Pro Central, consulte el capítulo "Administración de Acrobat Connect Pro" en *Utilización de Adobe Acrobat Connect Pro 7.5*, disponible en línea en www.adobe.com/go/connect_documentation_es.

- 1 Abra el archivo `CarpetaInstalaciónRaíz\custom.ini` y agregue los parámetros siguientes en el archivo con los valores deseados:

THRESHOLD_MAIL_TIME_OF_DAY_HOURS La hora GMT en que se enviarán los informes mensuales de notificación de capacidad. Este valor debe ser un número entero de 0 a 23. Este parámetro sólo se puede configurar en el archivo `custom.ini`, no en Connect Pro Central.

THRESHOLD_MAIL_TIME_OF_DAY_MINUTES El minuto en que se enviarán los informes mensuales de notificación de capacidad. Este valor debe ser un número entero de 0 a 59. Este parámetro sólo se puede configurar en el archivo `custom.ini`, no en Connect Pro Central.

Nota: Si uno de los parámetros anteriores no se especifica o es incorrecto, el correo electrónico se enviará a las 3:00 a.m. (GMT).

Estos son valores de muestra agregados al archivo `custom.ini`:

```
THRESHOLD_MAIL_TIME_OF_DAY = 5  
THRESHOLD_MAIL_TIME_OF_MINUTES = 30
```

- 2 Para reiniciar Acrobat Connect Pro, haga lo siguiente:
 - a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
 - b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

Definición de los umbrales de capacidad

Los administradores de cuenta de Acrobat Connect Pro pueden definir umbrales de capacidad en Connect Pro Central. Cuando la cuenta supera estos umbrales, se envía una notificación. Puede agregar parámetros en el archivo `custom.ini` que definen los umbrales predeterminados de capacidad en Connect Pro Central.

Para obtener más información sobre la configuración de las notificaciones de cuenta en Connect Pro Central, consulte el capítulo “Administración de Acrobat Connect Pro” en *Utilización de Adobe Acrobat Connect Pro 7.5* disponible en línea en www.adobe.com/go/connect_documentation_es.

- 1 Abra el archivo `CarpetaInstalaciónRaíz\custom.ini` y agregue cualquiera de los parámetros siguientes en el archivo con los valores deseados:

THRESHOLD_NUM_OF_MEMBERS El porcentaje de umbral predeterminado para la cuota de anfitriones de reunión y autores. Este valor debe ser un número entero de 10 a 100 divisible por 10. Si el valor no se especifica o es incorrecto, el valor será 80.

THRESHOLD_CONC_USERS_PER_MEETING El porcentaje de umbral predeterminado para la cuota Usuarios simultáneos por reunión. Este valor debe ser un número entero de 10 a 100 divisible por 10. Si el valor no se especifica o es incorrecto, el valor será 80.

THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT El porcentaje de umbral predeterminado para la cuota Asistentes a una reunión en todas las cuentas. Este valor debe ser un número entero de 10 a 100 divisible por 10. Si el valor no se especifica o es incorrecto, el valor será 80.

THRESHOLD_CONC_TRAINING_USERS El porcentaje de umbral predeterminado para la cuota Alumnos simultáneos. Este valor debe ser un número entero de 10 a 100 divisible por 10. Si el valor no se especifica o es incorrecto, el valor será 80.

Estos son valores de muestra agregados al archivo `custom.ini`:

```
THRESHOLD_NUM_OF_MEMBERS = 90
THRESHOLD_CONC_USERS_PER_MEETING = 90
THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT = 90
THRESHOLD_CONC_TRAINING_USERS = 75
```

- 2 Para reiniciar Acrobat Connect Pro, haga lo siguiente:
 - a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
 - b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

Configuración de PDF para la conversión SWF

Acerca de la conversión en PDF

Puede utilizar la opción Pod para compartir en una reunión de Connect Pro para compartir documentos en PDF. Los anfitriones y los presentadores pueden sincronizar la navegación para todos los asistentes y utilizar una pizarra electrónica como apoyo. Puede cargar documentos PDF en la opción Pod para compartir de su escritorio o desde la biblioteca de contenidos de Connect Pro. La opción de compartir documentos mediante Pod para compartir ofrece las siguientes ventajas respecto a la compartición en pantalla.

- Los anfitriones y presentadores pueden cargar previamente y organizar documentos en una sala de reuniones.
- Experiencia de visualización de mayor calidad para todos los asistentes.
- Menores requisitos de ancho de banda para los participantes y presentadores.
- Es más fácil que varios presentadores trabajen juntos.
- Es más fácil colaborar por medio de una pizarra.

Si los documentos PDF se comparten mediante la opción Compartir pod, Connect Pro los convierte en formato Flash. Connect Pro Server ofrece parámetros de configuración para controlar la conversión a PDF.

Configuración de PDF para conversión a SWF

- 1 Abra el archivo *RootInstallationFolder\custom.ini* en un editor de texto.
- 2 Edite cualquiera de los siguientes parámetros de configuración:

Parámetro	Valor predeterminado	Descripción
ENABLE_PDF2SWF	true	Un valor booleano especifica si está o no habilitada la conversión a PDF o SWF en el servidor. Establezca este parámetro en "false" para desactivar la conversión por motivos de rendimiento.
PDF2SWF_PAGE_TIMEOUT	5	El valor de tiempo de espera por página, en segundos.
PDF2SWF_CONVERTER_PORTS_START	4000	El valor más bajo del rango de puertos empleados para conversiones de PDF a SWF.
PDF2SWF_CONVERTER_PORTS_END	4030	El valor más alto del rango de puertos utilizado para las conversiones de PDF a SWF.
PDF2SWF_CONCURRENCY_LIMIT	3	El número máximo de conversiones de PDF a SWF simultáneas que pueden tener lugar en un servidor de aplicaciones. Si un servidor de aplicaciones recibe más solicitudes, éstas se ponen en cola.
PDF2SWF_QUEUE_LIMIT	5	El número máximo de conversiones PDF a SWF que pueden esperar simultáneamente en una misma cola. Si un servidor de aplicaciones recibe más solicitudes, el usuario verá el mensaje "Connect Pro no ha podido convertir el archivo para su visualización, inténtelo de nuevo más tarde". Un administrador ve lo siguiente en los registros: <status code="request-retry"><exception>java.lang.Exception: Conversion Load too much on server.
PDF2SWF_TIMEOUT_NUMBER_OF_PAGES	3	El número máximo de páginas que se permiten para el tiempo de espera antes de que se detenga la conversión.

- 3 Reinicie Connect Pro Central Application Server. Consulte “[Inicio y parada de Acrobat Connect Pro Server](#)” en la página 87.

Integración con Microsoft Live Communications Server 2005 y Microsoft Office Communications Server 2007

Flujo de trabajo para la configuración de la integración de presencia

Si integra Acrobat Connect Pro con un servidor de comunicaciones en tiempo real de Microsoft, los anfitriones de reunión pueden ver la presencia LCS u OCS de los participantes registrados de la reunión en la Lista de invitados e iniciar conversaciones de texto con usuarios en línea.

Para obtener más información sobre la Lista de invitados, consulte *Utilización de Adobe Acrobat Connect Pro 7.5* disponible en línea en www.adobe.com/go/connect_documentation_es.

1. Deben estar instalados Acrobat Connect Pro Server y un servidor de comunicaciones.

Instale y verifique la instalación de Acrobat Connect Pro Server y un servidor de comunicaciones. Acrobat Connect Pro Server admite la integración con Microsoft Live Communications Server 2005 y Microsoft Office Communications Server 2007. Consulte “[Instalación de Connect Pro Server y Flash Media Gateway](#)” en la página 15 y la documentación del servidor de comunicaciones.

2. Configuración del servidor de comunicaciones.

Configure el servidor de comunicaciones para intercambiar datos con Acrobat Connect Pro Server. Consulte “[Configure Live Communications Server 2005 u Office Communications Server 2007](#)” en la página 52

3. Parada de Connect Pro Presence Service.

Acrobat Connect Pro Server incluye Connect Pro Presence Service. Detenga el servicio antes de configurar Acrobat Connect Pro. Consulte “[Inicio y parada de Connect Pro Presence Service](#)” en la página 56.

4. Configuración de Connect Pro Presence Service.

Configure Acrobat Connect Pro para que pueda intercambiar datos con el servidor de comunicaciones. El servidor de presencia está instalado en `RootInstallationFolder\presserv`. Consulte “[Configuración de Connect Pro Presence Service](#)” en la página 54.

5. Inicio de Connect Pro Presence Service.

Consulte “[Inicio y parada de Connect Pro Presence Service](#)” en la página 56.

6. Habilitar la Lista de invitados y el pod de chat en Connect Pro Central.

Inicie sesión como administrador en Connect Pro Central. Seleccione Administración > Cumplimiento y control > Gestión de pods. Anule la selección de la opción para desactivar la Lista de invitados y el pod de chat.

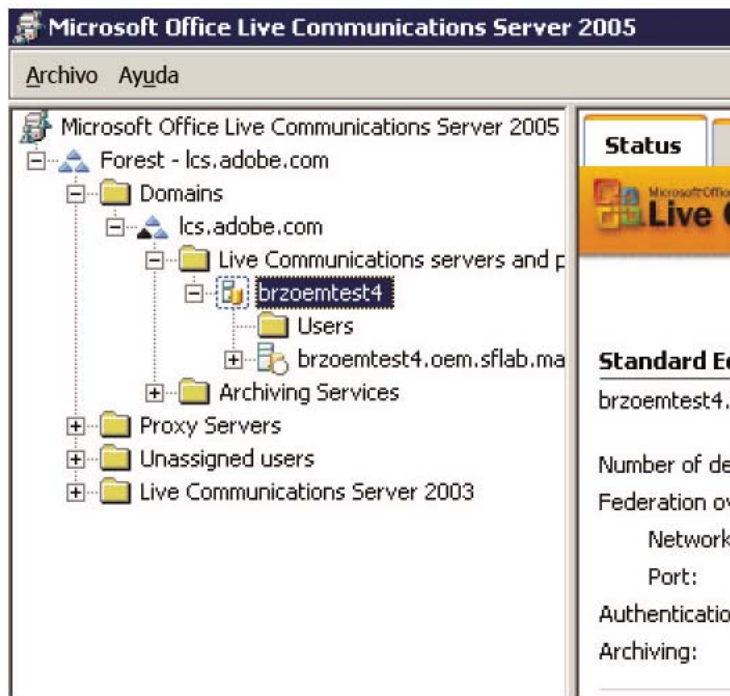
Configure Live Communications Server 2005 u Office Communications Server 2007

- 1 Seleccione Inicio > Programas > Herramientas administrativas > Live Communications Server 2005 u Office Communications Server 2007 para abrir la consola de configuración.

- 2 Haga clic con el botón secundario del mouse en Bosque, seleccione Propiedades y realice las acciones siguientes:
 - a Seleccione la ficha Federación.
 - b Seleccione la casilla de verificación para habilitar la federación y conectividad de mensajería instantánea pública.
 - c Introduzca la dirección de red de Acrobat Connect Pro.
 - d Introduzca el puerto 5072.

5072 es el número de puerto predeterminado de Connect Pro Presence Service en el archivo \presserv\conf\lcs gw.xml.

- e Haga clic en Aceptar.
- 3 En el panel izquierdo de la consola de configuración, expanda Dominios, expanda su dominio y expanda los servidores y grupos de Live Communications.
- 4 Haga clic con el botón secundario del mouse en el nombre de su grupo y seleccione propiedades.



- 5 En el cuadro de diálogo Propiedades del servidor, realice las acciones siguientes:
 - a Seleccione la Autorización de host. Agregue la dirección IP de Acrobat Connect Pro. Verifique si Sólo saliente es No, si la aceleración como servidor es Sí, y si el valor de tratar como autenticación es Sí.
 - b Si hay un equilibrador de carga instalado delante de su servidor Acrobat Connect Pro, agregue la dirección IP del equilibrador de carga.
 - c Haga clic en Aceptar.
- 6 En el panel izquierdo de la consola de configuración, expanda el FQDN de su servidor y seleccione Aplicaciones.
- 7 Realice las acciones siguientes:
 - a Haga clic en el ajuste de la aplicación de filtro URL de mensajería instantánea. En el cuadro de diálogo Propiedades, anule la selección de Habilitar. Si este ajuste está habilitado, los anfitriones de reunión no pueden enviar URL en mensajes instantáneos.

8 Cierre la consola de configuración.

Configuración de los clientes del servidor de comunicaciones

La integración de Acrobat Connect Pro con los servidores de comunicaciones de Microsoft funciona con los clientes estándar de Microsoft Office Communicator 2005 (MOC 2005). Los clientes no requieren ninguna configuración especial. No obstante, para que se pueda hacer clic en los URL de las reuniones de Connect en MOC 2005, modifique la propiedad "Allow hyperlinks in an instant message" de la plantilla Communicator Administrative. Para obtener más información, consulte <http://technet.microsoft.com/es-es/library/bb963959.aspx>.

- 1 Seleccione Inicio > Ejecutar.
- 2 Introduzca gpedit.msc en el cuadro Abrir para abrir la ventana Directiva de grupo.
- 3 Haga clic para expandir Configuración del equipo.
- 4 Haga clic para expandir Plantillas administrativas.
- 5 Haga clic con el botón secundario del mouse en los ajustes de directiva de Microsoft Office Communicator y seleccione Propiedades.

Nota: Si la plantilla de los ajustes de directiva de Microsoft Office Communicator no está en la carpeta Plantillas administrativas, agréguela. Ubique Communicator.adm en el paquete de cliente Microsoft Office Communicator 2005 y cópielo en C:\WINDOWS\inf. En la ventana Directivas de grupo, haga clic con el botón secundario del mouse en Plantillas administrativas, haga clic en Agregar/Quitar plantillas, haga clic en Agregar, busque el archivo y haga clic en Abrir.

Configuración de Connect Pro Presence Service

Complete los cuatro procedimientos siguientes para configurar Connect Pro Presence Service e intercambiar datos con un servidor de comunicaciones. Tras completar la configuración, reinicie Connect Pro Central Application Server.

Definición de la conexión de pasarela entre Connect Pro Presence Service y el servidor de comunicaciones

- 1 Abra el archivo `RootInstallationFolder\presserv\conf\lcs gw.xml` en un editor XML.
- 2 Edite el archivo con los datos siguientes; sustituya los valores en negrita con sus valores:

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
<block xmlns="accept:config:sip-lcsgw">
<service trace="off" name="lcsgw" id="internal.server">
<stack name="lcs">
<via/>
</stack>
<state type="enabled"/>
<host type="external">lcs.adobe.com</host>
<domain-validation state="false"/>
<binding name="connector-0" transport="tcp">
<port>5072</port>
<bind>10.59.72.86</bind> <!-- LCS server IP -->
<area>lcs.adobe.com</area> <!-- LCS domain -->
</binding>
</service>
</block>
</config>
```

Parámetro	Descripción
<anfitrión>	Dominio SIP de usuarios LCS u OCS
<bind>	Dirección IP del servidor (o equilibrador de carga) LCS u OCS
<area>	Dominio SIP de usuarios LCS u OCS

Configuración del archivo custom.ini

- 1 Abra *RootInstallationFolder\custom.ini* en un editor de texto.
- 2 Introduzca los parámetros y valores siguientes:

Parámetro	Valor
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Este valor distingue entre mayúsculas y minúsculas.
OPN_HOST	La dirección de red de Connect Pro Presence Service (por ejemplo, localhost).
OPN_PORT	El puerto interno que se utiliza entre Acrobat Connect Pro y Connect Pro Presence Service. El valor predeterminado (10020) debe coincidir con el valor del archivo <i>RootInstallationFolder\presserv\conf\router.xml</i> . No modifique este valor.
OPN_PASSWORD	El cupón interno que se utiliza entre Acrobat Connect Pro y Connect Pro Presence Service. El valor predeterminado (secreto) debe coincidir con el valor del archivo <i>RootInstallationFolder\presserv\conf\router.xml</i> . No modifique este valor.
OPN_DOMAIN	El nombre de dominio del servidor Acrobat Connect Pro (servidor de aplicaciones). Connect Pro Presence Service utiliza este nombre para identificar al servidor de aplicaciones. En un clúster, cada servidor de aplicaciones debe tener su propio nombre de dominio.
MEETING_PRESENCE_POLL_INTERVAL	Los clientes de host encuestan an servidor de presencia a intervalos regulares para recuperar el estado de los invitados. Este parámetro define el número de segundos entre solicitudes de encuesta. El valor predeterminado es 30. No modifique este valor.

Estos son los ajustes de muestra:

```
OPN_ADAPTOR=com.macromedia.breeze.opn.OPNGateway
OPN_HOST=localhost
OPN_PORT=10020
OPN_PASSWORD=secret
OPN_DOMAIN=breeze01.com
```

Definición de la pasarela SIP a Connect Pro Presence Service

- 1 Abra el archivo *\\presserv\conf\router.xml* en un editor XML.
- 2 Edite el archivo con los datos siguientes; sustituya los valores en negrita con sus valores:

```
<block xmlns="accept:config:xmpp-gateway">
...
<block xmlns="accept:config:sip-stack-manager">
<service trace="off">
<bind>10.133.192.75</bind> <!-- presence server machine IP -->
<state type="enabled"/></service></block>
```

En la etiqueta `<bind>`, introduzca la dirección IP del equipo con Acrobat Connect Pro. Si se devuelven varias direcciones IP, seleccione la dirección IP interna o externa que el servidor LCS u OCS remoto puede resolver para conectar con Acrobat Connect Pro.

- 3 Reinicie Connect Pro Central Application Server.

Configuración de Connect Pro Presence Service en un clúster

Si está ejecutando Connect Pro en un clúster, ejecute Connect Pro Presence Service sólo en un equipo del clúster. No obstante, configure Connect Pro Presence Service en todos los equipos del clúster para que puedan intercambiar tráfico de presencia.

- 1 Abra *instal_raíz\custom.ini* en un editor de textos.
- 2 Introduzca los parámetros y valores siguientes:

Parámetro	Valor
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Este valor distingue entre mayúsculas y minúsculas.
OPN_HOST	El FQDN del equipo que ejecuta Connect Pro Presence Service. El valor del parámetro OPN_HOST es el mismo en todos los equipos de un clúster.
OPN_PORT	El puerto interno que se utiliza entre Acrobat Connect Pro y Connect Pro Presence Service. El valor predeterminado (10020) debe coincidir con el valor del archivo <i>RootInstallationFolder\presserv\conf\router.xml</i> . No modifique este valor.
OPN_PASSWORD	El cupón interno que se utiliza entre Acrobat Connect Pro y Connect Pro Presence Service. El valor predeterminado (secreto) debe coincidir con el valor del archivo <i>RootInstallationFolder\presserv\conf\router.xml</i> . No modifique este valor.
OPN_DOMAIN	El dominio que Connect Pro Presence Service utiliza para identificar un servidor de Connect Pro en un clúster. Cada equipo del clúster debe tener un valor diferente. El parámetro OPN_DOMAIN puede tener cualquier valor (por ejemplo, presence.connect1, presence.connect2, connect3) siempre que sea único dentro del clúster.
MEETING_PRESENCE_POLL_INTERVAL	Los clientes de host encuestan a un servidor de presencia a intervalos regulares para recuperar el estado de los invitados. Este parámetro define el número de segundos entre solicitudes de encuesta. El valor predeterminado es 30. No modifique este valor.

Estos son los ajustes de muestra:

