

Migrazione, installazione e configurazione di ADOBE® ACROBAT® CONNECT™ PRO SERVER 7.5

© 2009 Adobe Systems Incorporated. All rights reserved.

Migrazione, installazione e configurazione di Adobe® Acrobat® Connect™ Pro Server 7.5 per 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.

Sommario

Capitolo 1: Preparazione alla migrazione, all'installazione e alla configurazione

Novità di Acrobat Connect Pro Server 7.5	1
Requisiti per l'installazione	2
Configurazioni supportate	3
Preparazione alla migrazione	4
Preparazione all'installazione	6

Capitolo 2: Installazione di Connect Pro

Installare Connect Pro Server e Flash Media Gateway	14
Verificare l'installazione	18
Installare Acrobat Connect Pro Edge Server	20
Disinstallare i server	21

Capitolo 3: Implementazione e configurazione di Connect Pro

Implementazione di Acrobat Connect Pro Server	23
Implementazione di Acrobat Connect Pro Edge Server	27
Integrazione con un servizio di directory	29
Implementazione di Universal Voice	37
Uso di adattatori per telefonia integrata	43
Configurazione della memorizzazione condivisa	45
Configurazione delle impostazioni di notifica dell'account	48
Configurazione della conversione da PDF a SWF	50
Integrazione con Microsoft Live Communications Server 2005 e Microsoft Office Communications Server 2007	51
Configurazione di SSO (Single Sign-On)	56
Configurazione di un proxy inverso davanti a Connect Pro Server	61
Hosting di Acrobat Connect Add-In	63

Capitolo 4: Protezione

SSL (Secure Sockets Layer)	65
PKI (Public Key Infrastructure)	79
Protezione dell'infrastruttura	82
Risorse e consigli per la protezione	85

Capitolo 5: Amministrazione di Connect Pro Server

Avviare e arrestare i server	87
Gestione e monitoraggio dei registri	90
Gestione dello spazio su disco	98
Backup dei dati	99
Creazione di rapporti personalizzati	101

Capitolo 1: Preparazione alla migrazione, all'installazione e alla configurazione

Prima di progettare e installare un sistema Adobe® Acrobat® Connect™ Pro Server 7.5, esaminate i requisiti di installazione, le configurazioni supportate e le informazioni tecniche. Per la migrazione ad Acrobat Connect Pro Server 7.5, seguite le istruzioni per effettuare il backup dei file.

Novità di Acrobat Connect Pro Server 7.5

Di seguito sono illustrate le funzioni nuove o modificate di Acrobat Connect Pro 7.5:

VMWare Acrobat Connect Pro Server 7.5 consente le installazioni negli ambienti VMWare. Per ulteriori informazioni, vedere il [libro bianco](#) sulla configurazione VMWare e i [requisiti di sistema](#) di Connect Pro Server.

Universal voice La soluzione Universal voice di Acrobat Connect Pro Server 7.5 consente di trasmettere ai partecipanti un'audioconferenza live via VoIP. Inoltre l'audioconferenza live può essere registrata con Connect Pro Meeting.

Per utilizzare la soluzione Universal Voice, durante l'installazione di Acrobat Connect Pro Server 7.5 installate e configurate Adobe Flash Media Gateway, che è incorporato nel programma di installazione di Acrobat Connect Pro Server 7.5 e consente le comunicazioni tra Acrobat Connect Pro Server 7.5 e l'infrastruttura SIP. Flash Media Gateway può essere installato sullo stesso server di Acrobat Connect Pro Server 7.5 o su un altro computer. Consultate ["Implementazione di Universal Voice"](#) a pagina 37.

***Nota:** oltre a Universal Voice, Acrobat Connect Pro Server 7.5 supporta adattatori telefonici totalmente integrati con controllo avanzato delle chiamate e notevole feedback dei partecipanti. Per ulteriori informazioni, vedete ["Opzioni di audioconferenza Connect Pro"](#) a pagina 13.*

Condivisione file Adobe® PDF per condividere i file PDF nelle stanze riunioni. In una stanza riunioni, selezionate dalla libreria Contenuti di Connect Pro Central o dal computer i file PDF da condividere. Nella libreria Contenuti i file sono archiviati come PDF, ma per essere visualizzati nelle stanze riunioni, vengono convertiti in file SWF. Per ulteriori informazioni, vedete [Condividere un documento](#).

Supporto migliorato per Microsoft® PowerPoint per condividere i documenti PPTX nelle stanze riunioni con una migliore fedeltà, compresi i documenti che contengono elementi grafici SmartArt, grafici e testo. I relatori possono caricare nelle stanze riunioni documenti PPTX di migliore fedeltà sia dai sistemi operativi Windows che Mac.

Adobe Acrobat Connect Pro Add-in per IBM Lotus Notes per pianificare e gestire le riunioni Adobe Acrobat Connect Pro da Lotus Notes. Per ulteriori informazioni, vedete [Guida all'installazione e all'implementazione di Adobe Acrobat Connect Pro Add-in per IBM Lotus Notes](#) e [Utilizzo di Adobe Acrobat Connect Pro Add-in per IBM Lotus Notes](#).

Collegamenti Assistenza e Stato nel menu della Guida delle stanze riunioni potete aggiungere le voci Assistenza e Stato al menu della Guida delle stanze riunioni utilizzando i parametri di configurazione nel file custom.ini. Specificate degli URL che consentano agli utenti delle riunioni di visualizzare informazioni sulle opzioni di assistenza tecnica e sullo stato del sistema. Potete utilizzare i servizi Web di Acrobat Connect Pro per creare una pagina contenente informazioni dinamiche sullo stato del sistema. Per ulteriori informazioni, vedete ["Aggiunta dei collegamenti Assistenza e Stato al menu Guida"](#) a pagina 48.

Requisiti per l'installazione

Requisiti hardware, software e utenti

Per i requisiti di Adobe Acrobat Connect Pro Server e Adobe Acrobat Connect Pro Edge Server, consultate www.adobe.com/go/connect_sysreqs_it.

Requisiti delle porte

Nella seguente tabella vengono elencate le porte attraverso le quali gli utenti possono stabilire connessioni TCP.

Numero	Indirizzo di associazione	Accesso	Protocollo
80	*/Qualsiasi scheda	Pubblico	HTTP, RTMP
443	*/Qualsiasi scheda	Pubblico	HTTPS, RTMPS
1935	*/Qualsiasi scheda	Pubblico	RTMP

Nota: RTMP (Real-Time Messaging Protocol) è un protocollo di Adobe.

Nella tabella seguente vengono descritte le porte aperte all'interno di un cluster. Ogni server Acrobat Connect Pro all'interno di un cluster deve essere in grado di stabilire connessioni TCP a tutti gli altri server del cluster attraverso queste porte.

Nota: queste porte non devono avere un accesso pubblico, anche se non si utilizza un cluster.

Numero	Porta di origine	Indirizzo di associazione	Accesso	Protocollo
8506	Qualsiasi	*/Qualsiasi scheda	Privato	RTMP
8507	Qualsiasi	*/Qualsiasi scheda	Privato	HTTP

Ogni server Acrobat Connect Pro in un cluster deve essere in grado di stabilire una connessione TCP al server di database attraverso la seguente porta:

Numero	Porta di origine	Accesso	Protocollo
1433	Qualsiasi	Privato	TSQL

Nella seguente tabella vengono elencate le porte del server che Acrobat Connect Pro usa per comunicare internamente. Queste porte non devono essere usate su un server in cui è implementato Acrobat Connect Pro. In caso contrario Acrobat Connect Pro potrebbe non avviarsi.

Numero	Indirizzo di associazione	Accesso	Protocollo
1111	127.0.0.1	Interno	RTMP
1434	127.0.0.1 Questa porta è attiva solo quando si usa il database incorporato.	Interno	TSQL
2909	127.0.0.1	Interno	RMI
4111	*/Qualsiasi scheda	Interno	JMX
8510	127.0.0.1	Interno	HTTP

Per informazioni sulle porte di Flash Media Gateway, consultate [“Porte e protocolli Flash Media Gateway”](#) a pagina 38.

Configurazioni supportate

Configurazioni server-database supportate

Acrobat Connect Pro usa un database per memorizzare le informazioni su utenti e contenuto. Di seguito vengono elencate le configurazioni di database e di Acrobat Connect Pro supportate:

Server singolo con motore di database incorporato Installate Acrobat Connect Pro su un singolo computer e quindi installate il motore di database incorporato, incluso nel programma di installazione di Acrobat Connect Pro, sullo stesso computer. Il motore del database incorporato è Microsoft® SQL Server® 2005 Express Edition.

Nota: potete utilizzare questa configurazione solo in ambienti di testing; non è invece adatta ad ambienti di produzione.

Server singolo con database SQL Server 2005 Standard Edition Installate Acrobat Connect Pro su un computer e Microsoft SQL Server 2005 Standard Edition sullo stesso computer.

Server singolo con database SQL Server 2005 Standard Edition esterno Installate Acrobat Connect Pro su un singolo computer, quindi installate SQL Server 2005 Standard Edition su un altro computer.

Server singolo con diversi database SQL Server 2005 Standard Edition esterni Installate Acrobat Connect Pro su un singolo computer, quindi installate SQL Server 2005 Standard Edition su più computer (ossia su un cluster) esterni ad Acrobat Connect Pro. Acrobat Connect Pro supporta il mirroring e il clustering dei database SQL Server.

Più server con database SQL Server 2005 Standard Edition esterno Installate Acrobat Connect Pro su più server (ossia su un cluster), quindi installate SQL Server 2005 Standard Edition su un altro computer.

Più server con diversi database SQL Server 2005 Standard Edition esterni Installate Acrobat Connect Pro su più server (ossia su un cluster), quindi installate SQL Server 2005 Standard Edition su un altro cluster. Acrobat Connect Pro supporta il mirroring e il clustering dei database SQL Server.

Nota: Microsoft SQL Server 2005 Standard Edition non è incluso in Acrobat Connect Pro Server 7.5 e deve essere acquistato separatamente.

Altri argomenti presenti nell’Aiuto

[“Preparazione all’installazione”](#) a pagina 6

[“Installare Connect Pro Server e Flash Media Gateway”](#) a pagina 14

Implementazioni di Flash Media Gateway supportate

Implementate Flash Media Gateway per abilitare Universal Voice. Le implementazioni supportate sono le seguenti:

Computer singolo Installate Connect Pro Server, Flash Media Gateway e SQL Server sullo stesso computer.

Due computer Installate Connect Pro Server e Flash Media Gateway sullo stesso computer e SQL Server su un computer diverso.

Un cluster di computer Installate ciascun Connect Pro Server e ciascun Flash Media Gateway su un proprio computer.

Altri argomenti presenti nell’Aiuto

[“Opzioni di audioconferenza Connect Pro”](#) a pagina 13

[“Implementazione di Universal Voice”](#) a pagina 37

Server di directory LDAP supportati

Potete configurare l'autenticazione attraverso il server della directory LDAP aziendale e importare dallo stesso i dati della directory in Acrobat Connect Pro. Per un elenco delle directory LDAP supportate, visitate www.adobe.com/go/connect_sysreqs_it.

Nota: Con Acrobat Connect Pro Server 7.5 possono essere integrati tutti i server di directory LDAP v.3, ma sono supportati solo quelli testati da Adobe.

Altri argomenti presenti nell' Aiuto

“Integrazione con un servizio di directory” a pagina 29

Periferiche di memorizzazione del contenuto supportate

Potete configurare il sistema Acrobat Connect Pro per la memorizzazione del contenuto su periferiche NAS (Network Attached Storage) e SAN (Storage Area Network). Per un elenco delle periferiche NAS e SAN supportate, visitate il sito Web all'indirizzo www.adobe.com/go/connect_sysreqs_it.

Altri argomenti presenti nell' Aiuto

“Configurazione della memorizzazione condivisa” a pagina 45

Preparazione alla migrazione

Percorsi di migrazione

Eseguite il programma di installazione di Adobe Acrobat Connect Pro Server 7.5 per effettuare l'aggiornamento da Adobe Connect Server 7.x ad Acrobat Connect Pro Server 7.5; si tratta dell'unico percorso di aggiornamento possibile. Il programma di installazione di Acrobat Connect Pro Server e la console di gestione applicazione offrono un'interfaccia grafica che semplifica la procedura di aggiornamento.

Per ulteriori informazioni sull'aggiornamento, contattate il supporto Adobe:
www.adobe.com/go/connect_licensed_programs_it.

Migrazione da Acrobat Connect Pro Server 7.x ad Acrobat Connect Pro Server 7.5

Attenetevi alla procedura seguente per effettuare la migrazione da Acrobat Connect Pro Server 7.x ad Acrobat Connect Pro Server 7.5.

1. Verificare la migrazione in un ambiente non di produzione.

Prima di effettuare la migrazione dell'ambiente di produzione, è consigliabile acquisire un'istantanea dell'ambiente di produzione corrente e verificare la migrazione in un ambiente non di produzione. Dopo aver eseguito la migrazione in un ambiente di verifica, passate al punto 2.

2. Informare gli utenti della migrazione.

Vedete “Informare gli utenti della migrazione” a pagina 5.

3. (Facoltativo) Eseguire il backup dei contenuti e dei file di configurazione.

Vedete “[Eseguire il backup dei file](#)” a pagina 5.

4. Eseguire il backup del database.

Vedere “[Eseguire il backup del database](#)” a pagina 100.

5. Eseguire l'installazione di Adobe Acrobat Connect Pro Server 7.5.

Consultate “[Installare Connect Pro Server e Flash Media Gateway](#)” a pagina 14. Il programma di installazione arresta i servizi di Acrobat Connect Pro Server ed effettua il backup dei file esistenti, incluso il file custom.ini.

6. Configurare Acrobat Connect Pro Server 7.5.

Consultate “[Configurazione di Acrobat Connect Pro con la procedura guidata della console di gestione applicazione](#)” a pagina 15.

7. Verificare l'installazione.

Consultate “[Verificare l'installazione](#)” a pagina 18.

Informare gli utenti della migrazione

Come per qualsiasi aggiornamento software, soprattutto per quelli che interessano un intero gruppo di lavoro, la comunicazione e la pianificazione sono di estrema importanza. Prima di eseguire la migrazione o di aggiungere moduli all'installazione di Acrobat Connect Pro esistente, Adobe consiglia di eseguire le operazioni seguenti:

- Allocate tempo sufficiente per garantire la perfetta riuscita della migrazione. Dovreste riuscire a completare l'aggiornamento durante il normale periodo di manutenzione.
- Informate in anticipo gli utenti del fatto che non potranno usare Acrobat Connect Pro durante la migrazione.
- Comunicate agli utenti i cambiamenti introdotti con la migrazione, ad esempio nuove funzioni o prestazioni migliorate. Per un elenco delle novità, visitate http://www.adobe.com/go/learn_cnn_whatsnew_it.

Eseguire il backup dei file

Il programma di installazione crea copie di backup delle directory appserv e comserv e del file custom.ini, quindi installa le nuove versioni, mentre la directory dei contenuti non viene cancellata né sovrascritta.

Volendo, potete scegliere di creare copie di backup di tali directory e file.

Aggiornamento da SQL Server 2005 Express edition

Eseguite la seguente procedura per migrare dal database incorporato a SQL Server 2005 Standard Edition installato su un altro computer.

Nota: tale migrazione può essere effettuata anche durante la migrazione da Acrobat Connect Pro Server 7.x ad Acrobat Connect Pro Server 7.5 oppure in qualsiasi momento dopo l'installazione di Acrobat Connect Pro Server 7.5.

1. Installare SQL Server 2005 Standard Edition su un computer diverso da quello su cui è installato Connect Pro Server.

Seguite le istruzioni fornite da Microsoft per installare SQL Server.

2. Eseguire il back up di SQL Server 2005 Express Edition.

Consultate “[Eseguire il backup del database](#)” a pagina 100.

3. Copiare il file .bak dal computer di Connect Pro al computer di SQL Server.

Quando eseguite il backup di SQL Server Express Edition, viene creato un file denominato *breeze.bak*, dove *breeze* è il nome del database.

4. Ripristinare il database sul computer su cui è installato SQL Server 2005 Standard Edition.

Per ulteriori informazioni sul ripristino di SQL Server, consultate Microsoft TechNet.

5. Immettere le informazioni sul database SQL Server 2005 Standard Edition nella console di gestione applicazione sul server in cui è installato Connect Pro.

Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server > Configura Adobe Acrobat Connect Pro Server 7.

Preparazione all'installazione

Panoramica tecnica di Acrobat Connect Pro

Un'installazione Acrobat Connect Pro consiste di diversi componenti: Connect Pro Central Application Server, Adobe® Flash® Media Server, Connect Pro Presence Service, Flash Media Gateway e un database.

Connect Pro Central Application Server è basato su J2EE con componenti di Macromedia® JRun™ di Adobe.

Denominato anche *server applicazioni*, gestisce utenti, gruppi, contenuto on-demand e sessioni client. Tra i compiti del server applicazioni figurano il controllo dell'accesso, la protezione, la gestione di quote e licenze nonché funzioni di gestione e controllo quali la replica e il failover del cluster. Si occupa inoltre della transcodifica di contenuto multimediale, inclusa la conversione di materiale di Microsoft® PowerPoint e audio in Adobe® Flash®. Il server applicazioni gestisce le richieste di riunione e di trasferimento di contenuto (diapositive, pagine HTTP, file SWF e file nel contenitore Condivisione file) attraverso una connessione HTTP o HTTPS.

Flash Media Server, denominato anche *server riunioni*, viene installato con Acrobat Connect Pro per gestire i flussi audio e video in tempo reale, la sincronizzazione dei dati e la fornitura di contenuto multimediale incluse le interazioni di Acrobat Connect Pro. Tra le attività di Flash Media Server figurano la riproduzione e la registrazione di riunioni, la tempistica di audio e video e la transcodifica, ovvero la conversione e la preparazione dei dati per l'interazione e la condivisione dello schermo in tempo reale. Flash Media Server riduce inoltre la latenza e il carico del server grazie alla memorizzazione nella cache dei flussi, dei dati condivisi e delle pagine Web a cui si accede di frequente. Flash Media Server trasferisce audio, video e i dati delle riunioni attraverso il protocollo ad alte prestazioni di Adobe RTMP o RTMPS (Real-Time Messaging Protocol).

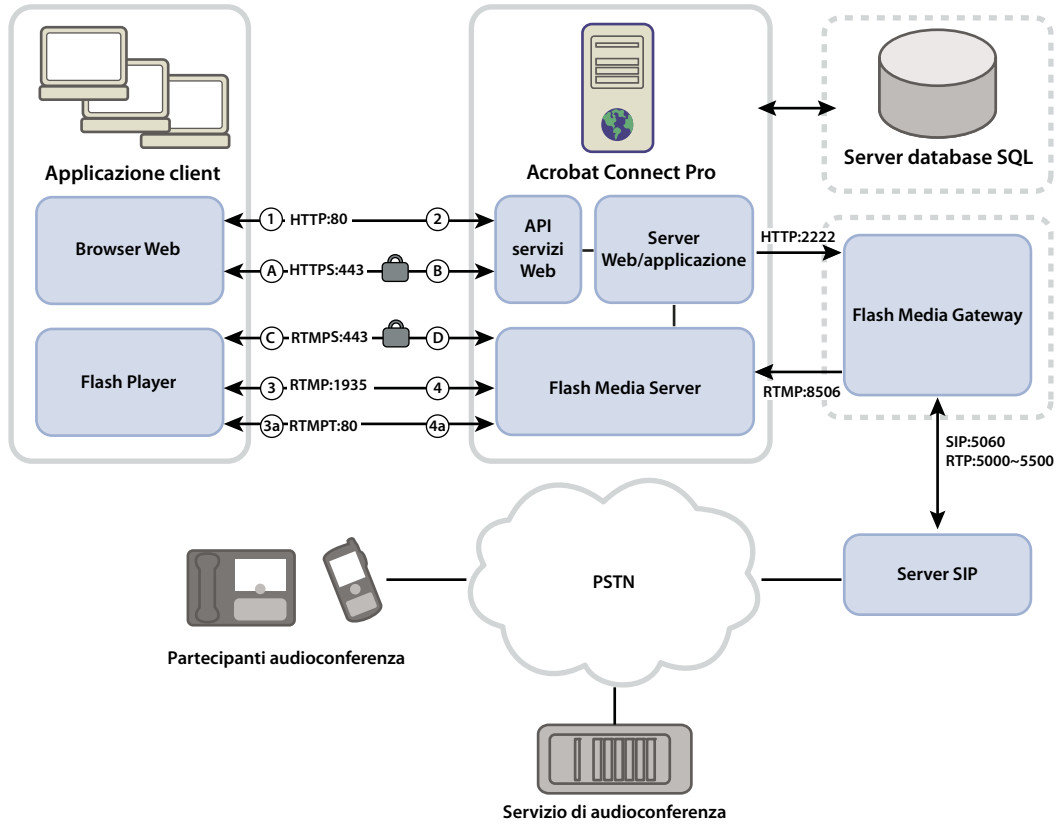
Connect Pro Presence Service integra Acrobat Connect Pro con Microsoft® Live Communication Server 2005 e Microsoft® Office Communication Server per visualizzare lo stato di presenza IM nelle stanze riunioni di Acrobat Connect Pro.

Flash Media Gateway vi consente di integrare Acrobat Connect Pro con la vostra infrastruttura SIP/RTP. Flash Media Gateway riceve l'audio da un server SIP e lo invia alle stanze riunioni di Connect Pro. Tale soluzione è denominata Universal Voice.

Acrobat Connect Pro richiede un database per la memorizzazione permanente dei metadati delle applicazioni e dei metadati transazionali, incluse le informazioni su utenti, gruppi, contenuto e di rapporto. Potete utilizzare il motore del database incorporato (SQL Server 2005 Express Edition) incluso nel programma di installazione di Acrobat Connect Pro Server 7.5 oppure acquistare e installare Microsoft SQL Server 2005 Standard Edition.