```
OPN_ADAPTOR=com.macromedia.breeze.opn.OPNGateway
OPN_HOST=localhost
OPN_PORT=10020
OPN_PASSWORD=secret
OPN_DOMAIN=presence.connect1
```

- 3 Reinicie Connect Pro Central Application Server.

Inicio y parada de Connect Pro Presence Service

Puede iniciar y detener Connect Pro Presence Service desde el menú Inicio o la ventana Servicios.

Inicio y parada de Connect Pro Presence Service desde el menú Inicio

- ❖ Realice una de las siguientes acciones:
 - Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Presence Service.
 - Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Presence Service.

Inicio y parada de Connect Pro Presence Service desde la ventana Servicios

- 1 Para abrir la ventana Servicios, seleccione Inicio > Panel de control > Herramientas administrativas > Servicios.

- 2 Seleccione Acrobat Connect Pro Presence Service y haga clic en Iniciar el servicio, Detener el servicio o Reiniciar el servicio.

Configuración de la identificación única (SSO)

Acerca de la identificación única

La identificación única es un mecanismo que autentica a los usuarios para todas las aplicaciones para las que tienen permiso de acceso en una red. La identificación única utiliza un servidor proxy para autenticar a los usuarios, por lo que no tienen que iniciar una sesión en Acrobat Connect Pro.

Acrobat Connect Pro admite los mecanismos de identificación única siguientes:

Autenticación por encabezado HTTP Configure un proxy de autenticación para que intercepte solicitudes de HTTP, analice las credenciales del usuario a partir del encabezado y pase dichas credenciales a Acrobat Connect Pro.

Autenticación mediante Microsoft NT LAN Manager (NTLM) Configure Connect Pro para que trate de autenticar automáticamente a los clientes durante la conexión mediante un controlador de dominio de Windows con el protocolo NTLMv1. Microsoft Internet Explorer en Microsoft Windows puede hacerse cargo de la autenticación NTLM sin pedir las credenciales al usuario.

Nota: Es posible que los clientes de Mozilla Firefox puedan hacerse cargo de la autenticación NTLM sin solicitarlas. Para obtener información sobre la configuración, consulte este [documento de Firefox](#).

Asimismo, puede escribir su propio filtro de autenticación. Para obtener más información, póngase en contacto con el servicio de asistencia técnica de Adobe.

Configuración de la autenticación por encabezado HTTP

Cuando se configura la autenticación por encabezado HTTP, las solicitudes de inicio de sesión de Acrobat Connect Pro se dirigen a un agente ubicado entre el cliente y Acrobat Connect Pro. El agente puede ser un proxy de autenticación o una aplicación de software que autentica al usuario, agrega otro encabezado a la solicitud de HTTP y envía la solicitud a Acrobat Connect Pro. En Acrobat Connect Pro, debe codificar sin marcas de comentario un filtro Java y configurar un parámetro en el archivo custom.ini que especifique el nombre del encabezado HTTP adicional.

Más temas de ayuda

“[Inicio y parada de Acrobat Connect Pro Server](#)” en la página 87

Configuración de la autenticación por encabezado HTTP en Acrobat Connect Pro

Para habilitar la autenticación por encabezado HTTP, configure una asignación de filtros Java y un parámetro de encabezado en el equipo en el que esté instalado Acrobat Connect Pro.

- 1 Abra el archivo `[root_install_dir]\appserv\conf\WEB-INF\web.xml` y haga lo siguiente:

- a Codifique sin marcas de comentario la asignación de filtros Java `HeaderAuthenticationFilter`

```
<filter-mapping>
  <filter-name>HeaderAuthenticationFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

- b Codifique con marcas de comentario la asignación de filtros Java `NtlmAuthenticationFilter`

```
<!--
<filter-mapping>
  <filter-name>NtlmAuthenticationFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

2 Detenga Acrobat Connect Pro:

- a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
- b Seleccione Inicio > Programas > Adobe Acrobat Connect Server 7 > Iniciar Adobe Connect Meeting Server.

3 Agregue la línea siguiente en el archivo custom.ini:

```
HTTP_AUTH_HEADER=header_field_name
```

El agente de autenticación debe agregar un encabezado a la solicitud HTTP que se envía a Acrobat Connect Pro. El nombre del encabezado debe ser *header_field_name*.

4 Guarde el archivo custom.ini y reinicie Acrobat Connect Pro:

- a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Adobe Connect Meeting Server.
- b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

Cómo escribir el código de autenticación

El código de autenticación debe autenticar al usuario, agregar un campo en el encabezado HTTP que contiene el inicio de sesión del usuario y enviar una solicitud a Acrobat Connect Pro.

- 1 Establezca un inicio de sesión del usuario de Acrobat Connect Pro para el valor del campo de encabezado *header_field_name*.
- 2 Envíe una solicitud de HTTP a Acrobat Connect Pro en la dirección URL siguiente:

```
http://connectURL/system/login
```

El filtro de Java de Acrobat Connect Pro detecta la solicitud, busca el encabezado *header_field_name* y busca un usuario con el id indicado en el encabezado. Si se encuentra al usuario, éste se autenticará y se enviará una respuesta.

- 3 Busque en el contenido HTTP de la respuesta de Acrobat Connect Pro la cadena "OK", que indica una autenticación correcta.
- 4 Busque la cookie *BREEZESESSION* en la respuesta de Acrobat Connect Pro.
- 5 Redirija al usuario a la dirección URL solicitada en Acrobat Connect Pro y pase la cookie *BREEZESESSION* como el valor del parámetro *session* tal como se indica a continuación:

```
http://connectURL?session=BREEZESESSION
```

Nota: Debe pasar la cookie *BREEZESESSION* en todas las solicitudes posteriores a Acrobat Connect Pro durante esta sesión de cliente.

Configuración de la autenticación por encabezado HTTP con Apache

El procedimiento siguiente describe un ejemplo de implementación de autenticación por encabezado HTTP que utiliza Apache como agente de autenticación.

- 1 Instale Apache como proxy inverso en un equipo diferente del que tenga instalado Acrobat Connect Pro.

2 Seleccione Inicio > Programas > Apache HTTP Server > Configure Apache Server > Edit the Apache httpd.conf Configuration file y haga lo siguiente:

a Codifique sin marcas de comentario la línea siguiente:

```
LoadModule headers_module modules/mod_headers.so
```

b Codifique sin marcas de comentario las tres líneas siguientes:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

c Agregue las líneas siguientes al final del archivo:

```
RequestHeader append custom-auth "ext-login"
ProxyRequests Off
<Proxy *>
Order deny,allow
Allow from all
</Proxy>
ProxyPass / http://hostname:[port]/
ProxyPassReverse / http://hostname:[port]/
ProxyPreserveHost On
```

3 Detenga Acrobat Connect Pro:

a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.

b Seleccione Inicio > Programas > Adobe Acrobat Connect Server 7 > Iniciar Adobe Connect Meeting Server.

4 En el equipo en el que haya instalado Acrobat Connect Pro , agregue las líneas de código siguientes al archivo custom.ini (situado de forma predeterminada en el directorio de instalación raíz, c:\breeze):

```
HTTP_AUTH_HEADER=custom-auth
```

El parámetro HTTP_AUTH_HEADER debe coincidir con el nombre configurado en el proxy. En este ejemplo, se ha configurado en la línea 1 del paso 2c. El parámetro es el encabezado de HTTP adicional.

5 Guarde el archivo custom.ini y reinicie Acrobat Connect Pro:

a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Adobe Connect Meeting Server.

b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

6 Abra el archivo [root_install_dir]\appserv\conf\WEB-INF\web.xml y haga lo siguiente:

a Codifique sin marcas de comentario la asignación de filtros Java HeaderAuthenticationFilter

```
<filter-mapping>
  <filter-name>HeaderAuthenticationFilter</filter-name>
  <url-pattern>*/</url-pattern>
</filter-mapping>
```

b Codifique con marcas de comentario la asignación de filtros Java NtlmAuthenticationFilter

```
<!--
<filter-mapping>
  <filter-name>NtlmAuthenticationFilter</filter-name>
  <url-pattern>*/</url-pattern>
</filter-mapping>
-->
```

Configuración de la autenticación NTLM

NTLMv1 es un protocolo de autenticación que se emplea en el protocolo de red SMB en la red Microsoft Windows. Puede utilizar NTLM para permitir a un usuario probar su identidad una vez en un dominio de Windows y, a partir de entonces, estará autorizado a acceder a otro recurso de red, como Connect Pro. Para establecer las credenciales de usuario, el navegador Web del usuario lleva a cabo una autenticación desafío - respuesta con el controlador de dominio a través de Connect Pro. Si este mecanismo no funciona, el usuario puede iniciar sesión directamente en Connect Pro. Sólo Internet Explorer en Windows admite el inicio de sesión único con autenticación NTLMv1.

Nota: De forma predeterminada, los controladores de dominio de Windows Server 2003 requieren una función de seguridad llamada Firmas de SMB. Las firmas SMB no se admiten en la configuración predeterminada del filtro de autenticación de NTLM. Puede configurar el filtro para que funcione con este requisito. Para obtener más información sobre ésta y otras funciones avanzadas, consulte la [documentación de autenticación JCIFS NTLM HTTP](#).

Cómo agregar parámetros de configuración

Repita esta operación para cada uno de los host de un clúster de Connect Pro:

- 1 Abra el archivo `root_install_dir\custom.ini` en un editor de texto y añada los siguientes parámetros:

```
NTLM_DOMAIN=[domain]
NTLM_SERVER=[WINS_server_IP_address]
```

El valor `[domain]` es el nombre del dominio de Windows del que los usuarios son miembros y que utilizan para autenticarse, por ejemplo, CORPNET. Es posible que necesite establecer este valor en la versión compatible anterior a Windows 2000 del nombre de dominio. Para obtener más información, consulte [Nota técnica 27e73404](#). Este valor se asigna a la propiedad del filtro `jcifs.smb.client.domain`. Si se establece este valor de forma directa en el archivo `web.xml` se anula el valor en el archivo `custom.ini`.

El valor `[WINS_server_IP_address]` es la dirección IP o una lista de direcciones IP de servidores WINS separadas por comas. Utilice la dirección IP, el nombre de host no funciona. Se consultan los servidores WINS en el orden especificado para resolver la dirección IP de un controlador de dominio para el dominio especificado en el parámetro `NTLM_DOMAIN`. (El controlador de dominio autentica a los usuarios). Además, puede especificar la propia dirección IP del controlador de dominio, por ejemplo, 10.169.10.77, 10.169.10.66. Este valor se asigna a la propiedad del filtro `jcifs.netbios.wins`. Al establecer este valor en el archivo `web.xml` se anula el valor del archivo `custom.ini`.

- 2 Guarde el archivo `custom.ini`.
- 3 Abra el archivo `root_install_dir\appserv\conf\WEB-INF\web.xml` en un editor de texto y lleve a cabo la siguiente operación:
 - a Quite la marca de comentario de la asignación `NtlmAuthenticationFilter` de forma que tenga el siguiente aspecto:

```
<filter-mapping>
  <filter-name>NtlmAuthenticationFilter</filter-name>
  <url-pattern>*/</url-pattern>
</filter-mapping>
```

- b Comente la asignación del filtro `HeaderAuthenticationFilter` de forma que tenga el siguiente aspecto:

```
<!--
<filter-mapping>
  <filter-name>HeaderAuthenticationFilter</filter-name>
  <url-pattern>*/</url-pattern>
</filter-mapping>
-->
```

- 4 Guarde el archivo `web.xml`.

5 Reinicie Connect Pro.

- a Seleccione Inicio > Todos los programas > Adobe Acrobat Connect Pro Server > Detener Adobe Acrobat Connect Pro Server.
- b Seleccione Inicio > Todos los programas > Adobe Acrobat Connect Pro Server > Inicio de Adobe Acrobat Connect Pro Server.

Reconciliación de las normativas de inicio de sesión

Connect Pro y NTLM tienen normativas de inicio de sesión diferentes para autenticar usuarios. Concilie estas directivas antes de que los usuarios puedan utilizar un inicio de sesión único.

El protocolo NTLM utiliza un identificador de inicio de sesión que puede ser un nombre de usuario (jperez), un número de id. de empleado (1234) o un nombre cifrado, según la normativa de la organización. De forma predeterminada, Connect Pro utiliza una dirección de correo electrónico (jperez@miempresa.com) como identificador de inicio de sesión. Cambie la directiva de inicio de sesión de Connect Pro, de forma que comparta un único identificador con NTML.

1 Abra Connect Pro Central.

Para abrir Connect Pro Central, abra una ventana de explorador e introduzca el FQDN del equipo en el que está instalado Connect Pro Host (por ejemplo, <http://connect.ejemplo.com>). Ha Introducido el valor del equipo de Connect Pro Host en la pantalla Ajustes del servidor de la consola de administración de la aplicación.

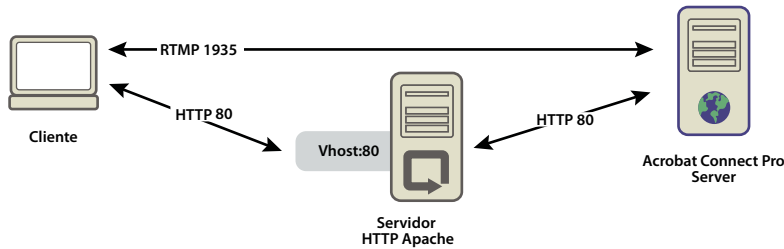
- 2 Seleccione la ficha Administración. Haga clic en Grupos y usuarios. Haga clic en Editar directivas de inicio de sesión y contraseña.
- 3 En la sección de Directiva de inicio de sesión, seleccione No en Utilizar la dirección de correo electrónico como el nombre de usuario de inicio de sesión.

Configuración de un proxy inverso frente al servidor Connect Pro Server

Uso de un proxy inverso

Puede configurar un proxy inverso frente a Connect Pro Server. El tráfico fluye por el proxy inverso antes de alcanzar Connect Pro Server. Utilice esta configuración para llevar a cabo la siguiente operación:

- Mantenga Connect Pro Server fuera de DMZ.
Coloque el proxy inverso en DMZ y Connect Pro Server al otro lado del servidor de seguridad de la organización.
- Autentique a los usuarios antes de que accedan al servidor Connect Pro.
El proxy inverso autentica a los usuarios con otro sistema y les autoriza a conectarse a Connect Pro Server.



El tráfico HTTP fluye por Apache HTTP Server hasta llegar a Connect Pro Server.

Configuración de un proxy inverso

Este ejemplo utiliza la instalación de Windows (32 bits) de Apache HTTP Server. La configuración es idéntica en cualquier sistema operativo compatible con Apache. Este ejemplo no utiliza SSL; el tráfico hacia el servidor de aplicaciones Connect Pro no se cifra.

Lleve a cabo la siguiente operación para forzar que todo el tráfico pase por el servidor Apache HTTP Server antes de que llegue a Connect Pro:

Nota: El tráfico RTMP no pasa por Apache HTTP Server en esta configuración.

1 Instale Apache HTTP Server.

De forma predeterminada, los archivos de configuración de Apache se sitúan en la carpeta c:\Program Files\Apache Software Foundation\Apache2.2\conf\.

2 Configure Apache para que escuche todo el tráfico del puerto 80.

Abra el archivo de c:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf en un editor de texto y añada lo siguiente:

```
#
# Listen: Allows you to bind Apache to specific IP addresses and
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
#
#
```

3 Cargue los módulos necesarios para el funcionamiento como un proxy inverso.

En el mismo archivo (httpd.conf), elimine la marca de comentario de las siguientes líneas:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
```

4 Vincule el archivo httpd.conf al archivo de configuración que dirige las conexiones a Connect Pro.

Añada la siguiente línea como la última línea del archivo httpd.conf:

```
Include conf/extra/httpd-connect.conf
```

- 5 Cree un archivo de texto llamado httpd-connect.conf y guárdelo en c:\Program Files\Apache Software Foundation\Apache2.2\conf\extra.
- 6 Añada las siguientes líneas al archivo httpd-connect.conf (inserte sus direcciones IP y puertos cuando se le indique):

```
#vhost for application server
<VirtualHost *:80>
ProxyRequests Off
ProxyPreserveHost On
ProxyPass / http://<IP-of-Connect-Application-Server>:80/
ProxyPassReverse / http://<IP-of-Connect-Application-Server>:80/
ServerName <FQDN of Apache host>
</VirtualHost>
```

- 7 Guarde el archivo y reinicie el servicio Apache.
- 8 En Connect Pro Server, abra la consola de administración de la aplicación en un navegador:
<http://localhost:8510/console/>
- 9 En la pantalla de configuración del servidor, lleve a cabo la siguiente operación:
 - Establezca el Connect Pro Host como el FQDN de Apache HTTP Server.
 - Establezca el nombre externo como el FQDN del equipo en el que se aloje Connect Meeting Server.
- 10 Reinicie el servicio Adobe Connect Pro (el servidor de aplicaciones) y el servicio Flash Media Server (FMS, el servidor para reuniones). Consulte [“Inicio y parada de los servidores”](#) en la página 87
RTMP se distribuye a Connect Pro y HTTP se distribuye a través de Apache.

Host del complemento Acrobat Connect

Acerca del complemento Acrobat Connect

Adobe Acrobat Connect Add-in es una versión de Flash Player que incluye funciones mejoradas para reuniones de Acrobat Connect Pro.

Cuando es necesario, Connect Acrobat Add-in se descarga de un servidor Adobe en un proceso sin interrupciones que el usuario no ve. Sin embargo, si su organización no permite que los empleados descarguen software de servidores externos, puede instalar Acrobat Connect Add-in en su propio servidor.

Se solicitará a los invitados, usuarios registrados y presentadores de la reunión que descarguen el complemento Acrobat Connect si tienen una versión anterior instalada y pasan a ser un anfitrión o presentador o reciben derechos mejorados del pod para compartir.

Los anfitriones de la reunión deben descargar el complemento Acrobat Connect si no está instalado o si hay una versión anterior instalada.

Personalización de la ubicación de descarga del complemento Connect

Puede instalar el complemento Acrobat Connect en su servidor y dirigir a los usuarios directamente a los archivos ejecutables. Puede que desee dirigir a los usuarios a una página con instrucciones de descarga que contenga vínculos a los archivos ejecutables. Puede crear su propia página de instrucciones de descarga o utilizar una proporcionada por Adobe. La página de Adobe está disponible en todos los idiomas compatibles.

Envío directo de los usuarios a los archivos ejecutables:

- 1 Ubique los archivos XML de idioma de Acrobat Connect Pro en el servidor que tenga instalado Acrobat Connect Pro. Los archivos XML están en los dos directorios siguientes: `[dir_instal_raíz]\appserv\web\common\intro\lang` y `[dir_instal_raíz]\appserv\web\common\meeting\lang`.
- 2 Introduzca la ruta a los archivos ejecutables para cada plataforma en la sección `addInLocation` de cada plataforma en cada archivo de idioma:

```
<m id="addInLocation" platform="Mac OS 10">/common/addin/AcrobatConnectAddin.z</m>
<m id="addInLocation" platform="Windows">/common/addin/setup.exe</m>
```

Nota: Se trata de las ubicaciones predeterminadas de los archivos ejecutables del complemento. Puede cambiar la ubicación en el servidor y cambiar las rutas de la sección `addInLocation` correspondientes.