Flusso di dati

Nel diagramma seguente è illustrato il flusso di dati tra un'applicazione client e Acrobat Connect Pro.



Il flusso può passare attraverso una connessione non crittografata o una connessione crittografata.

Connessione non crittografata

Le connessioni non crittografate avvengono su HTTP ed RTMP e seguono i percorsi descritti nella tabella. I numeri riportati nella tabella corrispondono ai numeri nel diagramma del flusso di dati.

Numero	Descrizione
1	Il browser del client richiede un URL di riunione o contenuto attraverso HTTP:80.
2	Il server Web risponde e trasferisce il contenuto o fornisce al client le informazioni necessarie per la connessione alla riunione.
3	Flash Player del client richiede una connessione alla riunione attraverso RTMP:1935.
3a	Flash Player del client richiede una connessione alla riunione ma può connettersi solo attraverso RTMP:80.
4	Flash Media Server risponde e apre una connessione permanente per il traffico dei flussi di Acrobat Connect.
4a	Flash Media Server risponde e apre una connessione con tunnel per il traffico dei flussi di Acrobat Connect.

Connessione crittografata

Le connessioni crittografate avvengono attraverso HTTPS e RTMPS e seguono i percorsi descritti nella tabella. Le lettere riportate nella tabella corrispondono alle lettere nel diagramma del flusso di dati.

Lettera	Descrizione
A	Il browser del client richiede un URL di riunione o contenuto attraverso una connessione protetta su HTTPS:443.
B	Il server Web risponde e trasferisce il contenuto attraverso una connessione protetta o fornisce al client le informazioni necessarie per la connessione alla riunione in modo protetto.
C	Flash Player del client richiede una connessione protetta a Flash Media Server attraverso RTMPS:443.
D	Flash Media Server risponde e apre una connessione protetta e permanente per il traffico dei flussi di Acrobat Connect Pro.

Flusso di lavoro di installazione

La seguente procedura vi consente di progettare, installare e configurare un sistema Acrobat Connect Pro. In alcuni passaggi dovrete prendere una decisione mentre in altri dovrete semplicemente completare un'attività. In ogni passaggio si rimanda a informazioni di base sulla decisione o sull'attività.

1. Scegliere il database da usare.

Per ulteriori informazioni, consultate [“Scegliere un database”](#) a pagina 10.

2. Installare Acrobat Connect Pro su un solo server.

Per ulteriori informazioni, consultate [“Installare Connect Pro Server e Flash Media Gateway”](#) a pagina 14. Se al passaggio 1 avete scelto il motore di database incorporato, installatelo. Tale motore è incluso nel programma di installazione di Acrobat Connect Pro.

3. Se al passaggio 1 avete scelto SQL Server 2005 Standard Edition, installatelo.

Per ulteriori informazioni, consultate la documentazione di SQL Server.

4. Implementare Acrobat Connect Pro.

Per ulteriori informazioni, consultate [“Implementazione di Acrobat Connect Pro Server”](#) a pagina 23.

5. Verificare la corretta installazione di Acrobat Connect Pro.

Per ulteriori informazioni, consultate [“Verificare l'installazione”](#) a pagina 18.

6. (Facoltativo) Integrare Acrobat Connect Pro nell'infrastruttura.

Ci sono diverse opzioni per integrare Acrobat Connect Pro nell'infrastruttura esistente dell'organizzazione. È consigliabile verificare il funzionamento di Acrobat Connect Pro dopo la configurazione di ciascuna delle seguenti funzioni.

Integrazione con un fornitore SIP Potete integrare Acrobat Connect Pro con il fornitore SIP della vostra azienda (denominato anche *fornitore VOIP*) per ottenere audioconferenze senza problemi di compatibilità. Consultate [“Implementazione di Universal Voice”](#) a pagina 37.

Integrazione con una directory LDAP Per non dover gestire diverse directory utenti, integrate Acrobat Connect Pro con il server di directory LDAP dell'organizzazione. Consultate [“Integrazione con un servizio di directory”](#) a pagina 29.

Configurare SSL (Secure Socket Layer) Potete assicurarvi che la comunicazione con Acrobat Connect Pro avvenga in modo protetto. Vedete [“SSL \(Secure Sockets Layer\)”](#) a pagina 65.

Memorizzare il contenuto su periferiche NAS/SAN Usate periferiche di rete per condividere i compiti di memorizzazione del contenuto. Consultate [“Configurazione della memorizzazione condivisa”](#) a pagina 45.

Integrazione con Live Communication Server e Office Communication Server Effettuate l'integrazione con un server di comunicazione per consentire agli ospitanti di riunioni di vedere lo stato IM degli invitati nelle stanze riunioni. Gli ospitanti di riunioni possono inoltre inviare messaggi agli utenti dei servizi di messaggistica immediata direttamente dalla stanza riunioni. Consultate [“Integrazione con Microsoft Live Communications Server 2005 e Microsoft Office Communications Server 2007”](#) a pagina 51.

Configurare un'infrastruttura a chiave pubblica (PKI) Se avete integrato Acrobat Connect Pro con un server di directory LDAP, potete aggiungere un livello di protezione richiedendo certificati client. Consultate [“PKI \(Public Key Infrastructure\)”](#) a pagina 79.

Hosting di Acrobat Connect Add-In Gli utenti possono scaricare facilmente Acrobat Connect Add-in dai server Adobe. Tuttavia, se la politica di protezione dell'organizzazione non consente il download da server esterni, potete ospitare il componente aggiuntivo sui server interni per facilitarne il download. Consultate [“Hosting di Acrobat Connect Add-In”](#) a pagina 63.

7. (Facoltativo) Scegliere se installare Acrobat Connect Pro Server 7.5 Server in un cluster.

Per ulteriori informazioni, consultate [“Scelta dell'implementazione di Acrobat Connect Pro in un cluster”](#) a pagina 9 e [“Implementare un cluster di server Acrobat Connect Pro”](#) a pagina 23.

8. (Facoltativo) Scegliere se installare server periferici.

Per ulteriori informazioni, consultate [“Scelta dell'implementazione di Acrobat Connect Pro Edge Server”](#) a pagina 11 e [“Implementare Acrobat Connect Pro Edge Server”](#) a pagina 27.

Scelta dell'implementazione di Acrobat Connect Pro in un cluster

È possibile installare tutti i componenti di Acrobat Connect Pro Server, incluso il database, su un solo server, ma questo tipo di configurazione è indicato solo per ambienti di verifica e non di produzione.

Un gruppo di server connessi, ognuno con una funzione identica, è in genere denominato *cluster*. In un cluster di Acrobat Connect Pro Server, installate una copia identica di Acrobat Connect Pro Server su ogni server del cluster.

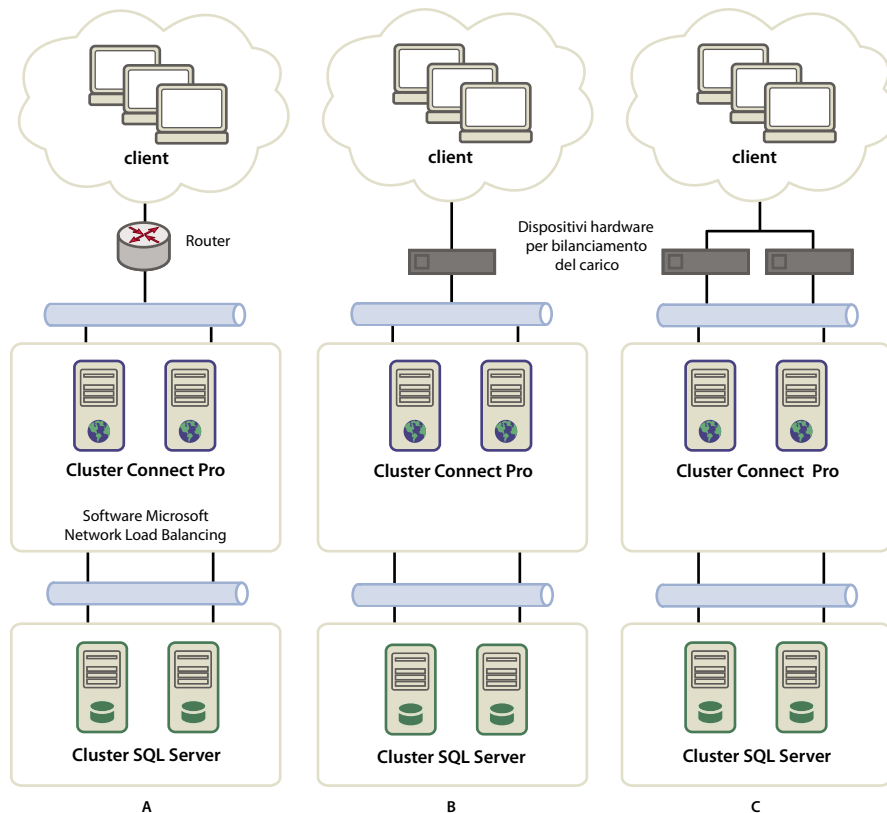
Nota: quando installate Acrobat Connect Pro Server in un cluster, dovete usare SQL Server 2005 Standard Edition e installarlo in un computer a parte.

Se un host del cluster è guasto, un altro host prende il suo posto e ospita la stessa riunione. È necessario usare hardware o software di terze parti per garantire il bilanciamento del carico del cluster. Spesso, l'hardware di bilanciamento del carico può anche fungere da acceleratore SSL.

Nota: nella console di gestione applicazione potete configurare la memorizzazione condivisa in modo che il contenuto venga memorizzato su periferiche esterne e nella cache di Acrobat Connect Pro Server.

I sistemi in rete affidabili sono progettati con componenti ridondanti. Se un componente è guasto, un altro componente identico (*ridondante*) prende il suo posto. Quando un componente prende il posto di un componente guasto, si verifica il *failover*.

Sarebbe consigliabile che ogni componente del sistema sia ridondante e non solo Acrobat Connect Pro Server. Potete ad esempio usare più periferiche hardware per il bilanciamento del carico (come BIG-IP di F5 Networks), un cluster di server in cui è installato Acrobat Connect Pro Server e database SQL Server su più computer esterni. Assicuratevi che il sistema che create sia dotato di numerosi componenti ridondanti e aggiungetene di nuovi quando necessario.



Tre opzioni di cluster

A. Un cluster con software per il bilanciamento del carico di rete e due database esterni B. Periferiche hardware per il bilanciamento del carico BIG-IP e due database esterni C. Due periferiche per il bilanciamento del carico BIG-IP, cluster e due database esterni

Altri argomenti presenti nell' Aiuto

["Implementare un cluster di server Acrobat Connect Pro"](#) a pagina 23

["Configurazione della memorizzazione condivisa"](#) a pagina 45

Scegliere un database

Acrobat Connect Pro Server usa un database per memorizzare informazioni su utenti, contenuto, corsi, riunioni e rapporti. Potete usare il motore di database incorporato (incluso nel programma di installazione), oppure installare Microsoft SQL Server 2005 Standard Edition (da acquistare separatamente).