Envío de los usuarios a las páginas de instrucciones de descarga de Adobe:

- 1 Ubique los archivos XML de idioma de Acrobat Connect Pro en el servidor que tenga instalado Acrobat Connect Pro. Los archivos XML están en los dos directorios siguientes: `[dir_instal_raíz]\appserv\web\common\intro\lang` y `[dir_instal_raíz]\appserv\web\common\meeting\lang`.
- 2 Introduzca la ruta a la página de instrucciones de descarga en la sección `addInLocation` de cada plataforma en cada archivo de idioma:

```
<m id="addInLocation" platform="Mac OS 10">/common/help/#lang#/support/addindownload.htm</m>
<m id="addInLocation" platform="Windows">/common/help/#lang#/support/addindownload.htm</m>
```

Nota: La ruta incluye una cadena `#lang#` que Acrobat Connect Pro convierte en el idioma de la reunión durante el tiempo de ejecución.

- 3 Los archivos `addindownload.htm` incluyen vínculos a los archivos ejecutables del complemento en sus ubicaciones predeterminadas en Acrobat Connect Pro (`/common/addin/setup.exe` y `/common/addin/AcrobatConnectAddin.z`). Si cambia la ubicación de los archivos ejecutables, actualice los vínculos en la página `addindownload.htm` para cada idioma.

Envío de los usuarios a las páginas de instrucciones de descarga creadas por usted:

- 1 Ubique los archivos XML de idioma de Acrobat Connect Pro en el servidor que tenga instalado Acrobat Connect Pro. Los archivos XML están en los dos directorios siguientes: `[dir_instal_raíz]\appserv\web\common\intro\lang` y `[dir_instal_raíz]\appserv\web\common\meeting\lang`.
- 2 En la sección `addInLocation` de cada plataforma en cada archivo de idioma, introduzca la ruta a la página de instrucciones que haya creado:

```
<m id="addInLocation" platform="Mac OS
10">common/help/#lang#/support/addin_install_instructions.html</m>
<m id="addInLocation"
platform="Windows">common/help/#lang#/support/addin_install_instructions.html</m>
```

Nota: Puede crear páginas de instrucciones independientes para cada plataforma.

- 3 Cree una página de instrucciones en cada idioma que desee admitir. Incluya vínculos a los archivos ejecutables del complemento para cada plataforma en la página de instrucciones.

Capítulo 4: Seguridad

La seguridad de Adobe Acrobat Connect Pro Server protege a su organización contra la pérdida de bienes y los actos malintencionados. Es importante asegurar la infraestructura de su organización, Acrobat Connect Pro Server y el servidor de la base de datos que utiliza Acrobat Connect Pro Server.

SSL (capa de conexión segura)

Acerca de la compatibilidad de SSL

Acrobat Connect Pro consta de dos servidores: Adobe® Flash® Media Server y el servidor de aplicaciones Acrobat Connect Pro. Flash Media Server se denomina *servidor de reuniones* porque funciona con reuniones en una conexión RTMP en tiempo real al cliente. El servidor de aplicaciones Acrobat Connect Pro gestiona la conexión HTTP entre el cliente y la lógica de la aplicación Acrobat Connect Pro.

Nota: En el menú Inicio, el servidor de reuniones se denomina “Connect Pro Meeting Server” y el servidor de aplicaciones, “Connect Pro Central Application Server”. En la ventana Servicios, el servidor de reuniones se denomina “Flash Media Server (FMS)” y el servidor de aplicaciones, “Adobe Connect Enterprise Service”.

Puede configurar una SSL para el servidor de aplicaciones, el servidor de reuniones o ambos:

Solución basada en hardware Utilizar un acelerador SSL para una configuración de SSL más sólida.

Adquiera un acelerador SSL por separado. Adobe ha comprobado que Acrobat Connect Pro funciona con los siguientes aceleradores SSL de hardware: F5 Big-IP 1000, Cisco Catalyst 6590 Switch y Radware T100.

Solución basada en software Utilización de la compatibilidad nativa para SSL en Acrobat Connect Pro.

Nota: SSL no puede utilizarse en Microsoft® Windows® 98.

Acrobat Connect Pro utiliza el método HTTP CONNECT para solicitar una conexión SSL. Los servidores proxy deben permitir que los clientes utilicen el método CONNECT. Si los clientes no pueden utilizar el método CONNECT, las conexiones RTMP utilizan HTTP/HTTPS.

Para obtener ayuda acerca de la configuración de SSL, póngase en contacto con el soporte técnico de Adobe en www.adobe.com/go/connect_licensed_programs_es.

Trabajo con certificados

Un certificado SSL comprueba la identidad del servidor para el cliente.

Para asegurar la conexión del servidor de reuniones (RTMP) y del servidor de aplicaciones (HTTP), debe disponer de dos certificados SSL, uno para cada conexión. Para configurar SSL para un clúster de equipos con Acrobat Connect Pro, debe tener un certificado SSL para cada servidor de reuniones. Todos los servidores de aplicaciones de un clúster pueden compartir el mismo certificado SSL.

Por ejemplo, para asegurar las conexiones del servidor de reuniones y del servidor de aplicaciones de un servidor individual, necesitaría en total dos certificados SSL. Para asegurar las conexiones del servidor de reuniones y del servidor de aplicaciones de un grupo de tres servidores, necesitaría un total de cuatro certificados SSL: uno para los servidores de aplicaciones y tres para los servidores de reuniones.

Obtener certificados

- ❖ Póngase en contacto con la entidad emisora de certificados, esto es, un tercero de confianza que verifica la identidad del solicitante. Los certificados con verificación propia no funcionan con Acrobat Connect Pro.

La entidad emisora de certificados le pedirá que genere un archivo de Solicitud de firma de certificado (CSR) de SSL. Envíe el CSR a la entidad emisora de certificados para que lo convierta en un certificado SSL. Contiene información acerca de su organización y el nombre de dominio completo (FQDN, del inglés "fully qualified domain name") asociado con el certificado SSL. Póngase en contacto con la entidad emisora de certificados para obtener instrucciones sobre la creación de una CSR.

Importante: Guarde las contraseñas de los certificados SSL en un lugar seguro y de fácil acceso.

Instalar certificados

- ❖ Instale los certificados SSL y los archivos de clave privada en formato PEM en la carpeta raíz (c:\breeze, de forma predeterminada) de Acrobat Connect Pro.

Si recibe un archivo CTR de una entidad emisora de certificados, puede cambiar el nombre del archivo para que su extensión sea .pem.

Nota: Debe tener dos archivos para cada conexión segura: un archivo para el certificado público y un archivo para la clave privada. El servidor envía el certificado público al cliente. La clave privada permanece en el servidor.

Configurar una SSL basada en software

Al configurar una SSL basada en software, debe asegurar el servidor de aplicaciones (HTTP), el servidor de reuniones (RTMP) o ambos. Independientemente de la configuración que elija, debe configurar primero el servidor DNS.

Configuración del servidor DNS

- ❖ Cree entradas DNS que definan un FQDN para cada conexión segura.

El FQDN para el servidor de aplicaciones es la dirección URL que los usuarios finales utilizan para conectarse a Acrobat Connect Pro. Introduzca este FQDN para el valor de Host de Connect Pro en la página Ajustes de servidor de la consola de gestión de la aplicación. Por ejemplo, un valor correcto es `connect.suempresa.com`

Los usuarios finales no ven el FQDN del servidor de reuniones. No obstante, debe tener un FQDN para el servidor de reuniones si desea llevar a cabo reuniones en una conexión segura. Introduzca este FQDN en el cuadro Nombre externo de la página Ajustes de servidor de la consola de gestión de la aplicación. Por ejemplo, un valor correcto es `fms.suempresa.com`.

Nota: En un clúster de servidores, todos los servidores de aplicaciones pueden compartir un certificado SSL, pero cada servidor de reuniones debe tener su propio certificado SSL. En un servidor único, para asegurar las conexiones HTTP (servidor de aplicaciones) y RTMP (servidor de reuniones), debe tener un total de dos certificados FQDN y dos certificados SSL (uno para cada protocolo).

Asegurar el servidor de reuniones y el servidor de aplicaciones

- 1 Abra el archivo `Adaptor.xml` que encontrará en `[root_install_dir]\comserv\win32\conf_defaultRoot_` y guarde una copia de seguridad en otra ubicación.
- 2 Introduzca el siguiente código en el archivo original `Adaptor.xml` entre las etiquetas `<Adaptor></Adaptor>` (sustituya el código en cursiva por sus propios valores):

```

<SSL>
  <Edge name="meetingserver">
    <SSLServerCtx>
<SSLCertificateFile>[root_install_dir]\sslMeetingPublicCert.pem</SSLCertificateFile>
    <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslMeetingPrivateKey.pem</SSLCertificateKeyFile>
      <SSLPassPhrase>my passphrase</SSLPassPhrase>
      <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
      <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
  </Edge>
  <Edge name="applicationserver">
    <SSLServerCtx>

<SSLCertificateFile>[root_install_dir]\sslAppServerPublicCert.pem</SSLCertificateFile>
    <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslAppServerPrivateKey.pem</SSLCertificateKeyFile>
      <SSLPassPhrase>my passphrase</SSLPassPhrase>
      <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
      <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
  </Edge>
</SSL>

```

Debe tener dos archivos para cada conexión segura: uno para el certificado público SSL y uno para la clave privada que pertenece al certificado. Especifique la ubicación del certificado público SSL en la etiqueta `<SSLCertificateFile>`. Especifique la ubicación de la clave privada en la etiqueta `<SSLCertificateKeyFile>`. El servidor envía el certificado público SSL a los clientes. La clave privada permanece en el servidor.

3 Localice la siguiente línea en el archivo `Adaptor.xml`:

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Sustituya el código del paso 3 por el siguiente:

```
<HostPort name="meetingserver" ctl_channel=":19350">meetingServerIP:-443</HostPort>
<HostPort name="applicationserver" ctl_channel=":19351">appServerIP:-443</HostPort>
```

5 Guarde el archivo `Adaptor.xml`.

6 (Opcional) Abra el archivo `Adaptor.xml` en un explorador Web para validar la sintaxis.

Si el explorador Web detecta algún error, corríjalo y vuelva a abrir el archivo en un explorador Web. Repita este proceso hasta que el archivo sea válido.

7 Abra el archivo `custom.ini` ubicado en el directorio raíz de la instalación (`c:\breeze`, de forma predeterminada) y guarde una copia de seguridad en otra ubicación.

8 Introduzca el siguiente código en el archivo `custom.ini` sin sustituir ni eliminar el texto existente:

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

Nota: El archivo `custom.ini` distingue entre mayúsculas y minúsculas; utilice mayúsculas para los nombres de parámetro y minúsculas para los valores.

9 Guarde el archivo `custom.ini`.

10 Abra el archivo VHost.xml ubicado en `[root_install_dir]\comserv\win32\conf_defaultRoot_defaultVHost_` y guarde una copia de seguridad en otra ubicación.

11 Localice la siguiente línea en el archivo VHost.xml:

```
<RouteEntry></RouteEntry>
```

12 Sustituya la línea del paso 11 con el siguiente código:

```
<RouteEntry protocol="rtmp">*:*:*:${ORIGIN_PORT}</RouteEntry>
```

13 Guarde el archivo VHost.xml.

14 (Opcional) Abra el archivo Vhost.xml en un explorador Web para validar la sintaxis.

15 Reinicie Adobe Connect Pro Server 7:

- a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
- b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Meeting Server.
- c Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Meeting Server.
- d Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

16 Abra la consola de gestión de aplicaciones (<http://localhost:8510/console> o Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Configuración de Connect Pro Server 7).

17 En la pantalla Ajustes de la aplicación, seleccione Ajustes del servidor y realice las acciones siguientes:

- a Escriba el nombre de dominio completo (FQDN) de su cuenta de Acrobat Connect Pro en el cuadro Host de Connect Pro. Este FQDN es la dirección URL que utilizan los usuarios finales para conectarse a Acrobat Connect Pro.
- b Escriba el nombre de dominio completo (FQDN) del servidor de reuniones de Acrobat Connect Pro en el cuadro Nombre externo de Asignaciones de anfitrión. El servidor utiliza este valor de forma interna.

Asegurar sólo el servidor de aplicaciones

1 Abra el archivo Adaptor.xml que encontrará en `[root_install_dir]\comserv\win32\conf_defaultRoot_` y guarde una copia de seguridad en otra ubicación.

2 Introduzca el siguiente código en el archivo original Adaptor.xml entre las etiquetas `<Adaptor></Adaptor>` (sustituya el código en cursiva por sus propios valores):

```
<SSL>
  <Edge name="applicationserver">
    <SSLServerCtx>

      <SSLCertificateFile>[root_install_dir]\sslAppServerPublicCert.pem</SSLCertificateFile>
      <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslAppServerPrivateKey.pem</SSLCertificateKeyFile>
      <SSLPassPhrase>my passphrase</SSLPassPhrase>
      <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
      <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
  </Edge>
</SSL>
```

Debe tener dos archivos: uno para el certificado público SSL y otro para la clave privada que pertenece al certificado. Especifique la ubicación del certificado público SSL en la etiqueta `<SSLCertificateFile>`. Especifique la ubicación de la clave privada en la etiqueta `<SSLCertificateKeyFile>`. El servidor envía el certificado público SSL a los clientes. La clave privada permanece en el servidor.

3 Localice la siguiente línea en el archivo `Adaptor.xml`:

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Agregue el siguiente código debajo de la línea del paso 3:

```
<HostPort name="applicationserver" ctl_channel=":19351">:-443</HostPort>
```

5 Guarde el archivo `Adaptor.xml`.

6 (Opcional) Abra el archivo `Adaptor.xml` en un explorador Web para validar la sintaxis.

Si el explorador Web detecta algún error, corríjalo y vuelva a abrir el archivo en un explorador Web. Repita este proceso hasta que el archivo sea válido.

7 Abra el archivo `custom.ini` ubicado en el directorio raíz de la instalación (`c:\breeze`, de forma predeterminada) y guarde una copia de seguridad en otra ubicación.

8 Introduzca el siguiente código en el archivo `custom.ini` sin sustituir ni eliminar el texto existente:

```
ADMIN_PROTOCOL=https://  
SSL_ONLY=yes  
HTTPS_PORT=8443
```

Nota: El archivo `custom.ini` distingue entre mayúsculas y minúsculas; utilice mayúsculas para los nombres de parámetro y minúsculas para los valores.

9 Guarde el archivo `custom.ini`.

10 Reinicie Acrobat Connect Pro Server 7:

- a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
- b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Meeting Server.
- c Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Meeting Server.
- d Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

Asegurar sólo el servidor de reuniones

1 Abra el archivo `Adaptor.xml` que encontrará en `[root_install_dir]\comserv\win32\conf_defaultRoot_` y guarde una copia de seguridad en otra ubicación.

2 Introduzca el siguiente código en el archivo original `Adaptor.xml` entre las etiquetas `<Adaptor></Adaptor>` (sustituya el código en cursiva por sus propios valores):

```

<SSL>
  <Edge name="meetingserver">
    <SSLServerCtx>

<SSLCertificateFile>[root_install_dir]\sslMeetingServerPublicCert.pem</SSLCertificateFile>
    <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslMeetingServerPrivateKey.pem</SSLCertificateKeyFile>
    <SSLPassPhrase>mypassphrase</SSLPassPhrase>
    <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
    <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
  </Edge>
</SSL>

```

Debe tener dos archivos: uno para el certificado público SSL y otro para la clave privada que pertenece al certificado. Especifique la ubicación del certificado público SSL en la etiqueta <SSLCertificateFile>. Especifique la ubicación de la clave privada en la etiqueta <SSLCertificateKeyFile>. El servidor envía el certificado público SSL a los clientes. La clave privada permanece en el servidor.

3 Localice la siguiente línea en el archivo Adaptor.xml:

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Sustituya el código del paso 3 por el siguiente:

```
<HostPort name="meetingserver" ctl_channel=":19350">:-443</HostPort>
```

5 Guarde el archivo Adaptor.xml.

6 (Opcional) Abra el archivo Adaptor.xml en un explorador Web para validar la sintaxis.

Si el explorador Web detecta algún error, corríjalo y vuelva a abrir el archivo en un explorador Web. Repita este proceso hasta que el archivo sea válido.

7 Abra el archivo Vhost.xml que encontrará en [root_install_dir]\comserv\win32\conf_defaultVhost_ y guarde una copia de seguridad en otra ubicación.

8 Localice la siguiente línea en el archivo Vhost.xml:

```
<RouteEntry></RouteEntry>
```

9 Sustituya la línea del paso 8 por el siguiente código:

```
<RouteEntry protocol="rtmp">*:*:*:${ORIGIN_PORT}</RouteEntry>
```

10 Guarde el archivo Vhost.xml.

11 (Opcional) Abra el archivo Vhost.xml en un explorador Web para validar la sintaxis.

12 Abra el archivo custom.ini ubicado en el directorio raíz de la instalación (c:\breeze, de forma predeterminada) y guarde una copia de seguridad en otra ubicación.

13 Introduzca el siguiente código en el archivo custom.ini sin sustituir ni eliminar el texto existente:

```
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

14 Guarde el archivo custom.ini.

15 Reinicie Acrobat Connect Pro Server 7:

- a** Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
- b** Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Meeting Server.
- c** Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Meeting Server.

- d Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

Comprobar la configuración

- 1 Si ha asegurado el servidor de aplicaciones, inicie la sesión en Connect Pro Central. Aparecerá un candado en el explorador.
- 2 Si ha asegurado el servidor de reuniones, acceda a una sala de reuniones de Acrobat Connect Pro. Verá un candado en la luz de conexión.

Configurar una SSL basada en hardware

Al configurar una SSL basada en hardware, debe asegurar el servidor de aplicaciones (HTTP), el servidor de reuniones (RTMP) o ambos. Independientemente de la configuración que elija, debe configurar primero el servidor DNS.

Para obtener instrucciones adicionales acerca de cómo configurar el acelerador de hardware, consulte la documentación del proveedor.

Configurar el servidor DNS

- ❖ Cree entradas DNS para todos los servidores que quiera asegurar.

Defina un FQDN para cada servidor asegurado (por ejemplo, aplicación.ejemplo.com y reunión1.ejemplo.com).

Nota: En un clúster de servidores, todos los servidores de aplicaciones pueden compartir un certificado SSL, pero cada servidor de reuniones debe tener su propio certificado SSL. En un servidor único, para asegurar las conexiones HTTP (servidor de aplicaciones) y RTMP (servidor de reuniones), debe tener un total de dos certificados FQDN y dos certificados SSL (uno para cada protocolo).

Configurar una SSL para los servidores de reuniones y de aplicaciones

- 1 Configure el dispositivo de hardware para que realice lo siguiente:
 - a Escuchar externamente en un puerto 443 para aplicación.ejemplo.com.
 - b Reenviar datos no cifrados al servidor de aplicaciones del puerto 8443.
 - c Escuchar externamente en un puerto 443 para reunión1.ejemplo.com.
 - d Reenviar datos no cifrados al servidor de reuniones del puerto 1935.
 - e (Opcional) Escuchar externamente en un puerto 80 para aplicación.ejemplo.com y reenviar datos no cifrados al servidor de aplicaciones del puerto 80. El servidor de aplicaciones redirige los usuarios al puerto 443.
- 2 Configure el cortafuegos para que realice lo siguiente:
 - a Permitir el tráfico al servidor de aplicaciones del puerto 443 (y en el puerto 80 si ha finalizado el paso 1e).
 - b Permitir el tráfico al servidor de reuniones del puerto 443.
- 3 Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Configuración de Connect Pro Server 7 para abrir la consola de gestión de la aplicación. En la pantalla Ajustes de la aplicación, seleccione Ajustes del servidor y realice las acciones siguientes:
 - a Escriba el nombre de dominio completo (FQDN) del servidor de aplicaciones (por ejemplo, connect.ejemplo.com) en el cuadro Host de Connect Pro. Este FQDN es la dirección URL que utilizan los usuarios finales para conectarse a Acrobat Connect Pro.
 - b Escriba el nombre de dominio completo (FQDN) del servidor de reuniones (por ejemplo, fms.ejemplo.com) en el cuadro Nombre externo de Asignaciones de anfitrión. El servidor utiliza este valor de forma interna.

4 Abra el archivo custom.ini ubicado en el directorio raíz de la instalación (c:\breeze, de forma predeterminada) y guarde una copia de seguridad en otra ubicación.

5 Introduzca el siguiente código en el archivo custom.ini sin sustituir ni eliminar el texto existente:

```
ADMIN_PROTOCOL=https://  
SSL_ONLY=yes  
HTTPS_PORT=8443  
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

Nota: El archivo custom.ini distingue entre mayúsculas y minúsculas; utilice mayúsculas para los nombres de parámetro y minúsculas para los valores.

6 Guarde el archivo custom.ini.

7 Reinicie Acrobat Connect Pro Server 7:

a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.

b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

Configurar una SSL sólo para el servidor de aplicaciones

1 Configure el dispositivo de hardware para que realice lo siguiente:

a Escuchar externamente en un puerto 443 para reunión1.ejemplo.com.

b Reenviar datos no cifrados al servidor de reuniones del puerto 1935.

2 Configure el cortafuegos para que permita el tráfico al servidor de reuniones del puerto 443.

3 Abra el archivo custom.ini ubicado en el directorio raíz de la instalación (c:\breeze, de forma predeterminada) y guarde una copia de seguridad en otra ubicación.

4 Introduzca el siguiente código en el archivo custom.ini sin sustituir ni eliminar el texto existente:

```
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

5 Guarde el archivo custom.ini.

Configurar una SSL sólo para el servidor de aplicaciones

1 Configure el dispositivo de hardware para que realice lo siguiente:

a Escuchar externamente en un puerto 443 para aplicación.ejemplo.com.

b Reenviar datos no cifrados al servidor de aplicaciones del puerto 8443.

c (Opcional) Escuchar externamente en un puerto 80 para aplicación.ejemplo.com y reenviar datos no cifrados al servidor de aplicaciones del puerto 80. El servidor de aplicaciones redirige los usuarios al puerto 443.

2 Configure el cortafuegos para que permita el tráfico al servidor de aplicaciones del puerto 443 (y en el puerto 80 si ha finalizado el paso 1c).

3 En Acrobat Connect Pro, agregue lo siguiente al archivo custom.ini de la carpeta raíz de la instalación (c:\breeze, de forma predeterminada):

```
ADMIN_PROTOCOL=https://  
SSL_ONLY=yes  
HTTPS_PORT=8443
```

Nota: El archivo custom.ini distingue entre mayúsculas y minúsculas; utilice mayúsculas para los nombres de parámetro y minúsculas para los valores.

4 Reinicie Acrobat Connect Pro Server 7:

- a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
- b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

Comprobar la configuración

- 1 Si ha asegurado el servidor de aplicaciones, inicie la sesión en Connect Pro Central. Aparecerá un candado en el explorador.
- 2 Si ha asegurado el servidor de reuniones, acceda a una sala de reuniones de Acrobat Connect Pro. Verá un candado en la luz de conexión.

Configuración de una SSL de software para un servidor Edge

Si dispone de SSL de software configurada en el servidor de origen, configure una SSL de software para cada servidor Edge que quiera proteger.

De igual forma que el servidor de origen, un servidor Edge consiste de dos servicios: un servicio de reuniones y un servicio de aplicaciones. Para configurar SSL para ambos servicios, necesita dos FQDN y dos direcciones IP. Puede compartir el FQDN del servidor de aplicaciones con el servidor de origen, pero el servicio de reuniones debe tener su propio FQDN. El FQDN del servicio de aplicaciones es la dirección URL que utilizan los usuarios para conectar con las cuentas de Acrobat Connect Pro.

Por ejemplo, si tiene un servidor Edge y un servidor de origen, debe tener tres FQDN y tres certificados SSL: uno para cada servicio de reuniones y uno para que los compartan los servicios de aplicaciones. Debe disponer de cuatro direcciones IP, una para cada servicio de reuniones y una para cada servidor de aplicaciones.

En esta configuración de ejemplo, el servidor de origen tiene las direcciones IP y los FQDN siguientes:

```
10.192.37.11 = connect.yourcompany.com  
10.192.37.10 = meeting1.yourcompany.com
```

El servidor Edge tiene las direcciones IP y FQDN siguientes:

```
10.192.37.100 = connect.yourcompany.com  
10.192.37.101 = edge1.yourcompany.com
```

Nota: Si está instalando los servidores Edge y de origen por primera vez, configúrelos sin SSL y verifique que puedan comunicarse entre ellos. Cuando haya determinado que pueden comunicarse, puede configurar SSL para ambos servidores.

Más temas de ayuda

“[Implementación de Acrobat Connect Pro Edge Server](#)” en la página 28

“[Acerca de la compatibilidad de SSL](#)” en la página 65

Configuración del servidor Edge

- 1 En el servidor de origen, abra el archivo `c:\breeze\comserv\win32\conf_defaultRoot_\Adaptor.xml` y copie toda la sección `<SSL></SSL>` de la forma siguiente:

```

<SSL>
  <Edge name="applicationserver">
    <SSLServerCtx>
      <SSLCertificateFile>C:\breeze\connect.yourcompany.com.pem</SSLCertificateFile>
      <SSLCertificateKeyFile type="PEM">C:\breeze\connect.yourcompany.comKEY.pem
      </SSLCertificateKeyFile>
      <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
      <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
  </Edge>
  <Edge name="meetingserver">
    <SSLServerCtx>
      <SSLCertificateFile>C:\breeze\meetingPublicCert.pem
      </SSLCertificateFile>
      <SSLCertificateKeyFile type="PEM">C:\breeze\meetingPrivateKey.pem
      </SSLCertificateKeyFile>
      <SSLPassPhrase></SSLPassPhrase>
      <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
      <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
  </Edge>
</SSL>

```

Nota: Puede ser que su código contenga valores diferentes, pero debe contener los mismos elementos XML.

- 2 En el servidor Edge, abra el archivo c:\breeze\edgeserver\win32\conf_defaultRoot_\Adaptor.xml y copie el bloque de código `<SSL></SSL>` del servidor de origen detrás de la etiqueta `<Adaptor>`.
- 3 Realice las acciones siguientes para configurar el servicio de aplicaciones y el servicio de reuniones del servidor Edge:
 - a El servicio de aplicaciones es la etiqueta `<Edge name="applicationserver">` dentro del bloque `<SSL>`. El servicio de aplicaciones utiliza el mismo FQDN que el servicio de aplicaciones en el servidor de origen. Copie el certificado y los archivos .pem de clave del servidor de origen a la misma ubicación en el servidor Edge. En este ejemplo, el FQDN es connect.yourcompany.com.

```

<Edge name="applicationserver">
  <SSLServerCtx>
    <SSLCertificateFile>C:\breeze\connect.yourcompany.com.pem</SSLCertificateFile>
    <SSLCertificateKeyFile type="PEM">C:\breeze\connect.yourcompany.comKEY.pem
    </SSLCertificateKeyFile>
    <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
    <SSLSessionTimeout>5</SSLSessionTimeout>
  </SSLServerCtx>
</Edge>

```

- b El servicio de reuniones es la etiqueta `<Edge name="meetingserver">` dentro del bloque `<SSL>`. Edite el XML para que el servicio de reuniones señale un certificado único y una clave para su FQDN único. En este ejemplo, el FQDN es edge1.yourcompany.com.

```
<Edge name="meetingserver">
  <SSLServerCtx>
    <SSLCertificateFile>C:\breeze\edge1.yourcompany.com.pem
  </SSLCertificateFile>
    <SSLCertificateKeyFile type="PEM">C:\breeze\edge1.yourcompany.comKEY.pem
  </SSLCertificateKeyFile>
    <SSLPassPhrase></SSLPassPhrase>
    <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
    <SSLSessionTimeout>5</SSLSessionTimeout>
  </SSLServerCtx>
</Edge>
```

- 4** En el archivo `Adaptor.xml`, busque la línea `<HostPort name="edge1">${FCS.HOST_PORT}</HostPort>`. Agregue las dos líneas siguientes tras ella:

```
<HostPort name="meetingserver" ctl_channel=":19354">206.192.37.100:-443</HostPort>
<HostPort name="applicationserver" ctl_channel=":19355">206.192.37.101:-443</HostPort>
```

Este código enlaza las direcciones IP internas del servidor Edge para proteger el puerto 443. Este ejemplo utiliza las direcciones IP internas 206.192.37.100 y 206.192.37.101. En su código, reemplace las direcciones IP internas de su servidor Edge.

- 5** Guarde el archivo `Adaptor.xml`.

- 6** Abra el archivo `Adaptor.xml` en un explorador Web para verificar que el XML sea válido.

Si hay errores de sintaxis, el explorador Web muestra un mensaje de error. Corrija los errores de XML y vuelva a comprobar el archivo.

- 7** En el servidor Edge, abra el archivo `c:\breeze\edgeserver\win32\conf\defaultRoot_defaultVHost_Vhost.xml`. Busque la etiqueta `<RouteEntry></RouteEntry>` y sustitúyala por lo siguiente:

```
<RouteEntry protocol="rtmp">*:*;10.192.37.11:8506</RouteEntry>
```

Con este código, el servidor Edge enrutará las conexiones RTMP de cualquier dirección IP y cualquier puerto al servidor de origen mediante el puerto 8506. Este ejemplo utiliza la dirección IP 10.192.37.11. En su código, sustituya la dirección IP del servicio de aplicaciones en el servidor de origen.

- 8** Guarde el archivo `Vhost.xml`.

- 9** Abra el archivo `Vhost.xml` en un explorador Web para verificar que el XML sea válido.

Si hay errores de sintaxis, el explorador Web muestra un mensaje de error. Corrija los errores de XML y vuelva a comprobar el archivo.

- 10** En el servidor Edge, abra el archivo `c:\breeze\edgeserver\custom.ini`.

- 11** Introduzca el parámetro `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` y ajústelo a la dirección IP o el FQDN del servidor de origen, como en el ejemplo siguiente:

```
FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT=connect.yourcompany.com:443
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
FCS_EDGE_HOST=edge1.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=sanfran
FCS_EDGE_EXPIRY_TIME=60000
FCS_EDGE_REG_INTERVAL=30000
```

Si desea configurar el sistema para que sólo se conecte a través de SSL, comente el parámetro

`FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT` de la forma siguiente:

```
# FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

Nota: Si el servidor Edge no puede resolver el FQDN del servidor de origen, utilice la dirección IP.

12 En el servidor Edge, abra el archivo C:\breeze\edgeserver\win32\conf\HttpCache.xml y actualice la etiqueta `<HostName>` de la forma siguiente:

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

13 Guarde el archivo HttpCache.xml.

14 Abra el archivo HttpCache.xml en un explorador Web para verificar que el XML sea válido.

Si hay errores de sintaxis, el explorador Web muestra un mensaje de error. Corrija los errores de XML y vuelva a comprobarlo.

Configuración del servidor de origen

1 Configure SSL en el servidor de origen. Para obtener más información, consulte “[SSL \(capa de conexión segura\)](#)” en la página 65.

2 En el servidor de origen, abra el archivo c:\breeze\custom.ini e introduzca lo siguiente para enlazar el servidor Edge con el servidor de origen:

```
edge.FCS_EDGE_CLUSTER_ID=1
```

Utilice el valor del parámetro `FCS_EDGE_CLUSTER_ID` configurado en el archivo custom.ini del servidor Edge. En este ejemplo, el valor es `sanfran`, por lo que el código es `edge.sanfran=1`.

Nota: El valor 0 está reservado y no puede utilizarse.

3 Reinicie Connect Pro Central Application Server y Connect Pro Meeting Server.

4 Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Configuración de Connect Pro Server 7 para abrir la consola de gestión de la aplicación. Realice las acciones siguientes:

a Haga clic en Ajustes del servidor.

b En el cuadro Nombres externos, verá el FQDN del servidor Edge con un cuadro vacío a su derecha. Si no ve el FQDN, espere unos minutos y actualice el explorador.

c Introduzca el FQDN del servidor Edge en el cuadro vacío y haga clic en Guardar. Así se registrará el servidor Edge con el servidor de origen.

5 Configure el servidor DNS local para que dirija a los usuarios al servidor Edge cuando soliciten una dirección URL de Acrobat Connect Pro.

Configuración de una SSL de hardware para un servidor Edge

Si dispone de SSL de hardware configurada en el servidor de origen, configure una SSL de hardware para cada servidor Edge que quiera proteger.

De igual forma que el servidor de origen, un servidor Edge consiste de dos servicios: un servicio de reuniones y un servicio de aplicaciones. Para configurar SSL para ambos servicios, necesita dos FQDN y dos direcciones IP. Puede compartir el FQDN del servidor de aplicaciones con el servidor de origen, pero el servicio de reuniones debe tener su propio FQDN. El FQDN del servicio de aplicaciones es la dirección URL que utilizan los usuarios para conectar con las cuentas de Acrobat Connect Pro.

Por ejemplo, si tiene un servidor Edge y un servidor de origen, debe tener tres FQDN y tres certificados SSL: uno para cada servicio de reuniones y uno para que los compartan los servicios de aplicaciones. Debe disponer de cuatro direcciones IP, una para cada servicio de reuniones y una para cada servidor de aplicaciones.

En esta configuración de ejemplo, el servidor de origen tiene las direcciones IP y los FQDN siguientes:

```
10.192.37.11 = connect.yourcompany.com
10.192.37.10 = meeting1.yourcompany.com
```

El servidor Edge tiene las direcciones IP y FQDN siguientes:

```
10.192.37.100 = connect.yourcompany.com
10.192.37.101 = edge1.yourcompany.com
```

Nota: Si está instalando los servidores Edge y de origen por primera vez, configúrelos sin SSL y verifique que puedan comunicarse entre ellos. Cuando haya determinado que pueden comunicarse, puede configurar SSL para ambos servidores.

Más temas de ayuda

[“Implementación de Acrobat Connect Pro Edge Server”](#) en la página 28

[“Acerca de la compatibilidad de SSL”](#) en la página 65

Configuración del servidor Edge

- 1 En el servidor Edge, abra el archivo `c:\breeze\edgeserver\custom.ini`.
- 2 Introduzca el parámetro `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` y ajústelo a la dirección IP o el FQDN del servidor de origen, como en el ejemplo siguiente:

```
FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT=connect.yourcompany.com:443
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
FCS_EDGE_HOST=edge1.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=sanfran
FCS_EDGE_EXPIRY_TIME=60000
FCS_EDGE_REG_INTERVAL=30000
```

Si desea configurar el sistema para que sólo se conecte a través de SSL, comente el parámetro

`FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT` de la forma siguiente:

```
# FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

Nota: Si el servidor Edge no puede resolver el FQDN del servidor de origen, utilice la dirección IP.

- 3 En el servidor Edge, abra el archivo `C:\breeze\edgeserver\win32\conf\HttpCache.xml` y actualice la etiqueta `<HostName>` de la forma siguiente:

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

- 4 Guarde el archivo `HttpCache.xml`.
- 5 Abra el archivo `HttpCache.xml` en un explorador Web para verificar que el XML sea válido.

Si hay errores de sintaxis, el explorador Web muestra un mensaje de error. Corrija los errores de XML y vuelva a comprobarlo.

Configuración del servidor de origen

- 1 Configure SSL en el servidor de origen. Para obtener más información, consulte [“SSL \(capa de conexión segura\)”](#) en la página 65.
- 2 En el servidor de origen, abra el archivo `c:\breeze\custom.ini` e introduzca lo siguiente para enlazar el servidor Edge con el servidor de origen:

```
edge.FCS_EDGE_CLUSTER_ID=1
```

Utilice el valor del parámetro `FCS_EDGE_CLUSTER_ID` configurado en el archivo `custom.ini` del servidor Edge. En este ejemplo, el valor es `sanfran`, por lo que el código es `edge.sanfran=1`.

Nota: El valor 0 está reservado y no puede utilizarse.

- 3 Reinicie Connect Pro Central Application Server y Connect Pro Meeting Server.
- 4 Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Configuración de Connect Pro Server 7 para abrir la consola de gestión de la aplicación. Realice las acciones siguientes:
 - a Haga clic en Ajustes del servidor.
 - b En el cuadro Nombres externos, verá el FQDN del servidor Edge con un cuadro vacío a su derecha. Si no ve el FQDN, espere unos minutos y actualice el explorador.
 - c Introduzca el FQDN del servidor Edge en el cuadro vacío y haga clic en Guardar. Así se registrará el servidor Edge con el servidor de origen.
- 5 Configure el servidor DNS local para que dirija a los usuarios al servidor Edge cuando soliciten una dirección URL de Acrobat Connect Pro.

Etiquetas XML de SSL

Etiqueta	Valor predeterminado	Descripción
<code>SSLCertificateFile</code>	Sin valor predeterminado.	La ubicación del archivo del certificado que se va a enviar al cliente. Si no se especifica una ruta absoluta, se da por supuesto que el certificado es relativo al directorio <code>Adaptor</code> .
<code>SSLCertificateKeyFile</code>	Sin valor predeterminado.	La ubicación del archivo de clave privada para el certificado. Si no se especifica una ruta absoluta, se da por supuesto que el archivo de clave es relativo al directorio <code>Adaptor</code> . Si el archivo de clave está cifrado, debe indicarse la expresión de acceso en la etiqueta <code>SSLPassPhrase</code> . El atributo <code>type</code> especifica el tipo de codificación utilizado por el archivo de clave de certificado. El tipo puede ser <code>PEM</code> o <code>ASN1</code> .
<code>SSLCipherSuite</code>	Consulte la descripción.	El algoritmo de encriptación. El algoritmo consiste en elementos delimitados por dos puntos. Estos elementos pueden ser algoritmos de intercambio de claves, métodos de autenticación, métodos de encriptación, tipos de resumen o un alias de un número seleccionado para las agrupaciones comunes. Para obtener una lista de los componentes, consulte la documentación de Flash Media Server. Esta etiqueta tiene el siguiente valor predeterminado: <code>ALL: !ADH: !LOW: !EXP: !MD5: @STRENGTH</code> Póngase en contacto con el soporte técnico de Adobe antes de cambiar los valores predeterminados.
<code>SSLPassPhrase</code>	Sin valor predeterminado.	La expresión de acceso que se utiliza para descifrar el archivo de clave privada. Si el archivo de clave privada no está cifrado, deje esta etiqueta en blanco.
<code>SSLSessionTimeout</code>	5	La cantidad de tiempo que una sesión habilitada para SSL sigue siendo válida, en minutos.

Parámetros de configuración SSL

Parámetro	Valor predeterminado	Descripción
ADMIN_PROTOCOL	http://	El protocolo utilizado por el servidor de aplicaciones. Ajústelo en https:// para configurar una SSL.
DEFAULT_FCS_HOSTPORT	:1935	El puerto utilizado por Flash Media Server para comunicarse mediante el protocolo RTMP. Ajústelo en:443,1935 para configurar una SSL.
HTTPS_PORT	Sin valor predeterminado.	El puerto en el que el servidor de aplicaciones escucha solicitudes HTTPS. Este parámetro está normalmente definido en 443 o 8443 para configurar una SSL.
SSL_ONLY	no	Ajústelo en yes si el servidor sólo admite conexiones seguras. Este ajuste fuerza a todas las direcciones URL de Acrobat Connect Pro a utilizar HTTPS.
RTMP_SEQUENCE	Sin valor predeterminado.	Los orígenes, bordes y puertos utilizados para conectar con Flash Media Server (el servidor de reuniones).

PKI (infraestructura de clave pública)

Acerca de PKI (infraestructura de clave pública)

Puede configurar una infraestructura de clave pública (PKI) para gestionar credenciales de identificación como parte de la arquitectura de seguridad de Acrobat Connect Pro para sus clientes. En el protocolo SSL, más familiar, el servidor debe demostrar su identidad al cliente; en PKI, el cliente debe demostrar su identidad al servidor.

Un tercero de confianza, denominado entidad emisora de certificados, verifica la identidad de un cliente y enlaza un certificado al cliente. El certificado (también denominado *clave pública*) está en el formato X.509. Cuando un cliente se conecta a Acrobat Connect Pro, un proxy negocia la conexión para PKI. Si el cliente dispone de una cookie de una sesión anterior o tiene un certificado válido, el cliente se conecta a Acrobat Connect Pro.

Para obtener más información sobre PKI, consulte el Centro de Tecnología PKI de Microsoft

Requisitos de usuario de PKI

Los usuarios deben utilizar Windows XP o Windows 2003 y disponer de un certificado de cliente válido instalado en su equipo local antes de participar en una reunión que requiera la autenticación PKI. Cuando un usuario participa en una reunión, se le presenta un cuadro de diálogo para que elija un certificado de cliente válido de los certificados instalados en su equipo.

Adobe recomienda que los clientes que utilicen Adobe Acrobat Connect Add-in cuando asistan a reuniones que requieran autenticaciones PKI. Los clientes deben utilizar el instalador independiente de Add-in para instalarlo antes de participar en la reunión.

Los clientes también pueden utilizar la versión más reciente de Adobe Flash Player en el explorador para asistir a reuniones, pero la compatibilidad PKI de Flash Player no es tan extensa como la de Add-in. Sin embargo, para ver archivos de reuniones, los clientes deben tener instalada la versión más reciente de Flash Player.

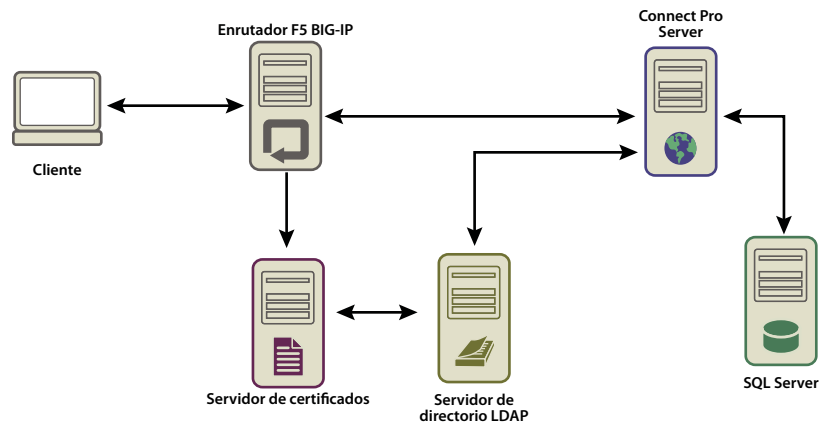
Puede diseñar un sistema PKI que sólo requiera autenticación para conexiones HTTP o para conexiones HTTP y RTMP. Si requiere certificados de cliente tanto en conexiones HTTP como RTMP, se les solicitará a los usuarios cada vez que se establezca una nueva conexión de servidor. Por ejemplo, no se solicitará que se inicie la sesión dos veces, una para HTTP y otra para RTMP. No se puede establecer una conexión RTMP sin autenticación HTTP, por lo que puede decidir solicitar autenticación del cliente sólo en la conexión HTTP.

Implementación PKI

Los pasos siguientes le guían a través de la implementación de referencia de PKI configurada con un enrutador F5 BIG-IP LTM 9.1.2 (compilación 40.2) como proxy. Utilice las secciones fundamentales para crear su propia solución, con un enrutador F5 y otro dispositivo.

Esta implementación de referencia cumple normativas de seguridad estrictas; por ejemplo, requiere un certificado de cliente tanto para las conexiones HTTP (servidor de la aplicación) como RTMP (servidor de la reunión).

Nota: Adobe recomienda encarecidamente que cree una normativa de seguridad antes de implementar PKI. Hay muchas tecnologías diferentes en PKI y mantener la seguridad es esencial cuando estos sistemas interactúan.



Flujo de datos en una infraestructura de clave pública

Este ejemplo asume lo siguiente:

- Se ha instalado Acrobat Connect Pro.
- Acrobat Connect Pro está integrado con un servicio de directorio LDAP.
- Un usuario importado del servicio de directorio LDAP puede entrar en una reunión de Acrobat Connect Pro.
- Hay un enrutador F5 instalado.

1. Configuración del servidor del directorio LDAP.

Debe especificarse un atributo `email` de LDAP para cada usuario. Este atributo se agrega al campo asunto del certificado de cliente.

F5 iRule busca la dirección de correo electrónico en `X.509::subject` e inserta el valor en el encabezado HTTP. Acrobat Connect Pro utiliza el encabezado HTTP para autenticar al usuario.

Nota: Este ejemplo utiliza el atributo `email`. Puede utilizar cualquier identificador único que expondrá el formato `X.509`, tenga una longitud de 254 caracteres o inferior y lo compartan el servicio de directorio LDAP y Acrobat Connect Pro.

2. Configuración de la normativa de inicio de sesión de Acrobat Connect Pro.

Acrobat Connect Pro debe utilizar una dirección de correo electrónico para el inicio de sesión de usuario. En el Connect Pro Central, seleccione la ficha Administración, a continuación haga clic en Usuarios y grupos y en Editar normativas de inicio de sesión y contraseña.

3. Configuración de un servidor de CA.

El servidor de CA (autoridad de certificación) recibe solicitudes de certificados, verifica identidades de cliente, emite certificados y gestiona una CRL (lista de revocación de clientes).

En esta implementación, la CA le dirige al servidor de directorio LDAP para obtener un certificado de cliente. La CA pide información del cliente al servidor LDAP y, si existe y no se ha revocado, la formatea en un certificado.

Compruebe en el campo asunto que el certificado de cliente está instalado y puede utilizarse. Presenta el siguiente aspecto:

```
E = adavis@asp.sflab.macromedia.com
CN = Andrew Davis
CN = Users
DC = asp
DC = sflab
DC = macromedia
DC = com
```

4. Configuración de Acrobat Connect Pro para utilizar la autenticación por encabezado HTTP.

En el archivo `[root_install_dir]\appserv\conf\WEB-INF\web.xml`, codifique sin marcas de comentario el código siguiente:

```
<filter-mapping>
  <filter-name>HeaderAuthenticationFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

Detenga el servidor de reuniones y el servidor de aplicaciones. En el archivo `custom.ini` del directorio de instalación raíz, agregue la línea siguiente:

```
HTTP_AUTH_HEADER=hah_login
```

Guarde el archivo `custom.ini` y reinicie Acrobat Connect Pro.

5. Configuración de la lógica de aplicación F5.

La lógica de la aplicación en F5 analiza el campo de asunto del certificado de cliente de la dirección de correo electrónico. La lógica pasa la dirección de correo electrónico a Acrobat Connect Pro en un encabezado HTTP adicional.

Si el cliente no dispone de un certificado, se rechaza. Si el cliente dispone de un certificado, debe autenticarse. Las verificaciones LDAP y OCSP (Online Certification Status Protocol) son ejemplos de mecanismos de autenticación.

Una vez autenticado el certificado, busque el identificador único conocido por Acrobat Connect Pro. En este ejemplo, se busca una dirección de correo electrónico en un certificado válido.

Si la solicitud incluye la cadena `session` o dispone de una cookie `BREEZESSESSION`, pasará sin autenticación porque el cliente ya se ha autenticado. Acrobat Connect Pro verifica estos argumentos con una consulta de la base de datos.

Si la solicitud no incluye la cadena `session` o la cookie `BREEZESSESSION`, el usuario debe iniciar la sesión en Acrobat Connect Pro. Para iniciar la sesión de un usuario, ponga el identificador único (en este caso la dirección de correo electrónico) en el campo `HTTP_AUTH_HEADER` y redirija la solicitud a la página de inicio de sesión de Acrobat Connect Pro.

El código siguiente es una regla F5 `iRule` colocada en el perfil HTTPS que se ocupa de las solicitudes:

```
set id [SSL::sessionid]
set the_cert [session lookup ssl $id]
set uname [X509::subject $the_cert]
set emailAddr [getfield $uname "emailAddress=" 2]
if { [HTTP::cookie exists BREEZESESSION] } {
    set cookie_payload [HTTP::cookie value BREEZESESSION]
}
elseif { [HTTP::uri] contains "/system/login" }
{
    # Connection has been redirected to the "login page"
    # The email address has been parsed from the certificate
    #
    HTTP::header insert hah_login $emailAddr
}
elseif { [HTTP::uri] contains "session" }
{
    #do nothing, Acrobat Connect Pro verifies the token found in session=$token
}
else
{
    # URI encode the current request, and pass it to
    # the Acrobat Connect Pro system login page because the client
    # does not have a session yet.
    HTTP::redirect https://[HTTP::host]/system/login/ok?next=[URI::encode
https://[HTTP::host][HTTP::uri]]
}
}
```

Más temas de ayuda

[“Inicio y parada de Acrobat Connect Pro Server”](#) en la página 87

Seguridad de la infraestructura

Seguridad de red

Acrobat Connect Pro depende de varios servicios de TCP/IP privados para sus comunicaciones. Estos servicios abren varios puertos y canales que deben protegerse de usuarios exteriores. Acrobat Connect Pro requiere que ponga los puertos que transmiten información confidencial detrás de un servidor de seguridad. El servidor de seguridad debe admitir la tecnología de inspección de paquetes además del filtrado de paquetes. El servidor de seguridad debería tener una opción para "rechazar todos los servicios de forma predeterminada excepto aquellos permitidos de forma explícita". El servidor de seguridad debería ser al menos un servidor de seguridad de dos sitios (dos o más interfaces de red). Esta arquitectura ayuda a evitar que los usuarios no autorizados atraviesen la seguridad del servidor de seguridad.

La solución más sencilla para asegurar Acrobat Connect Pro es bloquear todos los puertos del servidor excepto el 80, el 1935 y el 443. Un dispositivo de servidor de seguridad de hardware externo proporciona una capa de protección contra las lagunas de seguridad del sistema operativo. Puede configurar capas de servidores de seguridad basados en hardware para formar DMZ. Si su departamento de seguridad actualiza el servidor cuidadosamente con las revisiones de seguridad más recientes de Microsoft, se puede configurar un servidor de seguridad de software para habilitar seguridad adicional.

Acceso a Intranet

Si los usuarios pueden acceder a Acrobat Connect Pro en su intranet, ponga los servidores de Acrobat Connect Pro y la base de datos de Acrobat Connect Pro en una subred independiente, separada por un servidor de seguridad. El segmento de red interno en el que se ha instalado Acrobat Connect Pro debería utilizar direcciones IP privadas (10.0.0.0/8, 172.16.0.0/12 o 192.168.0.0/16) para que sea más difícil para los atacantes enrutar el tráfico a una IP pública y desde la IP interna traducida de la dirección de red. Si desea obtener más información, consulte RFC 1918. Esta configuración del servidor de seguridad debería tener en cuenta todos los puertos de Acrobat Connect Pro y si están configurados para tráfico entrante o saliente.

Seguridad del servidor de base de datos

Tanto si la base de datos está instalada en el mismo servidor que Acrobat Connect Pro como si no, debe comprobar que la base de datos sea segura. Los equipos en los que esté instalada una base de datos deberían estar en una ubicación física segura. Las siguientes son precauciones adicionales:

- Instale la base de datos en la zona segura de su intranet.
- No conecte nunca la base de datos a Internet directamente.
- Realice copias de seguridad frecuentes de sus datos y guarde las copias en una ubicación externa segura.
- Instale las revisiones más recientes del servidor de la base de datos.
- Utilice conexiones de confianza de SQL.

Para obtener información sobre la seguridad de SQL Server, consulte el sitio web de seguridad de Microsoft SQL.

Creación de cuentas de servicio

La creación de una cuenta de servicio de Acrobat Connect Pro le permite ejecutar Acrobat Connect Pro de forma más segura. Adobe recomienda la creación de una cuenta de servicio y una cuenta de SQL Server 2005 Express Edition para Acrobat Connect Pro. Para obtener más información, consulte los artículos de Microsoft “How to change the SQL Server or SQL Server Agent service account without using SQL Enterprise Manager in SQL Server 2000 or SQL Server Configuration Manager in SQL Server 2005” y “The Services and Service Accounts Security and Planning Guide”.

Creación de una cuenta de servicio

- 1 Cree una cuenta local llamada ConnectService que no incluya ningún grupo predeterminado.
- 2 Establezca los servicios de Adobe Connect Enterprise Service, Flash Media Administration Server y Flash Media Server (FMS) en esta nueva cuenta.
- 3 Establezca “Control total” para la clave de registro siguiente:
`HKLM\SYSTEM\ControlSet001\Control\MediaProperties\PrivateProperties\Joystick\Winmm`
- 4 Establezca “Control total” en las carpetas NTFS de la ruta de la carpeta raíz Acrobat Connect Pro (c:\breeze de forma predeterminada).

Las subcarpetas y los archivos deben tener los mismos permisos. Para clústeres, modifique las rutas correspondientes para cada nodo de equipo.

- 5 Establezca los derechos de inicio de sesión siguientes para la cuenta ConnectService:

Iniciar sesión como servicio—SeServiceLogonRight

Creación de una cuenta de SQL Server 2005 Express Edition

- 1 Cree una cuenta local llamada ConnectSqlService que no incluya ningún grupo predeterminado.

2 Cambie la cuenta de servicio de SQL Server 2005 Express Edition de LocalSystem a ConnectSqlService.

3 Establezca “Control total” de ConnectSqlService para las claves de registro siguientes:

```
HKEY_LOCAL_MACHINE\Software\Clients\Mail  
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\80  
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\[databaseInstanceName]
```

Para clústeres, siga este paso para cada nodo del clúster. El permiso de control total se aplica a todas las claves secundarias de una instancia de base de datos concreta

4 Establezca “Control total” para ConnectSqlService en las carpetas de bases de datos. Las subcarpetas y los archivos también deben tener los mismos permisos. Para clústeres, modifique las rutas correspondientes para cada nodo de equipo.

5 Establezca los derechos de usuario siguientes para el servicio ConnectSqlService:

Funcionar como parte de un sistema operativo—SeTcbPrivilege Evitar comprobaciones transversas—SeChangeNotify Bloquear páginas en la memoria—SeLockMemory Iniciar sesión como tarea de lotes—SeBatchLogonRight Iniciar sesión como un servicio—SeServiceLogonRight Reemplazar un cupón de nivel de proceso—SeAssignPrimaryTokenPrivilege

Seguridad de instalaciones de servidor único

El flujo de trabajo siguiente resume el proceso de configuración y seguridad de Acrobat Connect Pro en un equipo único. Asume que la base de datos se instalará en el mismo equipo y que los usuarios accederán a Acrobat Connect Pro por Internet.

1. Instalación de un servidor de seguridad.

Dado que los usuarios tienen permitida la conexión a Acrobat Connect Pro a través de Internet, el servidor está abierto a los ataques de los piratas informáticos. Si utiliza un servidor de seguridad, puede bloquear el acceso al servidor y controlar las comunicaciones que se producen entre Internet y el servidor.

2. Configure el servidor de seguridad.

Tras instalar el servidor de seguridad, configúrelo como sigue:

- Puertos entrantes (de Internet): 80, 443, 1935.
- Puertos salientes (al servidor de correo): 25.
- Utilice sólo el protocolo TCP/IP.

Como la base de datos está en el mismo servidor que Acrobat Connect Pro, no tiene que abrir el puerto 1434 en el servidor de seguridad.

3. Instalación de Acrobat Connect Pro.

4. Verificación de que las aplicaciones de Acrobat Connect Pro funcionen.

Tras instalar Acrobat Connect Pro, compruebe que funcione correctamente desde Internet y desde la red local.

5. Pruebe el servidor de seguridad.

Tras haber instalado y configurado el servidor de seguridad, compruebe que funcione correctamente. Para probar el servidor de seguridad, intente utilizar los puertos bloqueados.

Seguridad de clústeres

Los sistemas de clústeres (con varios servidores) son de por sí más complejos que las configuraciones con un único servidor. Un clúster de Acrobat Connect Pro puede estar en un centro de datos o distribuirse a través de varios centros de operaciones en red. Puede instalar y configurar servidores con Connect Pro en varias ubicaciones y sincronizarlos a través de la replicación de bases de datos.

Nota: Los clústeres deben utilizar Microsoft SQL Server 2005 Standard Edition y no el motor de procesamiento de la base de datos integrada.

Las sugerencias siguientes son importantes para la seguridad de los clústeres:

Redes privadas La solución más simple para los clústeres en una ubicación única es crear una subred adicional para el sistema Acrobat Connect Pro. Este método ofrece un alto nivel de seguridad.

Servidores de seguridad de software locales Para los servidores de Acrobat Connect Pro que están ubicados en un clúster pero comparten una red pública con otros servidores, puede ser apropiado configurar un servidor de seguridad de software en cada servidor.

Sistemas VPN En las instalaciones multiservidor con Acrobat Connect Pro en diferentes ubicaciones físicas, considere utilizar un canal encriptado para comunicarse con los servidores remotos. Muchos distribuidores de software y hardware ofrecen tecnología VPN para asegurar las comunicaciones con servidores remotos. Acrobat Connect Pro depende de esta seguridad externa para cifrar el tráfico de datos.

Sugerencias y recursos de seguridad

Mejores prácticas de seguridad

La lista de verificación siguiente describe las prácticas recomendadas para proteger su sistema Acrobat Connect Pro:

Utilice SSL para proteger el tráfico de red Puede asegurar la conexión con el servidor de reuniones, el servidor de aplicaciones o ambas.

Ejecute sólo los servicios que necesite No debería ejecutar aplicaciones como un controlador de dominio, un servidor web o un servidor FTP en el mismo equipo que Acrobat Connect Pro. Para que sea más difícil que otra aplicación se utilice para comprometer el servidor, reduzca el número de aplicaciones y servicios que se ejecuten en el equipo que dispone de Acrobat Connect Pro.

Actualice la seguridad del sistema operativo Compruebe con regularidad si hay actualizaciones esenciales que cubran problemas de seguridad y aplique las revisiones necesarias. Un servidor de seguridad elimina algunos de estos problemas de seguridad. En general, mantenga los servidores actualizados con todas las actualizaciones de seguridad actuales aprobadas por Microsoft y el resto de distribuidores de plataformas relevantes.

Sistemas de host seguros Si almacena información confidencial en los servidores, tenga en cuenta la seguridad física de los sistemas. Acrobat Connect Pro depende de la seguridad del sistema host contra intrusos, por lo que los servidores deben mantenerse seguros cuando se ponen en riesgo datos privados y confidenciales. Acrobat Connect Pro está diseñado para aprovechar las funciones del entorno nativo, como la encriptación de archivos del sistema.

Utilice contraseñas sólidas Las contraseñas sólidas protegen los datos. Los administradores de Acrobat Connect Pro pueden establecer normativas de inicio de sesión y contraseñas en Connect Pro Central. Las instalaciones de Acrobat Connect Pro suelen utilizar Microsoft SQL Server 2005 Standard Edition, que también requiere una protección de contraseña segura.