Nota: il motore database incorporato è Microsoft SQL Server 2005 Express Edition.

Database incorporato

Il motore database incorporato è consigliato solo per uso a scopo di testing e sviluppo. Il motore usa le stesse strutture dati di SQL Server 2005 Standard Edition, ma non è altrettanto affidabile.

Il motore database incorporato presenta i seguenti limiti:

- A causa di restrizioni della licenza, il motore deve essere installato sullo stesso computer in cui è installato Acrobat Connect Pro Server. Tale computer deve essere dotato di un solo processore.
- Le dimensioni massime del database sono pari a 2 GB.

- Il motore di database incorporato non dispone di un'interfaccia utente grafica, bensì di un'interfaccia basata su riga di comando.

Microsoft SQL Server 2005 Standard Edition

In ambienti di produzione è consigliabile usare il motore database Microsoft SQL Server 2005 Standard Edition, un sistema di gestione di database (DBMS) scalabile progettato per il supporto di un numero elevato di utenti simultanei. SQL Server 2005 Standard Edition offre inoltre un'interfaccia utente grafica per la gestione del database e la creazione di query.

Potete installare SQL Server 2005 Standard Edition sullo stesso computer in cui è installato Acrobat Connect Pro Server o su un computer diverso. Se lo installate su un computer diverso, sincronizzate i computer sulla stessa origine ora. Per ulteriori informazioni, consultate il seguente articolo TechNote: www.adobe.com/go/2e86ea67.

Installate SQL Server in modalità di login mista per poter usare l'autenticazione SQL. Impostate il database in modo che non faccia distinzione tra maiuscole e minuscole.

È necessario usare SQL Server nei seguenti scenari di implementazione:

- Installazione del database su un computer in cui non è installato Acrobat Connect Pro Server.
- Acrobat Connect Pro Server è implementato in un cluster.
- Acrobat Connect Pro Server è installato su computer multiprocessore con tecnologia Hyper-Threading.

Altri argomenti presenti nell'Aiuto

[“Configurazioni server-database supportate”](#) a pagina 3

[“Installare Connect Pro Server e Flash Media Gateway”](#) a pagina 14

Scelta dell'implementazione di Acrobat Connect Pro Edge Server

Con l'implementazione di Acrobat Connect Edge Server nella rete, i client si connettono al server periferico, che a sua volta si collega ad Acrobat Connect Pro (anche detto *server di origine*). Questa connessione si verifica in modo trasparente. Gli utenti hanno infatti l'impressione di essere connessi direttamente al server della riunione.

I server periferici offrono i seguenti vantaggi:

Latenza ridotta della rete I server periferici memorizzano nella cache il contenuto on-demand (ad esempio presentazioni e riunioni registrate) e suddividono i flussi dal vivo, riducendo così il traffico verso l'origine. I server periferici collocano le risorse in prossimità dei client.

Protezione I server periferici sono un livello supplementare tra la connessione Internet del client e l'origine.

Se la licenza di cui disponete lo consente, potete installare e configurare un cluster di server periferici.

L'implementazione di server periferici in un cluster offre i seguenti vantaggi:

Failover Quando un server periferico è guasto, i client vengono instradati verso un altro server periferico.

Supporto per eventi di grandi dimensioni Se avete bisogno di più di 500 connessioni simultanee alla stessa riunione, un singolo server periferico non avrà socket sufficienti. Un cluster consente un numero maggiore di connessioni alla stessa riunione.

Bilanciamento del carico Se avete bisogno di più di 100 riunioni simultanee, un singolo server periferico potrebbe non disporre di memoria sufficiente. I server periferici possono essere implementati in un cluster con dispositivo per il bilanciamento del carico.

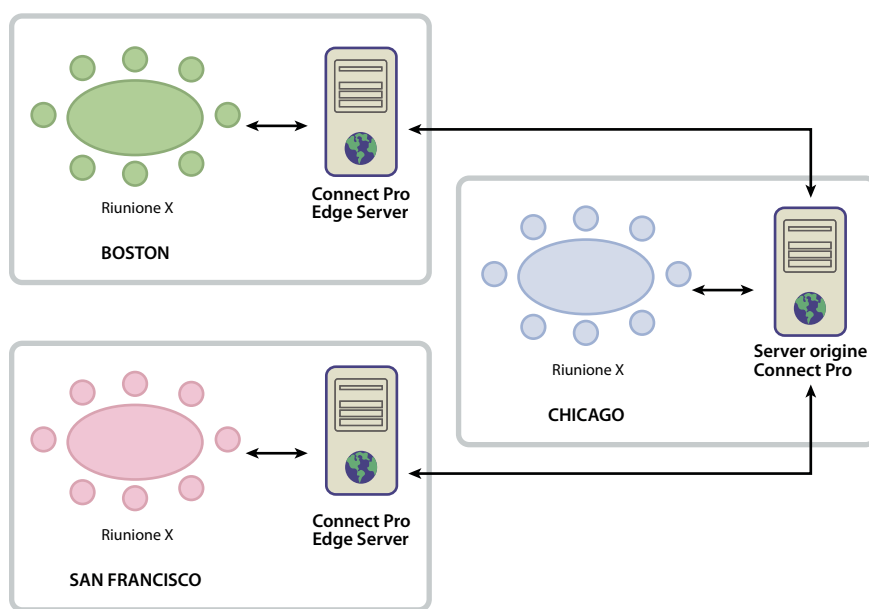
Funzionamento dei server periferici

I server periferici eseguono l'autenticazione degli utenti e ne autorizzano le richieste relative a servizi Web quale Acrobat Connect Pro Meeting invece di inoltrare ogni richiesta al server di origine e usarne le risorse per queste attività. Se i dati richiesti sono memorizzati nella cache del server periferico, tali dati vengono restituiti al client richiedente senza chiamare Acrobat Connect Pro Server.

Se i dati richiesti non sono memorizzati nella cache del server periferico, quest'ultimo inoltra la richiesta del client al server di origine, dove viene eseguita l'autenticazione dell'utente e viene autorizzata la richiesta di servizi. Il server di origine restituisce i risultati al server periferico richiedente, che consegna quindi i risultati al client richiedente. Il server periferico memorizza quindi queste informazioni nella cache, da cui altri utenti autenticati possono accedervi.

Esempio di implementazione di server periferici

Considerate il seguente esempio di implementazione di server periferici:



I client della sede di Chicago usano l'origine ubicata in un centro dati a Chicago. I server periferici di Boston e San Francisco raccolgono le richieste dei client locali e le inoltrano all'origine. I server periferici ricevono le risposte dall'origine a Chicago e le trasmettono ai client nelle proprie zone di pertinenza.

Altri argomenti presenti nell' Aiuto

[“Installare Acrobat Connect Pro Edge Server”](#) a pagina 20

[“Implementazione di Acrobat Connect Pro Edge Server”](#) a pagina 27

Creazione e ottimizzazione di un ambiente VMWare

L'installazione di Connect Pro Server su VMWare non è diversa dall'installazione su un computer fisico. Per informazioni sui requisiti hardware, software e di configurazione, consultate i [documenti tecnici](#) sull'esecuzione di Connect Pro Server in un ambiente virtuale.

Opzioni di audioconferenza Connect Pro

Connect Pro prevede due modalità di connessione ai fornitori di audioconferenze: con Universal Voice e con gli adattatori per telefonia integrata. Ciascuna soluzione presenta vantaggi diversi. Per ciascun fornitore audio potete configurare una sola soluzione o entrambe. Per ogni account Connect Pro potete configurare quanti fornitori di audioconferenze desiderate.

Universal Voice consente a Connect Pro di ricevere l'audio da qualunque fornitore di audioconferenze. L'audio può essere registrato insieme alla conferenza Web e inviato ai partecipanti VoIP.

La soluzione Universal Voice utilizza un componente denominato Flash Media Gateway che viene installato con Connect Pro Server. Flash Media Gateway riceve l'audio da un server SIP e lo invia a Connect Pro mediante RTMP. Per utilizzare Universal Voice è necessario disporre di un proprio server SIP o di un account con un fornitore SIP. Per informazioni sulla configurazione di Flash Media Gateway, consultate ["Implementazione di Universal Voice"](#) a pagina 37.

Dopo l'implementazione di Universal Voice, gli amministratori di account possono utilizzare Connect Pro Central per configurare le informazioni di audioconferenza. Per ulteriori informazioni, consultate www.adobe.com/go/learn_cnn_uvconfig_it.

Gli adattatori per telefonia integrata sono estensioni Java che consentono la comunicazione tra Connect Pro e determinati fornitori di audioconferenze. Gli adattatori per telefonia integrata offrono controlli di chiamata avanzati. Adobe fornisce diversi adattatori per telefonia integrata all'indirizzo www.adobe.com/go/learn_cnn_adaptors_it.

Potete inoltre utilizzare l'API Java per telefonia di Connect Pro per sviluppare un adattatore per telefonia integrata da un qualunque fornitore di audioconferenze. Per ulteriori informazioni, consultate [Uso della telefonia con Adobe Acrobat Connect Pro](#).

Inoltre Universal Voice può essere configurato per gli adattatori per telefonia integrata. Consultate ["Configurazione di Universal Voice per gli adattatori per telefonia integrata"](#) a pagina 43.

Nella tabella seguente sono descritte le funzioni di entrambe le soluzioni:

	Fornitore audio Universal Voice	Adattatore telefonico integrato
Trasmissione audio a partecipanti VoIP	Sì	No (a meno che non sia configurato un adattatore per Universal Voice)
Controllo avanzato delle chiamate. Ad esempio, disattivazione dell'audio, pausa e così via.	No	Sì
Registrazione dell'audio con Connect Pro Meeting	Sì	Sì
Richiede Flash Media Gateway (incluso nel programma di installazione di Connect Pro)	Sì	No (a meno che non sia configurato un adattatore per Universal Voice)

Capitolo 2: Installazione di Connect Pro

Per installare Acrobat Connect Pro Server 7.5, Acrobat Connect Pro Edge Server 7.5 e Flash Media Gateway, eseguite il programma di installazione e seguite i passi della procedura guidata della console di gestione applicazione.

Installare Connect Pro Server e Flash Media Gateway

Eeguire il programma di installazione

- 1 Eseguite l'accesso al computer come amministratore.
- 2 Chiudete tutte le applicazioni aperte.
- 3 Inserite il DVD di installazione nell'unità DVD. Nella schermata di avvio fate clic sul pulsante di installazione di Adobe Acrobat Connect Pro Server 7.5.

Se l'installazione non viene avviata automaticamente, fate doppio clic sul file install.exe nella cartella Connect\7.5\Disk1\InstData\VM\install.exe.

- 4 Selezionate una lingua e fate clic su OK per continuare.
- 5 Nella schermata introduttiva fate clic su Avanti per continuare.
- 6 Selezionate i prodotti che desiderate installare, quindi fate clic su Avanti per continuare:
 - Connect Pro Server
 - Flash Media Gateway

Nota: se non avete un fornitore SIP/VOIP upstream, non installate Flash Media Gateway. Per ulteriori informazioni, vedete *“Opzioni di audioconferenza Connect Pro”* a pagina 13.

- 7 Nella schermata Contratto di Licenza leggete il contratto, selezionate Accetto i termini del contratto di licenza e fate clic su Avanti.
- 8 Per selezionare il percorso di installazione di Connect Pro Server, effettuate una delle seguenti operazioni, quindi fate clic su Avanti:
 - Fate clic su Avanti per accettare il percorso di installazione predefinito di Connect Pro Server (c:\breeze) oppure fate clic su Scegli per selezionare un percorso diverso.
 - Se avete scelto un percorso diverso e desiderate utilizzare quello predefinito, fate clic su Ripristina cartella predefinita.
 - Se Acrobat Connect Pro è già installato su questo computer, viene visualizzata la schermata Aggiornamento installazione Connect Pro esistente. Selezionate la casella di controllo per confermare che avete eseguito il backup del database e della directory principale di Connect Pro.
- 9 Per selezionare il percorso di installazione di Flash Media Gateway, effettuate una delle seguenti operazioni, quindi fate clic su Avanti:
 - Fate clic su Avanti per accettare il percorso di installazione predefinito (C:\Program Files\Adobe\Flash Media Gateway) oppure fate clic su Scegli per selezionare un percorso diverso.
 - Se avete scelto un percorso diverso e desiderate utilizzare quello predefinito, fate clic su Ripristina cartella predefinita.

- Se sul computer è già installato Flash Media Gateway, viene visualizzata la schermata di aggiornamento dell'installazione di Flash Media Gateway.

10 Inserite il vostro numero di serie e fate clic su Avanti.

***Nota:** Adobe vi ha inviato una e-mail con un collegamento al sito delle licenze. Selezionate il collegamento per recuperare il vostro numero di serie.*

11 Se viene visualizzata la schermata del motore di database incorporato, effettuate una delle seguenti operazioni:

- Se desiderate installare un database su un altro computer, selezionate Non installare il motore database incorporato.
- Per installare il database incorporato, selezionate Installa il motore database incorporato nella seguente posizione. Per eseguire l'installazione nel percorso predefinito (c:\Program Files\Microsoft SQL Server), fate clic su Avanti. Per selezionare un percorso diverso, fate clic su Scegli.

***Nota:** se il programma di installazione rileva che sul computer è già installato Microsoft SQL Server, il database non viene installato. Se si sta eseguendo una migrazione e utilizzate già il database incorporato, Connect Pro utilizza il database esistente. Tuttavia, a volte il programma di installazione rileva una vecchia versione di SQL Server che non funziona con Connect Pro. Seguite le istruzioni in ["Disinstallare Acrobat Connect Pro Server"](#) a pagina 21 e riavviate l'installazione.*

12 Se installate il motore del database incorporato, specificate una password complessa e fate clic su Avanti.

13 Esaminate il riepilogo relativo alla preinstallazione. Fate clic su Precedente per modificare le impostazioni. Fate clic su Installa per installare il software.

14 Nella schermata Inizializzazione del servizio Connect Pro, effettuate una delle operazioni seguenti:

- Selezionate Avvia Connect Pro... (consigliato).
- Selezionate Non avviare subito Connect Pro [...].

Se decidete di avviare Connect Pro al successivo riavvio, eseguite la configurazione di Connect Pro prima di avviarlo per la prima volta. Per aprire la console di gestione applicazione e configurare Connect Pro, selezionate Start -> Programmi -> Adobe Acrobat Connect Pro Server -> Configura Connect Pro Enterprise Server.

15 Se decidete di avviare Acrobat Connect Pro, un messaggio indica che il servizio viene avviato.

Acrobat Connect Pro Server esegue quattro servizi Windows: Adobe Connect Enterprise Service, Flash Media Server (FMS), Flash Media Administration Server e Acrobat Connect Pro Presence Server. Flash Media Gateway viene eseguito come servizio di Flash Media Gateway. Consultate ["Avviare e arrestare i server"](#) a pagina 87.

16 Fate clic su Fine per uscire dal programma di installazione.

Se avete scelto di avviare Connect Pro, si apre una finestra del browser con la procedura guidata di gestione applicazione, per effettuare le operazioni di configurazione.

Configurazione di Acrobat Connect Pro con la procedura guidata della console di gestione applicazione

Dopo aver installato Acrobat Connect Pro, il programma di installazione avvia la procedura guidata di gestione applicazione, in cui sono fornite le istruzioni per configurare le impostazioni del database e del server, caricare il file di licenza e creare un amministratore.

***Nota:** se un'altra applicazione è in esecuzione sulla porta 80, la console di gestione applicazione non verrà aperta. Arrestate l'applicazione in esecuzione sulla porta 80 e riaprite la console di gestione applicazione.*

Per aprire la console di gestione applicazione scegliete Start > Programmi > Adobe Acrobat Connect Pro Server > Configura Connect Pro Enterprise Server oppure utilizzate il seguente URL: <http://localhost:8510/console>.

1. Leggere la schermata Benvenuti.

In questa schermata vengono fornite informazioni di base sulla procedura guidata.

2. Immettere le impostazioni del database.

Impostate i valori per i parametri elencati di seguito. Fate clic su Avanti per connettervi al database e rivedere le impostazioni.

Host database Il nome host del computer in cui è installato il database. Se avete installato il database incorporato, il valore è localhost.

Nome database Il nome del database. Il valore predefinito è breeze.

Porta database La porta usata dal database per comunicare con Acrobat Connect Pro. Il valore predefinito è 1433. (Se usate il motore di database incorporato, impostate questo valore predefinito su 1434.)

Utente database Il nome dell'utente del database. Se avete installato il database incorporato, il valore predefinito è sa.

Password dell'utente del database La password per l'utente del database. Se avete installato il database incorporato, la password viene impostata nel programma di installazione.

3. Immettere le impostazioni del server.

Nome account Un nome che identifica l'account di Acrobat Connect Pro, ad esempio "Account Acrobat Connect Pro 7".

Host di Connect Pro Un nome di dominio completo (FQDN, Fully Qualified Domain Name) usato dai client per connettersi a Connect Pro. Se ad esempio l'URL dell'account è <http://connect.esempio.com>, il valore Host di Connect Pro è connect.esempio.com.

Porta HTTP La porta usata da Acrobat Connect Pro per comunicare con HTTP. Il valore predefinito è 80. Se specificate un valore diverso da 80, i client devono aggiungere il numero della porta al nome host nell'URL quando accedono all'account di Acrobat Connect Pro.

Mappature host Nome è il nome host del computer in cui è installato Acrobat Connect Pro. Nome esterno è il nome di dominio completo usato dai client per connettersi ad Acrobat Connect Pro.

Nota: non aggiungete una porta al nome di dominio completo nella casella Nome esterno.

Host SMTP Il nome host del computer che ospita il server di posta elettronica SMTP.

Nome utente SMTP Il nome utente utilizzato per l'autenticazione sull'host SMTP. Se il campo viene lasciato vuoto, Connect Pro tenta di inviare le e-mail senza eseguire l'autenticazione con il server SMTP.

Password SMTP La password per il nome utente SMTP.

E-mail sistema L'indirizzo e-mail da cui vengono inviati i messaggi amministrativi.

E-mail supporto tecnico L'indirizzo e-mail del supporto tecnico per gli utenti di Acrobat Connect Pro.

E-mail CCN Un indirizzo e-mail di copia per conoscenza nascosta a cui vengono inviate tutte le notifiche utente. Questa variabile consente la registrazione amministrativa dei messaggi e-mail inviati tramite Acrobat Connect Pro senza esporre un indirizzo e-mail interno.

Memorizzazione condivisa Un volume e una directory su un server esterno in cui viene memorizzato il contenuto, ad esempio `\\volume\directory`. Se desiderate memorizzare il contenuto in più volumi, separateli con punto e virgola (;). Prima di configurare questa funzione, consultate "[Configurazione della memorizzazione condivisa](#)" a pagina 45.

Dimensione cache contenuto Un numero intero compreso tra 1 e 100 che specifica la percentuale di spazio libero su disco da usare per la memorizzazione del contenuto in Acrobat Connect Pro. Poiché la dimensione della cache può aumentare oltre il valore percentuale che avete specificato, è consigliabile impostare un valore compreso tra 15 e 50. Se non specificate alcun valore o immettete 0, la cache non viene usata e viene eseguito il mirroring del contenuto su Acrobat Connect Pro ed eventuali volumi esterni. Prima di configurare questa funzione, consultate “[Configurazione della memorizzazione condivisa](#)” a pagina 45.

4. Specificare le impostazioni per Flash Media Gateway.

Inserite i nomi dei computer e i nomi esterni per i server Flash Media Gateway. Le impostazioni non hanno effetto immediato. Quando fate clic su OK per confermare le impostazioni, Connect Pro potrebbe riavviare tutti i server Flash Media Gateway. Le impostazioni vengono inviate a tutti i server Flash Media Gateway in un cluster.

Fate clic su **Aggiungi** per aggiungere i server Flash Media Gateway. Inserite i seguenti parametri:

Nome Il nome del computer su cui è installato Flash Media Gateway, ad esempio, mariarossi-pc.

Nome esterno Il nome di dominio completo del server su cui è installato Flash Media Gateway, ad esempio, mariarossi-pc.esempio.com.

Nota: non aggiungete una porta al nome di dominio completo nella casella Nome esterno.

Lo Stato indica se Connect Pro Server può connettersi o meno al server Flash Media Gateway. Per diventare attivo, il server Flash Media Gateway potrebbe richiedere alcuni secondi. Uno stato “Attivo” non indica che le impostazioni SIP sono state inviate al server Flash Media Gateway. Se Connect Pro Server non riesce a collegarsi con Flash Media Gateway, lo stato risulta “Inattivo”.

Fate clic su **Avanti** e inserite i seguenti parametri:

Nome utente Il nome utente per il profilo SIP che il server Flash Media Gateway utilizza per creare le sessioni SIP, ad esempio sipUN1.

Password La password per il profilo SIP che il server Flash Media Gateway utilizza per creare le sessioni SIP.

Indirizzo SIP L'indirizzo del server SIP per il profilo SIP che il server Flash Media Gateway utilizza per creare le sessioni SIP, ad esempio, 10.12.13.14:12345.

Host predefinito per il profilo SIP. Questo parametro rappresenta l'indirizzo del server SIP da utilizzare se la registrazione con il server SIP non riesce ed in genere è lo stesso dell'indirizzo SIP.

Registrazione Scegliete se un server Flash Media Gateway va registrato sul server SIP.

Porta SIP La porta su cui il server Flash Media Gateway riceve le richieste SIP, ad esempio, 5060.

Limite di porta inferiore Il numero di porta più basso che è possibile utilizzare per i dati audio RTP. L'impostazione predefinita è 5000.

Limite di porta superiore Il numero di porta più alto che è possibile utilizzare per i dati audio RTP. L'impostazione predefinita è 6000.