Uso de LDAP o del inicio único para la autenticación Se recomienda utilizar LDAP o el inicio único para la autenticación de Connect Pro. Si no utiliza LDAP o el inicio único, asegúrese de que los usuarios finales no utilicen para Connect Pro la misma contraseña que usan para otros sistemas

Realice auditorías de seguridad con regularidad Realice auditorías de sus sistemas periódicamente para asegurarse de que todas las funciones de seguridad continúan funcionando como desea. Por ejemplo, puede utilizar un buscador de puertos para probar un servidor de seguridad.

Recursos y referencias de seguridad

Los recursos siguientes le ayudarán a asegurar sus servidores:

Seguridad de red El Instituto SANS (System Administration, Networking, and Security) es una organización de educación e investigación cooperativa que incluye administradores de sistema, profesionales de seguridad y administradores de red. Ofrece cursos sobre seguridad de red, así como certificación en seguridad de redes.

Seguridad de SQL Server La página de recursos de seguridad de Microsoft SQL en el sitio Web de Microsoft proporciona información sobre la seguridad de SQL Server.

Herramientas NMap es un potente programa de búsqueda de puertos que le informa de los puertos a los que escucha un sistema. Está disponible de forma gratuita bajo la Licencia Pública General GNU (GPL).

***Nota:** La eficacia de cualquier medida de seguridad la determinan varios factores, como las medidas de seguridad proporcionadas por el servidor y el software de seguridad instalado. El software de Acrobat Connect Pro no está diseñado para proporcionar seguridad a su servidor o la información contenida en él. Para obtener más información, consulte el aviso legal sobre garantía en el acuerdo de licencia aplicable proporcionado por Acrobat Connect Pro.*

Capítulo 5: Administración de Connect Pro Server

La administración de Acrobat Connect Pro Server implica las siguientes acciones:

- Administración y supervisión de archivos de registro para mantener el tiempo de funcionamiento del sistema
- Mantenimiento del espacio en disco
- Copia de seguridad de datos
- Creación y generación de informes de uso

Inicio y parada de los servidores

Inicio y parada de Acrobat Connect Pro Server

Puede iniciar o detener Acrobat Connect Pro desde el menú Inicio, la ventana Servicios o la línea de comandos. Antes de iniciar Connect Pro Server, compruebe que se esté ejecutando la base de datos.

Parada de Acrobat Connect Pro desde el menú Inicio

- 1 Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Application Server.
- 2 Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Meeting Server.

Inicio de Acrobat Connect Pro desde el menú Inicio

- 1 Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Meeting Server.
- 2 Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Application Server.

Parada de Acrobat Connect Pro desde la ventana Servicios

- 1 Para abrir la ventana Servicios, seleccione Inicio > Panel de control > Herramientas administrativas > Servicios.
- 2 Detenga el servicio Adobe Connect Enterprise Service.
- 3 Detenga el servicio Flash Media Server (FMS).
- 4 Detenga el servicio Flash Media Administration Server.

Inicio de Acrobat Connect Pro desde la ventana Servicios

- 1 Seleccione Inicio > Todos los programas > Herramientas administrativas > Servicios para abrir la ventana Servicios.
- 2 Inicie el servicio Flash Media Server (FMS).
- 3 Inicie el servicio Flash Media Administration Server.
- 4 Inicie el servicio Adobe Connect Enterprise Service.

Parada de Acrobat Connect Pro desde la línea de comandos

- 1 Seleccione Inicio > Ejecutar para abrir la ventana Ejecutar. Introduzca **cmd** para abrir un símbolo del sistema.
- 2 Vaya al directorio breeze\appserv\win32.
- 3 Introduzca el siguiente comando para detener Acrobat Connect Pro:

```
net stop ConnectPro
```

- 4 Introduzca lo siguiente para detener Flash Media Server:

```
net stop FMS
```

- 5 Introduzca lo siguiente para detener Flash Media Server Administration Server:

```
net stop FMSAdmin
```

Inicio de Acrobat Connect Pro desde la línea de comandos

- 1 Seleccione Inicio > Ejecutar para abrir la ventana Ejecutar. Introduzca **cmd** para abrir un símbolo del sistema.
- 2 Vaya al directorio breeze\appserv\win32.
- 3 Introduzca lo siguiente para iniciar Flash Media Server:

```
net start FMS
```

- 4 Introduzca lo siguiente para iniciar Flash Media Server Administration Server:

```
net start FMSAdmin
```

- 5 Para iniciar Acrobat Connect Pro, introduzca lo siguiente:

```
net start ConnectPro
```

Inicio y parada de Connect Pro Presence Service

Puede iniciar y detener Connect Pro Presence Service desde el menú Inicio o la ventana Servicios. Inicie Connect Pro Presence Service sólo si el sistema Acrobat Connect Pro está integrado con Microsoft Live Communications Server u Office Communications Server.

Más temas de ayuda

“[Integración con Microsoft Live Communications Server 2005 y Microsoft Office Communications Server 2007](#)” en la página 52

Parada del servicio de presencia desde el menú Inicio

- ❖ Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Presence Service.

Inicio del servicio de presencia desde el menú Inicio

- ❖ Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Presence Service.

Parada, inicio o reinicio del servicio de presencia desde la ventana Servicios

- 1 Para abrir la ventana Servicios, seleccione Inicio > Panel de control > Herramientas administrativas > Servicios.
- 2 Seleccione Acrobat Connect Pro Presence Service.
- 3 Seleccione Iniciar, Detener o Reiniciar el servicio.

Inicio y parada de Flash Media Gateway

Puede iniciar y detener Flash Media Gateway desde la ventana Servicios o desde la línea de comandos. Compruebe si Connect Pro Server se está ejecutando antes de iniciar Flash Media Gateway.

Inicio y parada de Flash Media Gateway desde la ventana Servicios

- 1 Para abrir la ventana Servicios, seleccione Inicio > Panel de control > Herramientas administrativas > Servicios.
- 2 Seleccione el servicio Flash Media Gateway.
- 3 Seleccione Iniciar, Detener o Reiniciar el servicio

Inicio y parada de Flash Media Gateway desde la línea de comandos

- 1 Seleccione Inicio > Ejecutar para abrir la ventana Ejecutar. Introduzca `cmd` para abrir un símbolo del sistema.
- 2 Introduzca lo siguiente para iniciar Flash Media Gateway:

```
net start fmg
```

- 3 Introduzca lo siguiente para detener Flash Media Gateway:

```
net stop fmg
```

Inicio y parada de Acrobat Connect Pro Edge Server

Puede iniciar o detener Acrobat Connect Pro Edge Server 7 desde el menú Inicio, la ventana Servicios o la línea de comandos.

Parada de Acrobat Connect Pro Edge Server 7 desde el menú Inicio

- ❖ Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Edge Server 7 > Detener Connect Pro Edge Server.

Inicio de Acrobat Connect Pro Edge Server 7 desde el menú Inicio

- ❖ Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Edge Server 7 > Iniciar Connect Pro Edge Server.

Parada de Acrobat Connect Pro Edge Server 7 desde la ventana Servicios

- 1 Seleccione Inicio > Configuración > Panel de control > Herramientas administrativas > Servicios para abrir la ventana Servicios.
- 2 Detenga el servicio Flash Media Server (FMS).
- 3 Detenga el servicio Flash Media Server Administration Server.

Inicio de Acrobat Connect Pro Edge Server desde la ventana Servicios

- 1 Seleccione Inicio > Configuración > Panel de control > Herramientas administrativas > Servicios para abrir la ventana Servicios.
- 2 Inicie el servicio Flash Media Server Administration Server.
- 3 Inicie el servicio Flash Media Server (FMS).

Parada de Acrobat Connect Pro Edge Server desde la línea de comandos

- 1 Seleccione Inicio > Ejecutar para abrir la ventana Ejecutar. Introduzca `cmd` para abrir un símbolo del sistema.
- 2 Introduzca lo siguiente para iniciar Flash Media Server:

```
net stop FMS
```

3 Introduzca lo siguiente para iniciar Flash Media Server Administration Server:

```
net stop FMSAdmin
```

Inicio de Acrobat Connect Pro Edge Server desde la línea de comandos

1 Seleccione Inicio > Ejecutar para abrir la ventana Ejecutar. Introduzca **cmd** para abrir un símbolo del sistema.

2 Introduzca lo siguiente para iniciar Flash Media Server Administration Server:

```
net start FMSAdmin
```

3 Introduzca lo siguiente para iniciar Flash Media Server:

```
net start FMS
```

Administración y supervisión de registros

Acerca de los archivos de registro

Utilice los archivos de registro de Acrobat Connect Pro Server para ver información sobre los eventos que ocurren durante la operación. Puede utilizar la información de los archivos de registro para crear mecanismos e informes de supervisión y para solucionar problemas. Los archivos de registro ofrecen información sobre las actividades de los usuarios y el rendimiento del servidor. Por ejemplo, los archivos de registro pueden indicar el motivo por el que se le ha denegado el acceso a un usuario cuando ha intentado iniciar sesión. O el motivo del fallo de una conexión telefónica.

Acrobat Connect Pro Server incluye cinco archivos de registro en la carpeta *RootInstallationFolder*\logs. Use los archivos *access.log* y *error.log* para controlar Acrobat Connect Pro. Los tres archivos de registro restantes son internos y no son necesarios para el funcionamiento del sistema.

access.log Contiene información sobre los intentos de acceso al servidor.

breeze.log Contiene información sobre el inicio correcto o fallido de *ConnectPro.exe*.

error.log Contiene información sobre los problemas del sistema.

service-err.log Recopila los errores que se producen en la aplicación y durante el inicio.

service-out.log Recopila los mensajes *STDOUT* y *STDERR* que genera Java Virtual Machine.

Entrada de muestra de archivos de registro

La entrada de muestra siguiente procede del archivo *access.log* e incluye un encabezado, una lista con los campos que se utilizan en la entrada de registro y los datos específicos de esta entrada de registro:

```
#Version: 1.0
#Start-Date: 2006-10-30 17:09:24 PDT
#Software: Adobe Acrobat Connect Pro Server 7
#Date: 2006-04-30
#Fields: date time x-comment x-module x-status x-severity x-category x-user x-access-request
time-taken db-logical-io db-transaction-update-count
2006-10-30 18:12:50 Not logged in. PRINCIPAL NO_ACCESS_NO_LOGIN W A PUBLIC
{cookie=breezxn5pquysyhgfttt, ip=138.1.21.100} GET http://joeuser.macromedia.com&mode=xml 0
20/5 0
```

En la siguiente tabla se explica la entrada de muestra:

Campo	Datos	Descripción
date	2006-10-30	Fecha en la que se produce el evento registrado.
time	18:12:50	Hora a la que se produce el evento registrado.
x-comment	Not logged in.	Indica que el usuario no ha podido iniciar sesión en el servidor de la aplicación.
x-module	PRINCIPAL	El evento se ha producido en el módulo Principal del servidor de la aplicación.
x-status	NO_ACCESS_NO_LOGIN	Indica que el usuario no ha podido iniciar sesión.
x-severity	W	Identifica el grado de gravedad del evento como una advertencia (W).
x-category	A	Indica que el evento consiste en un problema de acceso (A) (que aparece en el archivo access.log).
x-user	PUBLIC	El usuario actual. En este caso se trata de un invitado no identificado o de un usuario público.
x-access-request	http://joeuser.macromedia.com&mode=xml	Origen de la solicitud.
time-taken	0	No se ha necesitado tiempo para procesar la solicitud.
db-logical-io	20/5	Se han necesitado 20 lecturas de la base de datos y se han devuelto cinco filas de datos.
db-transaction-update-count	0	No se ha actualizado ninguna fila de base de datos durante el procesamiento de la solicitud.

Rotación de archivos de registro

Puede alternar los archivos access.log y error.log. Modifique los valores predeterminados de los siguientes parámetros en el archivo custom.ini (en *RootInstallationFolder*\custom.ini de forma predeterminada) para especificar la frecuencia con la que se deben alternar los archivos de registro:

```
ACCESS_LOG_ROTATE_DAYS=1.0
ACCESS_LOG_ROTATE_KEEP=7
ERROR_LOG_ROTATE_DAYS=1.0
ERROR_LOG_ROTATE_KEEP=7
```

Los parámetros *_DAYS determinan en días la frecuencia con la que deben alternarse los archivos de registro. Para medio día, utilice el valor 0,5.

Los parámetros *_KEEP determinan los días que se deben conservar los archivos de registro antes de eliminarse. Los archivos de registro se conservan durante una semana de forma predeterminada.

Cuando haya modificado el archivo custom.ini, reinicie Connect Pro Central Application Server.

Formato del archivo de registro

Los archivos de registro utilizan el formato de archivo de registro W3C Extended. Puede leerlos con cualquier editor de texto.

Campos de registro en los archivos access.log y error.log

Las entradas de registro incluyen 11 campos de registro que ofrecen información sobre el tipo de evento que se ha producido, cuándo se ha producido, la gravedad y otros datos relevantes:

Campo	Formato	Descripción
date	AAAA/MM/DD	Fecha en la que se ha llevado a cabo la transacción.
time	HH:MM:SS	Hora en el equipo local a la que se ha llevado a cabo la transacción.
x-comment	Cadena	Contiene información en forma de frases sobre la entrada de registro. Este campo se sitúa siempre en el extremo izquierdo del registro.
x-module	Cadena	Indica el lugar en el que se ha producido el error.
x-status	Cadena	Indica el evento que se ha producido.
x-severity	Texto (un carácter)	Indica el grado de gravedad del evento registrado: muy grave (C), error (E), advertencia (W) o informativo (I).
x-category	Texto (un carácter)	Indica si la entrada de registro representa un evento de acceso (A) o del sistema (S).
x-user	Cadena	Texto que representa al usuario actual. Sólo es pertinente si el campo x-category indica (A). De lo contrario, el campo se rellena con un guión (-) que indica que el campo no incluye ningún valor.
x-access-request	Cadena	Texto que representa la solicitud de acceso. El texto puede ser una dirección URL o un nombre de API con parámetros pasados. Sólo es pertinente si el campo x-category indica (A). De lo contrario, el campo se rellena con un guión (-) que indica que el campo no incluye ningún valor.
time-taken	Númerica	Tiempo necesario para procesar la solicitud (en segundos). Sólo es pertinente si el campo x-category indica (A). De lo contrario, el campo se rellena con un guión (-) que indica que el campo no incluye ningún valor.
db-logical-io	Cadena	Número de lecturas de la base de datos que se necesitan para procesar la solicitud y número de filas que se devuelven con el formato <reads>/<rows>.
db-transaction-update-count	Cadena	Número de filas actualizadas en transacciones durante el procesamiento de las solicitudes. Si la solicitud utiliza más de una transacción, el valor es la suma de las actualizaciones.

Entradas del campo módulo

Los módulos son componentes del sistema que gestionan un conjunto de operaciones relacionadas entre sí. Los módulos pertenecen al servidor de la aplicación o al servidor de reuniones. El campo x-module indica el lugar en el que se produce el evento:

Entrada de registro para el campo x-module	Descripción	Server
ACCESS_KEY	Gestiona las claves de acceso.	Servidor de aplicaciones
ACCOUNT	Gestiona las operaciones de la cuenta.	Servidor de aplicaciones
ACL	Gestiona las operaciones relacionadas con ACL.	Servidor de aplicaciones
AICC	Gestiona la comunicación de AICC entre el servidor y el contenido.	Servidor de aplicaciones
BUILDER	Construye SCO.	Servidor de aplicaciones
Client	Métodos de cliente.	Servidor de reuniones
CLUSTER	Gestiona las operaciones relacionadas con los clúster.	Servidor de aplicaciones
CONSOLE	Gestiona las operaciones relacionadas con las consolas.	Servidor de aplicaciones
Content	Pod para compartir.	Servidor de reuniones

Entrada de registro para el campo x-module	Descripción	Server
DB	Representa la base de datos.	Servidor de aplicaciones
EVENT	Gestiona las operaciones relacionadas con los eventos.	Servidor de aplicaciones
HOSTED_MANAGER	Gestiona las cuentas del sistema (crear, actualizar, eliminar, ajustes, etc.).	Servidor de aplicaciones
MEETING	Gestiona las operaciones relacionadas con las reuniones.	Servidor de aplicaciones
Misc	Módulo misceláneo.	Servidor de reuniones
NOTIFICATION	Gestiona todas las operaciones relacionadas con el correo electrónico.	Servidor de aplicaciones
PERMISSION	Gestiona las operaciones relacionadas con los permisos.	Servidor de aplicaciones
Poll	Pod de Encuesta.	Servidor de reuniones
PLATFORM_FRAMEWORK	Representa el marco de la plataforma.	Servidor de aplicaciones
PRINCIPAL	Gestiona las operaciones relacionadas con los principales.	Servidor de aplicaciones
REPORT	Representa los informes.	Servidor de aplicaciones
Room	Gestiona la apertura y el cierre de la sala de reuniones.	Servidor de reuniones
RTMP	Representa a RTMPHandler.	Servidor de aplicaciones
SCO	Gestiona las operaciones relacionadas con SCO.	Servidor de aplicaciones
SEARCH	Gestiona las operaciones relacionadas con las búsquedas.	Servidor de aplicaciones
START_UP	Representa al componente de inicio.	Servidor de aplicaciones
TELEPHONY	Gestiona las operaciones relacionadas con la telefonía.	Servidor de aplicaciones
TRACKING	Gestiona las operaciones relacionadas con las transcripciones.	Servidor de aplicaciones
TRAINING	Gestiona las operaciones relacionadas con la formación.	Servidor de aplicaciones

Entradas del campo comentario y estado

Los campos x-comment y x-status indican el tipo de evento que se ha producido. El campo x-status muestra un código para cada evento registrado. El campo x-comment muestra una descripción de los eventos registrados.

En la tabla siguiente se muestran los códigos de estado, los comentarios asociados a cada código y una explicación para cada evento registrado:

Entrada de registro para el campo x-status	Entrada de registro para el campo x-comment	Descripción
ACCESS_DENIED	Client trying to access protected method. Access is denied. {1}	Se registra cuando el cliente intenta acceder a un método protegido.
BECAME_MASTER	Server {1} has been designated the master.	Se registra cuando el programador se cierra y el servidor asume su función.
CLUSTER_CON_BROKEN	Server {1} unable to reach {2} on port {3} to perform cluster operations.	Se registra cuando Acrobat Connect Pro no puede acceder a otro servidor del clúster.
CLUSTER_FILE_TRANSFER_ERROR	Unable to transfer {1} from server {2}.	Se registra cuando se produce un error al transferir un archivo.
CONNECT	New client connecting: {1}	Se registra cuando un nuevo cliente realiza la conexión.
CONNECT_WHILE_GC	Connecting while the app is shutting down - forcing shutdown.	Se registra cuando un cliente intenta realizar la conexión en el momento en el que la aplicación se está cerrando.
DB_CONNECTION_ERROR	Unable to connect to database {1}.	Se registra cuando Acrobat Connect no puede acceder a la base de datos.
DB_CONNECTION_TIME_OUT	Timed out waiting for database connection.	Se registra cuando la conexión a la base de datos tarda demasiado.
DB_VERSION_ERROR	Database {1} is incompatible with the current version of >Acrobat Connect Pro.	Se registra cuando la base de datos no está actualizada.
DISCONNECT	A client is leaving. Details: {1}	Se registra cuando el cliente se desconecta.
EXT_ERROR	External error thrown by a third party.	Se registra cuando el código externo emite un error.
FMS_CON_BROKEN	Health check failed due to broken FMS service connection.	Se registra cuando la conexión de servicio contiene un error.
FMS_NOT_FOUND	Unable to connect to FMS at start up.	Se registra cuando Acrobat Connect no puede establecer la conexión de servicio durante el inicio.
INTERNAL_ERROR	Internal error occurred.	Se registra cuando se produce un error interno.
INVALID	-	Se registra cuando se intenta llevar a cabo una operación no válida.
INVALID_DUPLICATE	Value {1} is a duplicate in the system.	Se registra cuando el valor que se introduce es igual a un valor del sistema.
INVALID_FORMAT	Field {1} of type {2} is invalid.	El valor especificado no es válido para este campo.
INVALID_ILLEGAL_OPERATION	Illegal operation performed.	La operación solicitada no es legal.
INVALID_ILLEGAL_PARENT	-	Se registra cuando una de las carpetas principales de ACL no es válida. Por ejemplo, si la carpeta A se encuentra dentro de la carpeta B, la carpeta B no puede estar en la carpeta A.
INVALID_MISSING	Field {1} of type {2} is missing.	Falta el valor necesario para este campo.

Entrada de registro para el campo x-status	Entrada de registro para el campo x-comment	Descripción
INVALID_NO_SUCH_ITEM	Value {1} is an unknown in the system.	El elemento solicitado no existe.
INVALID_RANGE	The specified value must be between {1} and {2}.	Se registra cuando el valor introducido no está en el rango admitido.
INVALID_TELEPHONY_FIELD	Telephony authentication values were not validated by the service provider.	El proveedor de servicios no pudo validar la cuenta de telefonía.
INVALID_VALUE_GTE	The specified value must be greater than or equal to {1}.	Se registra cuando el valor introducido no está en el rango admitido.
INVALID_VALUE_LTE	The specified value must be less than or equal to {1}.	Se registra cuando el valor introducido no está en el rango admitido.
KILLING_LONG_CONNECTION	Client has been in the room for 12 hours, disconnecting.	Se registra cuando el cliente se desconecta al superar el límite de tiempo.
LICENSE_EXPIRED	Your license has expired and your account will be disabled on {1}. Please upload a new license file through the console manager to continue using Acrobat Connect Pro.	Se registra cuando un cliente utiliza Acrobat Connect Pro durante el período de prueba y éste está a punto de finalizar.
LICENSE_EXPIRY_WARNING	Your license will expire on {1}. Please upload a new license file through the console manager to continue using Acrobat Connect Pro.	Se registra cuando faltan 15 días o menos para caducar.
MASTER_THREAD_TIMED_OUT	Master thread has not reported progress in {1} milliseconds.	El subproceso del programador no se está ejecutando.
MEETING_BACKUP_END	Server {1} is no longer the backup for room {2}.	La copia de seguridad de la reunión ha finalizado.
MEETING_BACKUP_START	Server {1} is now the backup for room {2}.	La copia de seguridad de la reunión ha comenzado.
MEETING_FAILOVER	Meeting {1} failed over to {2}.	Se registra cuando se produce un error de una reunión en este servidor.
MEETING_TMP_READ	Meeting template {1} read for room {2}.	Se ha leído una plantilla desde una reunión.
MEETING_TMP_WRITTEN	Meeting template {1} written to room {2}.	Se ha escrito una plantilla para una reunión.
NO_ACCESS_ACCOUNT_EXPIRED	Your account has expired.	La cuenta a la que se ha accedido ha caducado.
NO_ACCESS_DENIED	Permission check failed.	Se ha producido un error de comprobación de permisos.
NO_ACCESS_LEARNER	No permission to take courses.	Debe ser miembro del grupo de alumnos para participar en el curso.
NO_ACCESS_LEARNING_PATH_BLOCKED	You have not fulfilled a prerequisite or preassessment.	Se ha producido un error relacionado con los requisitos previos o con la evaluación previa.
NO_ACCESS_NO_EXTERNAL_USER_MODIFICATION	External users cannot be modified.	El usuario no puede modificar los usuarios de LDAP.
NO_ACCESS_NO_LICENSE_FILE	Your license file has not been uploaded.	No se encuentra el archivo de licencia.
NO_ACCESS_NO_LOGIN	Not logged in.	Se produce un error cuando el usuario no ha iniciado la sesión.

Entrada de registro para el campo x-status	Entrada de registro para el campo x-comment	Descripción
NO_ACCESS_NO_QUOTA	A {1} quota error occurred for account {2} with limit {3}.	Se ha superado la cuota.
NO_ACCESS_NO_RETRY	You have reached the max limit and may not take the course again.	El usuario ha superado el límite de intentos y no puede realizar el curso de nuevo.
NO_ACCESS_NO_SERVER	Server not available.	El servidor solicitado no está disponible.
NO_ACCESS_NOT_AVAILABLE	The requested resource is unavailable.	Se registra cuando el recurso solicitado no está disponible.
NO_ACCESS_NOT_SECURE	SSL request made on a non-SSL server.	Se ha enviado una solicitud segura a un servidor que no es seguro.
NO_ACCESS_PASSWORD_EXPIRED	Your password has expired.	Se registra cuando caduca una contraseña de usuario.
NO_ACCESS_PENDING_ACTIVATION	Your account has not been activated yet.	No se ha activado la cuenta aún.
NO_ACCESS_PENDING_LICENSE	Your account activation is pending a license agreement.	La cuenta no se puede utilizar hasta que se lea el acuerdo de licencia.
NO_ACCESS_SCO_EXPIRED	The course you tried to access is no longer available.	Se ha superado la fecha de finalización del curso.
NO_ACCESS_SCO_NOT_STARTED	Course is not open yet.	Aún no se ha alcanzado la fecha de inicio del curso.
NO_ACCESS_WRONG_ZONE	Content accessed from wrong zone.	Se muestra cuando un contenido o un usuario acceden al servidor desde la zona equivocada.
NO_DATA	Permission check failed.	La consulta no ha devuelto datos.
NO_DISKSPACE	Health check failed due to lack of disk space.	Se registra cuando la cuenta agota el espacio disponible en el disco.
NOT_AVAILABLE	The requested resource is unavailable.	Si el recurso no está disponible, se produce un error.
OK	-	La solicitud se ha procesado correctamente.
OPERATION_SIZE_ERROR	Operation too large to complete.	Se registra cuando no se puede finalizar la operación debido a que es demasiado grande.
REQUEST_RETRY	Unable to process request. Please try again.	La solicitud ha fallado.
RESPONSE_ABORTED	Client that made request is not available to receive response.	Se registra cuando el usuario cierra el explorador antes de que el servidor puedan devolver una respuesta.
RTMP_SVC_BLOCKED	Acrobat Connect Pro service request blocked from {1} because the server has not fully started up yet.	Se ha solicitado una conexión de servicio desde SCO, pero el servidor se está iniciando aún.
RTMP_SVC_CLOSED	Acrobat Connect Pro service connection closed for {1}.	Se ha cerrado la conexión de servicio para SCO.
RTMP_SVC_REQUEST	Acrobat Connect Pro service request received from {1}.	Se ha solicitado una conexión de servicio desde SCO.

Entrada de registro para el campo x-status	Entrada de registro para el campo x-comment	Descripción
RTMP_SVC_START	Acrobat Connect Pro service connection established with {1}.	Se ha establecido una conexión de servicio con SCO.
SCRIPT_ERROR	Run-Time Script Error. Details: {1}	Se registra cuando se detecta un error de secuencia de comandos.
SERVER_EXPIRED	Health check failed due to server expiry (expiry date={1}, current time={2}).	Se registra cuando el servidor no termina de ejecutar la comprobación de condición debido a que agota el tiempo de espera.
SOME_ERRORS_TERMINATED	Some actions terminated with an error.	Se registra cuando se produce un error que hace que ciertas acciones finalicen inesperadamente.
START_UP_ERROR	Start up error: {1}.	Se registra cuando se emite una excepción durante el inicio.
START_UP_ERROR_UNKNOWN	Unable to start up server. Acrobat Connect Pro might already be running.	Se registra cuando se produce un error desconocido durante el inicio. JRUN imprime el error.
TEL_CONNECTION_BROKEN	Telephony connection {1} was unexpectedly broken.	Se registra cuando se interrumpe la conexión telefónica.
TEL_CONNECTION_RECOVERY	Telephony connection {1} was reattached to conference {2}.	Se registra cuando Acrobat Connect recupera la conexión a la conferencia.
TEL_DOWNLOAD_FAILED	Unable to download {1} for archive {2}.	Se registra cuando se agota el tiempo de espera durante la descarga de archivos de audio de telefonía.
TOO_MUCH_DATA	Multiple rows unexpectedly returned.	Se registra cuando una operación devuelve más datos de los esperados.
UNKNOWN_TYPE	{1}	Se registra cuando se desconoce el tipo de variable.

Nota: en la tabla anterior, {1} y {2} son variables que se sustituirán por valores en la entrada de registro.

Entradas del campo gravedad

El campo x-severity indica la gravedad de la condición, lo que ayuda a determinar el nivel de respuesta adecuado.

Entrada de registro para x-severity	Significado	Acción sugerida	Ejemplo
C	Muy grave	Configure herramientas de supervisión de otros fabricantes que envíen mensajes de aviso a buscas cuando se emita una entrada de registro con este grado de gravedad.	No se puede establecer comunicación con la base de datos. No se puede iniciar o finalizar un proceso. Se ha producido un fallo que afecta al sistema.
E	Error	Configure herramientas de supervisión de otros fabricantes para que envíen mensajes de correo electrónico cuando se emita una entrada de registro con este grado de gravedad.	No se puede establecer comunicación con Adobe® Premiere®. La conversión ha fallado. Se ha producido un error que afecta a un usuario o a una cuenta, pero no al sistema completo.
W	Advertencia	Genere periódicamente informes y consúltelos para identificar posibles mejoras de funcionamiento y productos.	Se ha superado el espacio permitido en el disco o la memoria.
I	Información	Revise las entradas de registro por motivos de auditoría o RCA.	El servidor se ha iniciado, detenido o reiniciado.

Entradas del campo categoría

El campo x-category determina si el evento se refiere a problemas de acceso (A) o problemas generales del sistema (S). Las entradas de la categoría A aparecen en el archivo access.log y las de la categoría S aparecen en el archivo error.log.

Entrada de registro para el campo x-category	Significado	Descripción
A	acceso	Código de estado relacionado con problemas de acceso. Se registra en el archivo access.log.
S	sistema	Código de estado relacionado con problemas generales del sistema. Se registra en el archivo error.log.

Mantenimiento del espacio en disco

Acerca del mantenimiento del espacio en disco

El sistema Acrobat Connect Pro debe tener un mínimo de 1 GB de espacio libre. Acrobat Connect Pro no tiene ninguna herramienta integrada que controle el espacio de disco; el administrador debe controlarlo con las utilidades del sistema operativo o herramientas de terceros.

El contenido puede guardarse en el servidor con Acrobat Connect Pro, en los volúmenes de almacenamiento externo o en ambos.

Más temas de ayuda

“[Configuración de almacenamiento compartido](#)” en la página 46

Mantenimiento del espacio de disco en los servidores de Acrobat Connect Pro

❖ Realice una de las acciones siguientes:

- Utilice Connect Pro Central para eliminar el contenido que no se utilice. Consulte Nombre del administrador [Eliminación de un archivo o carpeta](#).
- Reemplace su disco de servidor por otro mayor.

Nota: Si el espacio libre en disco es inferior a 1 GB, el servidor se detendrá.

Mantenimiento del espacio de disco en los dispositivos de almacenamiento compartido

❖ Controle el espacio libre y los nodos de sistema de archivo disponibles en el dispositivo principal de almacenamiento compartido. Si son inferiores a 10%, agregue más almacenamiento al dispositivo o agregue otro dispositivo de almacenamiento compartido.

Nota: 10% es el valor recomendado. Asimismo, si utiliza almacenamiento compartido, defina un valor de tamaño de caché máximo en la consola de gestión de la aplicación o la caché llenará el disco.

Borrado de la caché de Edge Server

Adobe recomienda crear una tarea programada semanalmente para borrar la memoria caché del edge server. Resulta adecuado ejecutar la tarea en un momento de utilización mínima de los sistemas, como el domingo por la mañana.

1 Cree un archivo cache.bat para eliminar el directorio de la memoria caché. La entrada de este archivo debe utilizar la sintaxis siguiente:

```
del /Q /S [cache directory]\*.*
```

El directorio predeterminado para la memoria caché es C:\breeze\edgeserver\win32\cache\http. Para eliminar la memoria caché, utilice el comando siguiente:

```
del /Q /S c:\breeze\edgeserver\win32\cache\http\*.*
```

2 Seleccione Inicio > Programas > Adobe Connect Pro Edge Server 7 > Detener Connect Pro Edge Server.

3 Ejecute el archivo cache.bat y compruebe que se eliminan los archivos del directorio de la memoria caché.

Nota: La estructura del directorio no se verá alterada y los archivos que el edge server bloquee no se eliminarán.

4 Seleccione Inicio > Programas > Adobe Connect Pro Edge Server 7 > Iniciar Connect Pro Edge Server.

5 Seleccione Inicio > Panel de control > Tareas programadas > Agregar tarea programada.

6 Seleccione cache.bat como nuevo archivo que debe ejecutarse.

7 Repita el procedimiento para cada edge server.

Copia de seguridad de datos

Acerca de la copia de seguridad de datos

Hay tres tipos de información de los cuales debe realizar copias de seguridad a intervalos regulares: contenido (cualquier archivo almacenado en las bibliotecas), ajustes de configuración e información de la base de datos.

Si no utiliza dispositivos de almacenamiento compartido, todo el contenido de las bibliotecas se almacena en la carpeta *RootInstallationFolder\content* (de forma predeterminada, C:\breeze\content). Los ajustes de configuración se almacenan en el archivo *custom.ini* en la carpeta de instalación raíz (de forma predeterminada, C:\breeze).

La copia de seguridad de la base de datos crea un duplicado de la información de la base de datos. Las copias de seguridad programadas le permiten recuperarse de varios fallos, como fallos de medios, errores de usuario y la pérdida permanente de un servidor. Realice una copia de seguridad de la base de datos a diario.

También puede utilizar las copias de seguridad para copiar una base de datos de un servidor a otro. Puede recrear toda la base de datos a partir de una copia de seguridad en un paso si restaura la base de datos. El proceso de restauración sobrescribe la base de datos existente o crea la base de datos si no existe. El estado de la base de datos restaurada será el de la base de datos cuando se realizó la copia de seguridad menos las transacciones que no se guardaron.

Las copias de seguridad se crean en dispositivos de copia seguridad, como un disco o medio de cinta. Puede utilizar una utilidad de SQL Server para configurar sus copias de seguridad. Por ejemplo, puede sobrescribir copias de seguridad antiguas o puede adjuntar copias de seguridad nuevas al medio de copia de seguridad.

Al realizar la copia de seguridad de la base de datos, siga las prácticas recomendadas:

- Programe una copia de seguridad para cada noche.
- Mantenga las copias de seguridad en un lugar seguro, preferiblemente en un sitio diferente de donde residen los datos.
- Guarde las copias de seguridad anteriores por un periodo designado por si la copia más reciente resulta dañada, destruida o perdida.
- Establezca un sistema de sobrescritura de copias de seguridad y reutilice las copias de seguridad más antiguas primero. Utilice fechas de caducidad en las copias de seguridad para evitar la sobrescritura prematura.
- Etiquete los soportes de copia de seguridad para identificar los datos y no sobrescribir las copias importantes.

Utilice las utilidades de SQL Server para realizar una copia de seguridad de la base de datos:

- Transact-SQL
- SQL Distributed Management Objects
- Asistente de creación de una copia de seguridad de base de datos
- SQL Server Management Studio

Copias de seguridad de los archivos del servidor

Realice copias de seguridad de la información del sistema y protéjala como protegería los recursos valiosos de su organización.

Es recomendable que realice este procedimiento cada noche.

1 Para detener Acrobat Connect Pro, haga lo siguiente:

- a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Central Service.
- b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Detener Connect Pro Meeting Service.

2 Realice una copia de seguridad del directorio de contenido.

La ubicación predeterminada es c:\breeze.

3 Realice una copia de seguridad del archivo *custom.ini*.

La ubicación predeterminada es c:\breeze\.

- 4 Para iniciar Acrobat Connect Pro, haga lo siguiente:
 - a Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Meeting Service.
 - b Seleccione Inicio > Programas > Adobe Acrobat Connect Pro Server 7 > Iniciar Connect Pro Central Service.

Realice una copia de seguridad de la base de datos

Para hacer una copia de seguridad de cualquier edición de Microsoft SQL Server, puede utilizar Microsoft SQL Server Management Studio o la ventana del símbolo del sistema.

La edición de SQL Server que se instala con Connect Pro Server no incluye SQL Server Management Studio. Sin embargo, puede descargar [Microsoft SQL Server Management Studio Express](#) desde la web de Microsoft.

Uso de SQL Server Management Studio para realizar una copia de seguridad de SQL Server

Importante: No desinstale la base de datos.

- 1 En Windows, seleccione Inicio > Programas > Microsoft SQL Server 2005 > SQL Server Management Studio.
- 2 En el panel del árbol de la ventana Explorador de objetos, haga clic con el botón secundario en la base de datos (llamada "breeze" de forma predeterminada) y elija Tareas > Realizar una copia de seguridad...

Nota: Para obtener instrucciones completas sobre la copia de seguridad y recuperación de la base de datos de SQL, consulte el sitio Web de asistencia técnica de Microsoft.

Uso de la ventana del símbolo del sistema para realizar una copia de seguridad de SQL Server

Para acceder a la información de ayuda para comandos de la base de datos, escriba `osql ?` en la línea de comandos de DOS y pulse Intro.

Importante: No desinstale la base de datos.

- 1 Inicie una sesión en el servidor que tenga instalado Connect Pro Server.
- 2 Cree una carpeta para almacenar los archivos de copia de seguridad de la base de datos.

Este ejemplo utiliza la carpeta `c:\Connect_Database`.

- 3 Seleccione Inicio > Ejecutar, introduzca **cmd** en el cuadro Abrir y haga clic en Aceptar.
- 4 En la línea de comandos, vaya al directorio en el que instaló la base de datos. De forma predeterminada, el directorio es `c:\Program Files\Microsoft SQL Server\90\Tools\Binn`.
- 5 En la línea de comandos, introduzca **osql -E** para iniciar sesión en el motor de procesamiento de la base de datos y pulse Intro.
- 6 Introduzca **BACKUP DATABASE database-name TO DISK = 'C:\Connect_Database\database-name.bak'** para ejecutar una utilidad de Microsoft SQL que realiza una copia de seguridad de la base de datos de Connect y pulse Intro.

El nombre predeterminado de la base de datos es *breeze*.

- 7 En la línea de comandos, introduzca **go** y pulse Intro.

La ventana de comandos muestra mensajes acerca de la copia de seguridad.

- 8 En la línea de comandos, escriba **quit** y pulse Intro.
- 9 Para verificar que la copia de seguridad se realizó correctamente, confirme que exista el archivo `breeze.bak` en el directorio `c:\Connect_Database`.

10 Para reiniciar la base de datos, desde el escritorio de Windows, seleccione Inicio > Panel de control > Herramientas administrativas > Servicios. En la ventana Servicios, haga clic con el botón secundario del mouse en SQL Server (MSSQLSERVER) y seleccione Inicio desde el menú contextual.

Creación de informes personalizados

Creación de informes personalizados mediante las vistas de esquema de estrella

Acrobat Connect Pro utiliza una base de datos para almacenar información sobre usuarios, contenido, cursos y reuniones. La base de datos se rellena con datos procedentes de la actividad de los usuarios. Se pueden utilizar herramientas como Adobe® ColdFusion® Studio y Business Objects Crystal Reports para consultar las vistas de esquema de estrella y visualizar los datos. También se pueden utilizar herramientas basadas en SQL, como SQL Query Analyzer.