Scadenza registrazione L'intervallo, in secondi, con cui Flash Media Gateway rinnova la registrazione con il server SIP. il valore predefinito è 2400 secondi.

5. Caricare il file della licenza.

Acrobat Connect Pro non viene attivato finché non scaricate un file di licenza da Adobe e lo installate nel computer in cui è installato Acrobat Connect Pro. Fate clic sul collegamento per scaricare il file di licenza da Adobe. Individuate il file e copiatelo nell'installazione di Acrobat Connect Pro.

6. Creare un amministratore degli account.

Per ogni account di Acrobat Connect Pro è necessario almeno un amministratore che esegua attività nell'applicazione Web Connect Pro Central. Gli account aggiornati dispongono già di almeno un amministratore, ma ne potete aggiungere uno supplementare in questa scheda.

7. Continuare a usare Acrobat Connect Pro.

In questa schermata potete accedere a Connect Pro Central (l'applicazione Web che vi consente di gestire l'account, creare riunioni, eventi e così via, e gestire il contenuto sul computer in cui è installato Acrobat Connect Pro), tornare alla console di gestione applicazione (per modificare o rivedere le impostazioni) oppure consultare la documentazione per ottenere ulteriori informazioni su Acrobat Connect Pro.

Verificare l'installazione

Verificare la connettività del database

Se potete accedere ad Connect Pro Central (un'applicazione Web inclusa in Acrobat Connect Pro), il database e Acrobat Connect Pro possono funzionare congiuntamente.

1 Andate al seguente URL: `http://[hostname]`.

Nota: in questo URL [hostname] è il valore che avete impostato per l'host di Connect Pro nella console di gestione applicazione.

2 Immettete l'ID e la password di login che avete impostato nella console di gestione applicazione.

Se l'accesso ha esito positivo, viene visualizzata la scheda principale di Connect Pro Central.

Verificare la possibilità di invio di notifiche e-mail

Se non avete inserito un valore nel campo Host SMTP della console di gestione applicazione, Acrobat Connect Pro non può inviare notifiche e-mail. Se avete specificato un host SMTP, effettuate quanto segue per verificare se Connect Pro può inviare le notifiche e-mail:

1 Fate clic sulla scheda Amministrazione nella scheda principale di Connect Pro Central.

2 Fate clic sulla scheda Utenti e gruppi.

3 Fate clic su Nuovo utente.

4 Nella pagina Informazioni sul nuovo utente immettete le informazioni richieste. Di seguito è riportato un elenco parziale di opzioni:

E-mail Usate l'indirizzo e-mail del nuovo utente. Assicuratevi che l'opzione Invia per e-mail le nuove informazioni su account utente, login e password sia selezionata.

Nuova password Create una password composta da 4 a 16 caratteri.

5 Fate clic su Avanti per continuare.

6 In Modifica appartenenza al gruppo selezionate un gruppo, assegnate l'utente a tale gruppo e fate clic su Fine.

7 Allocate tempo sufficiente per consentire all'utente di controllare le notifiche e-mail.

Se l'utente riceve la notifica, Acrobat Connect Pro funziona e potete inviare messaggi e-mail usando il server di posta elettronica.

- 8 Se l'e-mail non viene recapitata al destinatario, effettuate le seguenti operazioni:
 - a Verificate che l'indirizzo e-mail sia valido.
 - b Verificate che l'e-mail non sia stata catalogata come messaggio di posta indesiderata.
 - c Verificate che Acrobat Connect Pro sia stato configurato con un host SMTP valido e assicuratevi che il servizio SMTP funzioni all'esterno di Acrobat Connect Pro.
 - d Contattate il supporto Adobe visitando il sito Web all'indirizzo www.adobe.com/go/connect_licensed_programs_it.

Verificare la possibilità di utilizzo di Adobe Presenter

Per verificare se potete usare Adobe Presenter, inviate una presentazione di Microsoft PowerPoint ad Acrobat Connect Pro da compilare come presentazione Flash, quindi visualizzatela.

Per inviare una presentazione PowerPoint ad Acrobat Connect Pro, installate Adobe Presenter su un computer in cui sia già installato PowerPoint.

- 1 Avviate un browser e aprite Connect Pro Central (<http://localhost:8510> o il nome di dominio completo di Connect Pro Server).
- 2 Fate clic su Risorse -> Guida introduttiva.
- 3 Nella pagina Guida introduttiva, fate clic su Pubblica presentazioni -> Installa Adobe Presenter.
- 4 Eseguire il programma di installazione.
- 5 Se non disponete già di una presentazione PowerPoint, create e salvate una presentazione contenente una o due diapositive.
- 6 Aprite la procedura guidata di pubblicazione di Connect Pro scegliendo Pubblica dal menu di Adobe Presenter in PowerPoint.
- 7 Selezionate Connect Pro e immettete le informazioni relative al server.
- 8 Accedete con il vostro indirizzo e-mail e la vostra password ed eseguite i passaggi indicati nella procedura guidata di pubblicazione. Assicuratevi di far parte del gruppo Autori (Amministrazione > Utenti e gruppi in Connect Pro Central).

Completati i passaggi della procedura guidata Pubblica, la presentazione PowerPoint viene caricata in Connect Pro e compilata come presentazione Flash.

- 9 Al termine della compilazione passate alla scheda Contenuto in Connect Pro Central e individuate la presentazione.
- 10 Aprite la presentazione per visualizzarla.

Verificare la possibilità di utilizzo di Training

Nota: Adobe Acrobat Connect Pro Training è una funzione opzionale il cui uso deve essere consentito dalla licenza di cui disponete.

- ❖ Fate clic sulla scheda Formazione in Connect Pro Central.

Se tale scheda è visibile e accessibile, Training funziona. Assicuratevi di far parte del gruppo Manager formazione (Amministrazione > Utenti e gruppi).

Verificare la possibilità di utilizzo di Meeting

Nota: Adobe Acrobat Connect Pro Meeting è una funzione opzionale il cui uso deve essere consentito dalla licenza di cui disponete.

Per verificare il funzionamento di Acrobat Connect Pro Meeting, dovete far parte del gruppo Ospitanti riunioni o Amministratori.

- 1 Accedete a Connect Pro Central come utente membro del gruppo Ospitanti riunioni o Amministratori.
- 2 Fate clic sulla scheda Riunioni e selezionate Nuova riunione.
- 3 Nella pagina Immettere informazioni sulla riunione immettete le informazioni richieste. Per l'opzione Meeting Access selezionate l'opzione Solo gli utenti registrati e gli ospiti accettati possono entrare nella stanza. Fate clic su Fine per creare la riunione.
- 4 Fate clic sul pulsante Entra nella stanza riunioni.
- 5 Accedete per entrare come utente registrato.
- 6 Se viene visualizzata la finestra del componente aggiuntivo Acrobat Connect, seguite le istruzioni per installarlo.

Se la stanza riunioni si apre, Acrobat Connect Pro Meeting funziona.

Verificare la possibilità di utilizzo di Events

Nota: Adobe Acrobat Connect Pro Events è una funzione opzionale il cui uso deve essere consentito dalla licenza di cui disponete.

- 1 Accedete a Connect Pro Central come utente membro del gruppo Manager evento o Amministratori.
- 2 Fate clic sulla scheda Gestione evento in Connect Pro Central.

Se questa scheda è visibile e accessibile, Connect Pro Events funziona.

Installare Acrobat Connect Pro Edge Server

Eeguire il programma di installazione

- 1 Chiudete tutte le applicazioni aperte.
- 2 Inserite il DVD di installazione nell'unità DVD. Nella schermata di avvio fate clic sul pulsante di installazione di Adobe Acrobat Connect Pro Edge Server

Se il programma di installazione non viene avviato automaticamente, fate doppio clic sul file setup.exe nella cartella principale del DVD di installazione.

- 3 Selezionate una lingua nella finestra di dialogo Selezionare la lingua d'installazione. Fate clic su OK per continuare.
- 4 Nella schermata Installazione fate clic su Avanti per continuare.
- 5 Nella schermata Contratto di Licenza leggete il contratto, selezionate Accetto i termini del contratto di licenza e quindi fate clic su Avanti.

- 6 Effettuate una delle seguenti operazioni:
 - Fate clic su Avanti per accettare il percorso di installazione predefinito (c:\breeze); oppure, per selezionare un percorso diverso, fate su Sfoglia, quindi su Avanti.
 - Se Adobe Acrobat Connect Pro Edge Server è già installato su questo computer, viene visualizzata la schermata Aggiornamento installazione Adobe Acrobat Connect Pro Edge Server esistente. Fate clic su Avanti.
- 7 Nella schermata di selezione della cartella del menu Start, effettuate una delle operazioni seguenti:
 - Fate clic su Avanti per accettare il percorso predefinito per i collegamenti del menu Start.
 - Fate clic su Sfoglia per selezionare un altro percorso.
- 8 Nella finestra di dialogo Pronto per l'installazione verificate il percorso in cui verranno installati Adobe Acrobat Connect Pro Edge Server e la cartella per il menu Start. Fate clic su Indietro per rivedere o modificare queste impostazioni o fate clic su Installa.
- 9 Per uscire dal programma di installazione di Adobe Acrobat Connect Pro Edge Server 7, fate clic su Fine.

Altri argomenti presenti nell' Aiuto

["Implementazione di Acrobat Connect Pro Edge Server"](#) a pagina 27

Disinstallare i server

Disinstallare Acrobat Connect Pro Server

Nota: La disinstallazione di Acrobat Connect Pro Server non comporta la disinstallazione di SQL Server.

- 1 Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server > Disinstalla Connect Pro Server.
- 2 Eliminate la cartella principale di Acrobat Connect Pro. Il percorso predefinito è c:\breeze.

Quando disinstallate Acrobat Connect Pro, i file custom.ini e config.ini e i file del contenuto non vengono eliminati. L'eliminazione della cartella principale comporta l'eliminazione di questi file.

Importante: la cartella principale contiene la cartella del contenuto. Per conservare il contenuto, copiatelo in un'altra posizione.

- 3 Selezionate Start > Esegui. Inserite **regedit** e fate clic su OK per aprire l'editor del Registro di sistema.
 - a Cercate My Computer -> HKEY_LOCAL_MACHINE -> SOFTWARE -> MICROSOFT -> WINDOWS -> CurrentVersion -> Uninstall.
 - b Selezionate tutte le chiavi per Adobe Acrobat Connect Pro ed eliminatele (i titoli potrebbero contenere una stringa sulla versione).
- 4 (Facoltativo) Se avete installato il motore del database incorporato, eliminate le seguenti chiavi di registro:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLSERVER

Disinstallare Acrobat Connect Pro Edge Server

- 1 Scegliete Start > Impostazioni > Pannello di controllo > Installazione applicazioni > Adobe Acrobat Connect Pro Edge Server > Rimuovi.
- 2 Eliminate la cartella principale di Acrobat Connect Pro. Il percorso predefinito è c:\breeze.