Las siguientes aplicaciones de Acrobat Connect Pro pueden enviar datos a informes:

Acrobat Connect Pro Meeting Asistencia, duración y contenido de la reunión.

Adobe Presenter Vistas del contenido, de las diapositivas y de la presentación.

Acrobat Connect Pro Training Información sobre la gestión del curso, como estadísticas de asistencia, de visualización del contenido y resultados de los cuestionarios.

Nota: Además, los informes se pueden ejecutar desde la aplicación Web de Connect Pro Central para, a continuación, visualizarlos o descargarlos en formato CSV. Para obtener más información, consulte [Generación de informes en Connect Pro Central](#).

Hecho SCO

Columna	Descripción
dim_sco_details_sco_id	Id. de SCO
dim_sco_details_sco_version	Versión de SCO
max_retries	Número máximo de intentos
owner_user_id	Id. de usuario del propietario de SCO
disk_usage_kb	Uso del disco en kilobytes
passing_score	Puntuación para aprobar
max_possible_score	Máxima puntuación posible
views	Número de vistas
unique_viewers	Número de usuarios que han visualizado el SCO
slides	Número de diapositivas
questions	Número de preguntas
max_score	Puntuación máxima
min_score	Puntuación mínima
average_score	Puntuación media

Columna	Descripción
average_passing_score	Puntuación media para aprobar
total_registered	Puntuación media para suspender
total_participants	Número total de participantes registrados
account_id	Número total de participantes

Detalles de SCO

Columna	Descripción
sco_id	Id. de SCO
sco_version	Versión de SCO
sco_name	Nombre
sco_description	Descripción
sco_type	Tipo de SCO
sco_int_type	Tipo de número entero
is_content	¿Es el SCO un SCO de contenido?
url	URL
parent_name	Nombre del SCO principal
parent_sco_id	Id. de SCO del SCO principal
parent_type	Tipo de SCO principal
date_sco_created	Fecha de creación
date_sco_modified	Fecha de modificación
sco_start_date	Fecha de inicio
sco_end_date	Fecha de finalización
version_start_date	Fecha de inicio de la versión
version_end_date	Fecha de finalización de la versión
sco_tag_id	Id. de la etiqueta
passing_score	Puntuación para aprobar
max_possible_score	Máxima puntuación posible
linked_sco_id	Id. de un SCO vinculado
linked_type	Tipo de SCO vinculado
owner_user_id	Id. de usuario del propietario
storage_bytes_kb	Bytes de almacenamiento en kilobytes
account_id	Id. de la cuenta

Hecho de actividad

Columna	Descripción
dim_activity_details_activity_id	Id. de la actividad
score	Puntuación
passed	Aprobado
completed	Completado
peak_session_users	Usuarios de la sesión en horas punta
number_correct	Número correcto
number_incorrect	Número incorrecto
number_of_questions	Número de preguntas
number_of_responses	Número de respuestas
account_id	Id. de la cuenta

Detalles de la actividad

Columna	Descripción
activity_id	Id. de la actividad
dim_sco_details_sco_id	Id. de SCO
dim_sco_details_sco_version	Versión de SCO
dim_users_user_id	Id. de usuario
dim_sco_details_parent_sco_id	Id. de SCO principal
puntuación	Puntuación
passed	Aprobado
completed	Completado
activity_type	Tipo de actividad
role	Función
date_activity_started	Fecha de inicio
date_activity_finished	Fecha de finalización
dim_cost_center_id	Id. de centro de costes
cost_center_audit_id	Id. de auditoría
session_start_date	Fecha de inicio de la sesión
session_end_date	Fecha de finalización de la sesión
attendance_activity	Actividad de la asistencia
session_id	Id. de la sesión
account_id	Id. de la cuenta

Pruebas de clasificación para el programa

Columna	Descripción
dim_sco_details_curriculum_sco_id	Id. del programa
dim_sco_details_curriculum_sco_version	Versión del programa
test_out_subject_sco_id	Id. de SCO del tema
test_out_target_sco_id	Id. de SCO objetivo
test_out_type	Tipo de prueba de clasificación
account_id	Id. de la cuenta

Requisitos previos del programa

Columna	Descripción
dim_sco_details_curriculum_sco_id	Id. del programa
dim_sco_details_curriculum_sco_version	Versión del programa
pre_requisite_subject_sco_id	Id. de SCO del tema
pre_requisite_target_sco_id	Id. de SCO objetivo
pre_requisite_type	Tipo de requisito previo
account_id	Id. de la cuenta

Requisitos de la finalización del programa

Columna	Descripción
dim_sco_details_curriculum_sco_id	Id. del programa
dim_sco_details_curriculum_sco_version	Versión del programa
completion_subject_sco_id	Id. de SCO del tema
completion_target_sco_id	Id. de SCO objetivo
completion_requirement_type	Tipo de requisito de finalización
account_id	Id. de la cuenta

Hecho de vistas de diapositivas

Columna	Descripción
dim_slide_view_details_slide_view_id	Id. de vista de diapositivas
dim_activity_details_activity_id	Id. de la actividad
slide_view_display_sequence	Secuencia de visualización
account_id	Id. de la cuenta

Detalles de las vistas de diapositivas

Columna	Descripción
slide_view_id	Id. de vista de diapositivas
date_slide_viewed	Fecha de visualización de la diapositiva
slide_name	Nombre de la diapositiva
slide_description	Descripción de la diapositiva
account_id	Id. de la cuenta

Hecho de respuestas

Columna	Descripción
dim_answer_details_answer_id	Id. de la respuesta
dim_activity_details_activity_id	Id. de la actividad
dim_question_details_question_id	Id. de la pregunta
answer_display_sequence	Secuencia de visualización
answer_score	¿Puntuación?
answer_correct	¿Es correcta?
account_id	Id. de la cuenta

Detalles de las respuestas

Columna	Descripción
answer_id	Id. de la respuesta
date_answered	Fecha de la respuesta
response	Respuesta
account_id	Id. de la cuenta

Hecho de preguntas

Columna	Descripción
dim_sco_details_sco_id	Id. de SCO
dim_sco_details_sco_version	Versión de SCO
dim_question_details_question_id	Id. de la pregunta
number_correct	Número de respuestas correctas
number_incorrect	Número de respuestas incorrectas
total_responses	Número total de respuestas
high_score	Mayor puntuación
low_score	Baja puntuación
average_score	Puntuación media

Columna	Descripción
account_id	Id. de la cuenta

Detalles de preguntas

Columna	Descripción
question_id	Id. de la pregunta
question_display_sequence	Secuencia de visualización
question_description	Descripción
question_type	Tipo de pregunta
account_id	Id. de la cuenta

Respuestas a preguntas

Columna	Descripción
dim_question_details_question_id	Id. de la pregunta
response_display_sequence	Secuencia de visualización de respuestas
response_value	Valor
response_description	Descripción
account_id	Id. de la cuenta

Grupos

Columna	Descripción
group_id	Id. del grupo
group_name	Nombre del grupo
group_description	Descripción del grupo
group_type	Tipo de grupo
account_id	Id. de la cuenta

Grupos de usuarios

Columna	Descripción
user_id	Id. de usuario
group_id	Id. del grupo
group_name	Nombre del grupo
account_id	Id. de la cuenta

Usuarios

Columna	Descripción
user_id	Id. de usuario
inicio de sesión	Iniciar sesión
first_name	Nombre
last_name	Apellido
email	Dirección de correo electrónico
user_description	Descripción del usuario
user_type	Tipo de usuario
most_recent_session	Fecha de la sesión más reciente
session_status	Estado de la sesión
manager_name	Nombre del administrador
disabled	Desactivado
account_id	Id. de la cuenta
custom_field_1	Valor del campo personalizado 1
custom_field_2	Valor del campo personalizado 2
custom_field_3	Valor del campo personalizado 3
custom_field_4	Valor del campo personalizado 4
custom_field_5	Valor del campo personalizado 5
custom_field_6	Valor del campo personalizado 6
custom_field_7	Valor del campo personalizado 7
custom_field_8	Valor del campo personalizado 8
custom_field_9	Valor del campo personalizado 9
custom_field_10	Valor del campo personalizado 10

Nombres de campos personalizados

Columna	Descripción
dim_column_name	Nombre de la columna del campo personalizado
custom_field_name	Nombre del campo personalizado
account_id	Id. de la cuenta

Centros de costes

Columna	Descripción
cost_center_id	Id. de centro de costes
cost_center_name	Nombre del centro de costes
cost_center_description	Descripción del centro de costes

Columna	Tipo de datos	Descripción
TRANSACTION_ID	INT	Id. exclusivo de esta transacción.
LOGIN	NVARCHAR	Nombre del usuario que ha llevado a cabo la transacción.
URL	NVARCHAR	Objeto con el que el usuario ha interactuado.
STATUS	NVARCHAR	Puede ser aprobado, suspendido, completado o en ejecución.
SCORE	FLOAT	Puntuación del usuario.
DATE_VISITED	DATETIME	Fecha en la que se llevó a cabo o visualizó la transacción.

Consulta y datos de muestra La siguiente consulta devuelve los datos de la tabla que le sigue:

```
select * from ext_transactions where url = '/p63725398/' order by login, date_visited asc;
```

TRANSACTION_ID	LOGIN	URL	STATUS	SCORE	DATE_VISITED
10687	prueba1- lnagaraj@prueba.enang.com	/p63725398/	En ejecución	0.0	2006-12-15 00:56:16.500
10688	prueba1- lnagaraj@prueba.enang.com	/p63725398/	En ejecución	0.0	2006-12-15 00:56:16.500
10693	prueba1- lnagaraj@prueba.enang.com	/p63725398/	En ejecución	0.0	2006-12-15 00:58:23.920
10714	prueba1- lnagaraj@prueba.enang.com	/p63725398/	En ejecución	10.0	2006-12-15 01:09:20.810
10698	prueba2- lnagaraj@prueba.enang.com	/p63725398/	En ejecución	10.0	2006-12-15 01:00:49.483
10723	prueba3- lnagaraj@prueba.enang.com	/p63725398/	En ejecución	10.0	2006-12-15 01:11:32.153
10729	prueba3- lnagaraj@prueba.enang.com	/p63725398/	completed	20.0	2006-12-15 01:12:09.700

Notas de consulta La vista EXT_TRANSACTIONS devuelve todas las transacciones existentes de un usuario y una sesión de formación. Para visualizar la última transacción, compruebe el valor máximo de DATE_VISITED.

Elija un valor en los campos STATUS y URL para obtener un listado de los usuarios que hayan aprobado una sesión de formación determinada. Por ejemplo:

```
select * from ext_transactions where url = '/p31102136/' and status = 'user-passed' order by login, date_visited asc;
```

Generación de datos Acciones de los usuarios que generan datos en esta vista:

- Asistencia a una reunión
- Visualización de un contenido
- Realización de una sesión de formación (un curso o un programa)

Datos excluidos •Número de certificado, que no existe en la base de datos

- Puntuación máxima, que a menudo no está disponible

EXT_TRANSACTIONS_VIEWS

La vista EXT_TRANSACTIONS_VIEWS recupera los datos de las diapositivas o páginas que los usuarios visualizan.

Columna	Tipo de datos	Descripción
TRANSACTION_ID	INT	Id. exclusivo de esta transacción (se puede unir a TRANSACTION_DETAILS para convertirse en una dirección URL).
PAGE	NVARCHAR	Número de diapositiva o página visualizada.
DATE_VIEWED	DATETIME	Fecha en la que se produjo la vista.

Consulta y datos de muestra La siguiente consulta devuelve los datos de la tabla que le sigue:

```
select * from ext_transaction_views where transaction_id = 10702 order by page asc;
```

TRANSACTION_ID	PAGE	DATE_VISITED
10702	0	2006-12-15 01:01:13.153
10702	1	2006-12-15 01:01:18.233
10702	2	2006-12-15 01:01:59.840
10702	3	2006-12-15 01:02:20.717

Generación de datos Los datos se generan en la vista cuando los usuarios visualizan contenido o una sesión de formación.

EXT_USERS

La vista EXT_USERS incluye a los usuarios y a los atributos de perfil asociados:

Columna	Tipo de datos	Descripción
LOGIN	NVARCHAR	Identificador exclusivo del usuario.
NAME	NVARCHAR	Nombre exclusivo del usuario.
EMAIL	NVARCHAR	Dirección de correo electrónico exclusiva.
MANAGER	NVARCHAR	Inicio de sesión del administrador. En Breeze 5.1, el administrador se define siempre en NULL.
TYPE	NVARCHAR	Usuario o invitado. En la versión 5.1, el tipo se define siempre en usuario.

Consulta y datos de muestra La siguiente consulta devuelve los datos de la tabla que le sigue:

```
select * from ext_users;
```

LOGIN	NAME	EMAIL	MANAGER	TYPE
prueba4-lnagaraj@prueba.enang.com	prueba4 laxmi	prueba4-lnagaraj@prueba.enang.com	NULL	user
prueba7-lnagaraj@prueba.enang.com	prueba7 laxmi	prueba7-lnagaraj@prueba.enang.com	NULL	user

Generación de datos Los datos de esta vista se actualizan siempre que se crea, actualiza o elimina un usuario o invitado.

Datos excluidos • Contraseña, que no se guarda en texto sin formato.

- Zona horaria e idioma, no disponibles en formato para lectura por parte del usuario. Por ejemplo, PST es 323.
- Último inicio de sesión, que utiliza demasiados recursos como para calcularse correctamente. En su lugar, utilice la consulta `max(date_visited)` desde la vista EXT_TRANSACTIONS para recuperar los datos.

- Sesión activa, que consiste en datos de la vista EXT_TRANSACTION. En su lugar, utilice la consulta `STATUS= ' IN-PROGRESS '` para recuperar los datos.
- Los usuarios eliminados no se muestran en la vista EXT_USERS. Los usuarios eliminados siguen mostrándose en la vista EXT_TRANSACTION.
- En esta vista no se incluyen datos sobre los grupos.
- Los datos de los campos personalizados nuevos o definidos previamente. Esta información está a disposición de los usuarios en la vista EXT_USER_FIELDS.

EXT_USER_FIELDS

La vista EXT_USER_FIELDS incluye los campos personalizados nuevos y predefinidos para un usuario determinado. También contiene campos personalizados de usuarios convertidos en invitados.

Columna	Tipo de datos	Descripción
LOGIN	NVARCHAR	Identificador exclusivo del usuario.
NAME	NVARCHAR	Nombre de un campo, como de números de teléfono.
VALUE	NVARCHAR	Valor del campo, como 415.555.1212.

Consulta y datos de muestra La siguiente consulta devuelve los datos de la tabla que le sigue:

```
select * from ext_user_fields where login = 'test4-lnagaraj@test.engang.com';
```

LOGIN	NAME	VALUE
prueba4-lnagaraj@prueba.engang.com	{correo electrónico}	prueba4-lnagaraj@prueba.engang.com
prueba4-lnagaraj@prueba.engang.com	{nombre}	prueba4
prueba4-lnagaraj@prueba.engang.com	{apellido}	laxmi
prueba4-lnagaraj@prueba.engang.com	{x-puesto}	ing sw 4
prueba4-lnagaraj@prueba.engang.com	{x-línea-directa}	NULL
prueba4-lnagaraj@prueba.engang.com	{x-tecla-teléfono-directa}	NULL
prueba4-lnagaraj@prueba.engang.com	SSN	777

Generación de datos Acciones que generan datos en esta vista: agregar, crear o actualizar campos nuevos o predefinidos para uno o varios usuarios.

EXT_USER_GROUPS

La vista EXT_USER_GROUPS incluye datos sobre los grupos y los miembros asociados a los grupos. La vista EXT_USER_GROUPS utiliza los datos que se indican en la siguiente tabla:

Columna	Tipo de datos	Descripción
LOGIN	NVARCHAR	Nombre del usuario.
NAME	NVARCHAR	Nombre del grupo.

Consulta y datos de muestra La siguiente consulta devuelve los datos de la tabla que le sigue:

```
select * from ext_user_groups where login = 'lnagaraj@adobe.com';
```

LOGIN	NAME
lnagaraj@adobe.com	{admins}
lnagaraj@adobe.com	{authors}
lnagaraj@adobe.com	{everyone}
lnagaraj@adobe.com	Laxmi Nagarajan

Notas de consulta En la versión 5.1 y versiones posteriores se admite el anidamiento de varios grupos. Por ejemplo, si el grupo A contiene el grupo B y usted es miembro del grupo B, también será miembro del grupo A.

Los grupos integrados, como el grupo Administradores, utilizan nombres en código en el esquema. Como en la siguiente consulta SQL: `SELECT * FROM EXT_USER_GROUPS where group='{admins}`. El nombre en código distingue entre grupos integrados y grupos definidos por usuarios.

Generación de datos Acciones de los usuarios que generan datos en esta vista:

- Creación, actualización o eliminación de un grupo
- Cambio de inscripciones a los grupos

EXT_OBJECTS

La vista EXT_OBJECTS incluye todos los objetos del sistema (como reuniones, contenido, cursos, etc.) y sus atributos.

Columna	Tipo de datos	Descripción
URL	NVARCHAR	Identificador exclusivo del objeto.
TYPE	NVARCHAR	Puede ser una presentación, curso, archivo FLV, archivo SWF, imagen, archivo, reunión, currículo, carpeta o evento.
NAME	NVARCHAR	Nombre del objeto, como aparece en la lista de contenido.
DATE_BEGIN	DATETIME	Fecha en la que está programado que el objeto comience.
DATE_END	DATETIME	Fecha en la que está programado que el objeto finalice.
DATE_MODIFIED	DATETIME	Fecha en la que se modificó el objeto.
DESCRIPTION	NVARCHAR	Información resumida sobre el objeto, que se introduce al crear una reunión, contenido u otro tipo de objeto.

Consulta y datos de muestra La siguiente consulta SQL devuelve los datos de la tabla que le sigue:

```
select * from ext_objects order by type asc;
```

URL	TYPE	NAME	DATE_BEGIN	DATE_END	DATE_MODIFIED	DESCRIPTION
/p79616987/	curso	api prueba	2006-12-08 23:30:00.000	NULL	2006-12-08 23:36:55.483	NULL
/p47273753/	programa	revisión programa prueba	2006-12-14 21:00:00.000	NULL	2006-12-14 21:00:30.060	NULL
/tz1/	reunión	{plantilla- predeterminada}	2006-12-12 19:15:00.000	2006-12-12 20:15:00.000	2006-12-12 19:25:07.750	presentación de lanzamiento
/p59795005/	presentación	In-QUIZ-TEST1	NULL	NULL	2006-12-15 00:43:19.797	reunión de administradores

Notas de consulta Para obtener todos los objetos de un determinado tipo, indique el deseado en el campo TYPE. Por ejemplo, en la siguiente consulta SQL se seleccionan los cursos y los programas:

```
select * from ext_objects where type in ('course', 'curriculum');
```

Utilice la siguiente consulta SQL para obtener una lista de tipos de sistemas disponibles:

```
select DISTINCT (type) from ext_objects;
```

Generación de datos Acciones de los usuarios que generan datos en esta vista:

- Creación o actualización de una reunión, un curso o un programa
- Carga o actualización de contenido

Datos excluidos •Duración, para la que puede utilizar `date_end - date_begin` para calcularla.

- Tamaño en disco, que indica las normas de la empresa sobre copias y originales
- Id. de la carpeta
- Los objetos eliminados no se muestran en la vista EXT_OBJECTS. Los objetos eliminados no existen en la vista EXT_TRANSACTION.