Disinstalla Flash Media Gateway

Flash Media Gateway viene disinstallato quando si disinstalla Acrobat Connect Pro Server. Per disinstallare Flash Media Gateway potete inoltre eseguire il programma: Program Files\Adobe\Flash Media Gateway\Uninstall_Flash Media Gateway\ Uninstall Flash Media Gateway.exe.

Capitolo 3: Implementazione e configurazione di Connect Pro

Dopo aver installato Adobe Acrobat Connect Pro Server, Flash Media Gateway o Adobe Acrobat Connect Pro Edge Server e aver completato la prima fase della configurazione con la console di gestione applicazione, configurate le seguenti opzioni facoltative e implementate il server.

Implementazione di Acrobat Connect Pro Server

Implementare Acrobat Connect Pro Server

- 1 Nel server DNS, definite un nome di dominio qualificato (FQDN) per Acrobat Connect Pro (ad esempio, connect.nomeazienda.com). Mappate il nome del dominio sull'indirizzo IP del computer host di Acrobat Connect Pro.
- 2 Se desiderate che Acrobat Connect Pro sia disponibile all'esterno della rete, configurate le seguenti porte su un firewall:

80 La porta predefinita per il server applicazioni di Acrobat Connect Pro. La porta terziaria per il server riunioni (Flash Media Server).

1935 La porta predefinita per il server riunioni (Flash Media Server).

443 La porta predefinita per SSL. La porta secondaria per il server riunioni (Flash Media Server).

Nota: se il traffico di Acrobat Connect Pro viene instradato attraverso un gateway (con un indirizzo IP diverso), assicuratevi che i firewall siano configurati per accettare richieste dall'indirizzo IP del gateway.

Per assistenza nell'implementazione di Acrobat Connect Pro, contattate il supporto Adobe all'indirizzo www.adobe.com/go/connect_licensed_programs_it.

Altri argomenti presenti nell' Aiuto

“[Requisiti delle porte](#)” a pagina 2

Implementare un cluster di server Acrobat Connect Pro

Prima di implementare un cluster, è necessario disporre di quanto segue:

- Una licenza che supporti il numero di nodi del cluster. Per ulteriori informazioni, contattate il vostro rappresentante Adobe di fiducia.
- Ogni computer del cluster deve avere un indirizzo IP statico e una voce DNS.
- Un server e-mail.
- SQL Server 2005 Standard Edition installato in un computer dedicato con indirizzo IP statico. Se installate Acrobat Connect Pro in un cluster, non è possibile usare il motore database incorporato. Tutti i server host di Acrobat Connect Pro sono collegati al database; tuttavia le restrizioni di licenza consentono la connessione di un solo server al motore database incorporato.

- Una soluzione hardware o software per il bilanciamento del carico. Un dispositivo hardware per il bilanciamento del carico richiede un computer a parte con indirizzo IP statico e voce DNS. Un sistema software può invece essere installato in uno dei nodi del cluster.
- Uno o più volumi per la memorizzazione condivisa. Questa configurazione non è obbligatoria, ma consigliata.

Prima di implementare Acrobat Connect Pro in un cluster, eseguite l'installazione su un singolo computer. Configurate inoltre funzioni aggiuntive (ad esempio SSL, l'integrazione con un servizio di directory, Single Sign-On, la memorizzazione di contenuto condivisa e così via) e verificate che funzionino come dovrebbero in un singolo server.

1 Installate e configurate Acrobat Connect Pro su un server dedicato.

Usate lo stesso numero di serie e lo stesso file di licenza ogni volta che installate Acrobat Connect Pro. Non installate il motore database incorporato e, se il sistema di memorizzazione condivisa richiede un nome utente e una password, non avviate Acrobat Connect Pro dal programma di installazione.

2 Se il sistema di memorizzazione condivisa richiede un nome utente e una password, effettuate le seguenti operazioni per aggiungere tali dati ad Adobe Connect Enterprise Service:

- a Aprite il pannello di controllo Servizi.
- b Fate doppio clic su Adobe Connect Enterprise Service.
- c Fate clic sulla scheda Connessione.
- d Selezionate Questo account e inserite il nome utente per il sistema di memorizzazione condivisa nel relativo campo. La sintassi per il nome utente è [dominiosecondario\]nomeutente.
- e Inserite e confermate la password per il sistema di memorizzazione condivisa.
- f Fate clic su Applica, quindi su OK.

3 Per avviare Acrobat Connect Pro, effettuate le operazioni seguenti:

- a Nel pannello di controllo Servizi, selezionate Flash Media Server (FMS) e fate clic su Avvia il servizio.
- b Nel pannello di controllo Servizi, selezionate Adobe Connect Enterprise Service e fate clic su Avvia il servizio.

4 Scegliete Start > Programmi > Adobe Connect Pro Server 7 > Configura Connect Pro Server 7 per aprire la console di gestione applicazione, quindi fate clic su Avanti.

5 Nella schermata Impostazioni database, inserite i dati per il database SQL Server e fate clic su Avanti.

Se Acrobat Connect Pro si collega correttamente al database, vengono visualizzati un messaggio di conferma e le impostazioni del database. Fate clic su Avanti.

6 Nella schermata Impostazioni server, effettuate le seguenti operazioni e fate clic su Avanti:

- a Inserite un nome account.
- b Nella casella di testo Host di Connect Pro, inserite il nome del computer in cui è in esecuzione il sistema di bilanciamento del carico.
- c Inserite il numero di porta HTTP. A seconda del sistema di bilanciamento del carico, potrebbe trattarsi della porta 80 o 8080.
- d Inserite il nome esterno del nodo del cluster.
- e Inserite il nome del dominio dell'host e del sistema SMTP e gli indirizzi e-mail del supporto.
- f Se usate un sistema di memorizzazione condivisa, inserite il percorso del volume (in caso di più volumi, separateli con punto e virgola).
- g Inserite la percentuale del server Acrobat Connect Pro da usare come cache locale.

Nota: il contenuto viene scritto nelle cache locale e nel volume di memorizzazione condivisa. Dopo il suo utilizzo, il contenuto viene mantenuto nella cache locale per 24 ore. Trascorso tale periodo, se la percentuale di utilizzo della cache viene superata il contenuto viene eliminato dalla cache.

- 7 Caricate il file della licenza e fate clic su Avanti.
- 8 Create un amministratore e fate clic su Fine.
- 9 Ripetete i passaggi da 1 a 8 per ogni server del cluster.
- 10 Per configurare il sistema di bilanciamento del carico, effettuate le seguenti operazioni:
 - a Configurate il sistema di bilanciamento del carico con ascolto della porta 80.
 - b Aggiungete i nomi di tutti i nodi del cluster al file di configurazione del sistema di bilanciamento del carico.

Nota: per informazioni dettagliate sulla configurazione del sistema di bilanciamento del carico, consultate la documentazione fornita con il sistema stesso.

- 11 Aprite un browser Web e inserite il nome di dominio del sistema di bilanciamento del carico, ad esempio `http://connect.esempio.com`.

Per assistenza nell'implementazione di un cluster, contattate il supporto Adobe all'indirizzo www.adobe.com/go/connect_licensed_programs_it.

Altri argomenti presenti nell' Aiuto

[“Installare Connect Pro Server e Flash Media Gateway”](#) a pagina 14

[“Configurazione della memorizzazione condivisa”](#) a pagina 45

Verifica delle operazioni in un cluster

Se un computer del cluster si spegne, il sistema per il bilanciamento del carico indirizza tutte le richieste HTTP a un computer funzionante nello stesso cluster.

Quando inizia una riunione, il server applicazioni assegna un host primario e un host di backup alla stanza riunioni in base al carico. Se l'host primario viene spento, i clienti si riconnettono all'host di backup.

È consigliabile verificare che il contenuto caricato su un server di un cluster venga replicato sugli altri computer del cluster.

Nelle seguenti procedure si parte dal presupposto che il cluster comprenda due computer, Computer1 e Computer2.

Verifica del bilanciamento del carico e del failover riunione

- 1 Avviate Acrobat Connect Pro su entrambi i computer.
 - a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Meeting Server.
 - b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Central Application Server.
- 2 Accedete a Connect Pro Central dal seguente URL:

`http://[nomehost]`

Per *nomehost* usate lo stesso valore per l'host di Connect Pro che avete immesso nella console di gestione applicazione.

- 3 Selezionate la scheda Riunioni e fate clic sul collegamento di una riunione per entrare nella stanza riunioni.

Se necessario, create una nuova riunione.

4 Arrestate Acrobat Connect Pro su Computer2.

a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Central Application Server.

b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Meeting Server.

Se il failover della riunione ha avuto esito positivo, alla riunione resta associata una spia di connessione verde.

5 In Connect Pro Central fate clic su una scheda o su un collegamento.

Se il sistema di bilanciamento del carico funziona correttamente, dovrete poter inviare richieste a Connect Pro Central e ricevere risposte.

Se il cluster comprende più di due computer, ripetete questa procedura di avvio/arresto per ogni computer del cluster.

Verificare la replica del contenuto

1 Avviate Acrobat Connect Pro su Computer1.

a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Meeting Server.

b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Central Application Server.

2 Arrestate Acrobat Connect Pro su Computer2.

a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Central Application Server.

b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Meeting Server.

3 Accedete a Connect Pro Central dal seguente URL:

`http://[nomehost]`

Per *nomehost* immettete lo stesso valore per l'host di Connect Pro che avete immesso nella console di gestione applicazione.

4 Caricate un'immagine JPEG o altro contenuto in Acrobat Connect Pro su Computer1:

- Assicuratevi di essere membri del gruppo Autori. (Un utente amministratore di account può aggiungere se stesso al gruppo Autori in Connect Pro Central.)
- Fate clic sulla scheda Contenuto.
- Fate clic su Nuovo contenuto e seguite le istruzioni visualizzate nel browser per aggiungere contenuto.

Una volta caricato il contenuto di prova, viene visualizzata una pagina Contenuto utente con l'elenco di tutti i contenuti che vi appartengono.

5 Fate clic sul collegamento del contenuto di prova appena caricato.

Viene visualizzata una pagina Informazioni sul contenuto con un URL per la visualizzazione del contenuto di prova.

6 Prendete nota dell'URL in quanto dovrete usarlo nel passaggio 10.

7 Fate clic sull'URL.

8 Avviate Computer2, attendete che Acrobat Connect Pro sia completamente avviato, quindi arrestate Computer1.

Se avete configurato una periferica di memorizzazione esterna, non dovete attendere l'avvio di Computer2 prima di eseguire l'arresto. Il contenuto richiesto viene infatti copiato dalla periferica esterna.

9 Chiudete la finestra del browser in cui state visualizzando il contenuto di prova.

10 Aprite una nuova finestra del browser e passate all'URL del contenuto di prova.

Se il contenuto di prova viene visualizzato, la replica su Computer2 ha avuto esito positivo. Una finestra vuota o un messaggio di errore indica che la replica ha avuto esito negativo.

Implementazione di Acrobat Connect Pro Edge Server

Flusso di lavoro per l'installazione di Acrobat Connect Pro Edge Server

1. Progettare le aree di server periferici.

Potete installare server periferici o cluster di server periferici in diverse ubicazioni, o *aree*, per allocare e bilanciare l'accesso ad Acrobat Connect Pro. Potete ad esempio installare un server periferico a San Francisco per gli utenti della costa occidentale e uno a Boston per gli utenti della costa orientale.

2. Installare Acrobat Connect Pro Edge Server.

Installate Acrobat Connect Pro Edge Server su ogni computer in ogni area. Se disponete ad esempio di un cluster di server periferici in un'area, installate Acrobat Connect Pro Edge Server su ogni computer del cluster. Consultate ["Installare Acrobat Connect Pro Edge Server"](#) a pagina 20.

3. Modificare il server DNS per ogni area.

Mappate il nome di dominio completo (FQDN) del server Acrobat Connect Pro di origine sull'indirizzo IP statico di Acrobat Connect Pro Edge Server in ogni area. Consultate ["Implementazione di Acrobat Connect Pro Edge Server"](#) a pagina 27.

4. Configurare il server periferico.

Dovete aggiungere parametri di configurazione al file custom.ini su ogni server periferico in cui è installato Acrobat Connect Pro Edge Server. Consultate ["Implementazione di Acrobat Connect Pro Edge Server"](#) a pagina 27.

5. Configurare il server di origine.

Dovete aggiungere parametri di configurazione al file custom.ini su ogni server in cui è installato Acrobat Connect Pro. Dovete inoltre impostare il nome esterno del server periferico nella console di gestione applicazione sul server di origine. Consultate ["Implementazione di Acrobat Connect Pro Edge Server"](#) a pagina 27.

6. Installare un sistema di bilanciamento del carico.

Se installate più server periferici in un'area, dovete usare un sistema di bilanciamento del carico tra i server periferici e configurarlo in modo che usi la porta 80. I server periferici usano la porta 8080. Per ulteriori informazioni, consultate la documentazione fornita con il sistema di bilanciamento del carico.

Implementare Acrobat Connect Pro Edge Server

Prima di implementare i server periferici, assicuratevi che Acrobat Connect Pro ed eventuali funzioni aggiuntive (ad esempio SSL, integrazione con un servizio di directory, Single Sign-On o un sistema di archiviazione condiviso per i contenuti) vengano eseguiti correttamente.

- 1 Sul server DNS mappate il nome di dominio completo (FQDN) del server di origine sull'indirizzo IP statico del server periferico. Se installate server periferici in più aree, ripetete questo passaggio per ogni area.

Nota: in alternativa potete usare un file host. In questo caso ogni client deve avere un file host che colleghi l'indirizzo IP statico del server periferico al nome FQDN del server di origine.

- 2 In Acrobat Connect Pro Edge Server aprite il file `[root_install_dir]\edgeserver\win32\conf\HttpCache.xml` e sostituite il nome del computer nel tag `HostName` con il nome FQDN del computer del server periferico, ad esempio `edge1.esempio.com`.

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

3 Su Acrobat Connect Pro Edge Server, create un nuovo file `[root_install_dir]\edgeserver\custom.ini` e immettete i valori e i parametri seguenti:

FCS_EDGE_HOST Nome di dominio completo (FQDN) del server periferico, ad esempio

```
FCS_EDGE_HOST=edge1.nomeazienda.com.
```

FCS_EDGE_REGISTER_HOST Nome FQDN del server di origine Acrobat Connect Pro, ad esempio

```
FCS_EDGE_REGISTER_HOST=connect.nomeazienda.com.
```

FCS_EDGE_CLUSTER_ID Nome del cluster. A ogni cluster di server periferici, o area, deve essere assegnato un ID univoco. Ogni computer del cluster deve avere lo stesso ID. Il formato consigliato è `nomeazienda-nomecluster`, ad esempio `FCS_EDGE_CLUSTER_ID=nomeazienda-us`.

Nota: dovete configurare questo parametro anche se state implementando un solo Acrobat Connect Pro Edge Server.

FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT Indirizzo IP o nome di dominio e numero di porta del computer in cui è installato Acrobat Connect Pro, ad esempio

```
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.nomeazienda.com:80.
```

Acrobat Connect Pro Edge Server si collega al server di origine Acrobat Connect Pro in questa posizione.

FCS_EDGE_PASSWORD (Facoltativo) Password per il server periferico. Se impostate un valore per questo parametro, dovete impostare lo stesso valore per ogni server periferico e server di origine.

FCS_EDGE_EXPIRY_TIME (Facoltativo) Numero in millisecondi entro il quale il server periferico deve registrarsi presso il server di origine prima che scada dal cluster e il sistema esegua il failover a un altro server periferico. Iniziate con il valore predefinito, `FCS_EDGE_EXPIRY_TIME=60000`.

FCS_EDGE_REG_INTERVAL (Facoltativo) Intervallo, in millisecondi, entro il quale il server periferico tenta di registrarsi presso il server di origine. Questo parametro determina la frequenza con cui il server periferico si rende disponibile per il server di origine. Iniziate con il valore predefinito, `FCS_EDGE_REG_INTERVAL=30000`.

DEFAULT_FCS_HOSTPORT (Facoltativo) Per configurare le porte dei server periferici, aggiungete la seguente riga:

```
DEFAULT_FCS_HOSTPORT=:1935,80,-443.
```

Il segno meno (-) davanti a 443 indica che la porta 443 è una porta protetta che riceve solo connessioni RTMPS. Se tentate una connessione RTMPS sulla porta 1935 o 80, la connessione avrà esito negativo. Analogamente, una richiesta di connessione RTMP non protetta sulla porta 443 avrà esito negativo.

Nota: se il server periferico usa un acceleratore hardware esterno, la porta 443 non deve essere configurata come porta protetta.

Seguono valori campione per il file `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 Riavviate il server periferico.

5 Nel server di origine Acrobat Connect Pro, aprite il file `[root_install_dir]\custom.ini` in un editor di testo e mappate il valore del parametro `FCS_EDGE_CLUSTER_ID` su un ID di zona; la sintassi è `edge.FCS_EDGE_CLUSTER_ID=zone-id`. Anche se state implementando un solo server periferico, dovete mappare l'ID del cluster su un ID di area.

Ogni cluster di server periferici deve avere un ID di area. L'ID di area può essere un numero intero positivo maggiore di 0. Potete avere ad esempio tre cluster mappati sulle aree da 1 a 3:

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

Esempio di file custom.ini per il server di origine:

```
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: se avete impostato un parametro `FCS_EDGE_PASSWORD` nel file `config.ini` del server periferico, impostate la stessa password anche nel file `custom.ini` sul server di origine.

- 6 Riavviate il server di origine.
- 7 Sul server di origine aprite la console di gestione applicazione (Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Configura Connect Pro Server). Selezionate la scheda Impostazioni applicazione, quindi selezionate Impostazioni server e nella sezione Mappature host immettete il nome esterno per il server periferico. Il nome esterno deve essere identico al valore impostato per il parametro `FCS_EDGE_HOST` sul server periferico.
- 8 Sul server di origine configurate Windows Firewall in modo che i server periferici possano accedere alla porta 8506.
- 9 Ripetete i passaggi da 2 a 4 per ogni server periferico di ogni area.
- 10 Ripetete i passaggi da 5 a 7 per ogni server di origine di ogni area.

Per assistenza nell'implementazione di server periferici, contattate il supporto Adobe all'indirizzo www.adobe.com/go/connect_licensed_programs_it.

Altri argomenti presenti nell' Aiuto

“Scelta dell'implementazione di Acrobat Connect Pro Edge Server” a pagina 11

Integrazione con un servizio di directory

Panoramica sull'integrazione con un servizio di directory

Potete integrare Acrobat Connect Pro con un servizio di directory per l'autenticazione degli utenti in base a una directory LDAP e per evitare di dover aggiungere manualmente singoli utenti e gruppi. Gli account utenti vengono creati automaticamente in Acrobat Connect Pro mediante sincronizzazioni manuali o programmate con la directory aziendale.

Per poter essere integrato con Acrobat Connect Pro, il server di directory deve usare il protocollo LDAP (Lightweight Directory Access Protocol) o LDAPS (Secure Lightweight Directory Access Protocol). LDAP è un protocollo client-server Internet per la ricerca di informazioni di contatto relative agli utenti in un server di directory compatibile con LDAP.

Acrobat Connect Pro si collega a una directory LDAP come client LDAP. Acrobat Connect Pro importa utenti e gruppi e ne sincronizza i dati con la directory LDAP. Potete inoltre configurare Acrobat Connect Pro per l'autenticazione degli utenti mediante confronto con la directory LDAP.

Qualsiasi servizio di directory conforme con LDAP può essere integrato con Acrobat Connect Pro. Per un elenco delle directory LDAP certificate, visitate www.adobe.com/go/connect_sysreqs_it.

Informazioni sulla struttura di directory LDAP

Le directory LDAP organizzano le informazioni in base allo standard X.500.

Un utente o un gruppo in una directory LDAP viene chiamato *voce*. Una voce è una raccolta di attributi. Un attributo è costituito da un tipo e da uno o più valori. I tipi usano stringhe quali `ou` (organizational unit) per unità organizzativa e `cn` (common name) per nome comune. I valori degli attributi sono informazioni quali un numero di telefono, un indirizzo e-mail e una foto. Per determinare la struttura di directory LDAP dell'organizzazione, contattate l'amministratore LDAP.

A ogni voce è assegnato un *nome distinto* (DN) che descrive un percorso alla voce attraverso una struttura ad albero dalla voce alla radice. Il DN di una voce nella directory LDAP è una concatenazione del nome della voce (denominato *nome distinto relativo*, RDN) e dei nomi delle voci che lo precedono nella struttura ad albero.

Una struttura ad albero può riflettere posizioni geografiche o suddivisioni in reparti all'interno di una società. Ad esempio, se Alicia Solis è un utente del reparto di controllo qualità (QA) presso Acme, Inc. in Francia, il DN di questo utente sarà:

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

Importare rami della directory

Quando importate utenti e gruppi da una directory LDAP in Acrobat Connect Pro, specificate un percorso a una sezione della struttura LDAP usando il DN della sezione. Ciò specifica l'ambito della ricerca. Supponete ad esempio di voler importare solo gli utenti di un determinato gruppo all'interno dell'organizzazione. Per fare ciò dovete conoscere l'ubicazione delle voci di tale gruppo nella struttura ad albero della directory.

Una tecnica comune consiste nell'usare il dominio Internet dell'organizzazione come radice della struttura. Ad esempio, Acme, Inc. può usare `dc=com` per specificare l'elemento radice della struttura. Un DN che specifica l'ufficio vendite di Singapore di Acme, Inc. potrebbe essere `ou=Singapore, ou=Marketing, ou=Employees, dc=Acme, dc=com`. (In questo esempio `ou` è l'abbreviazione di unità organizzativa e `dc` è l'abbreviazione di componente di dominio.)

Nota: alcune directory LDAP hanno più di una radice. In tal caso, potete importare rami distinti.

Importare utenti e gruppi

Le voci relative a utenti e gruppi possono essere strutturate in due modi in una directory LDAP: sotto lo stesso nodo di un ramo e sotto diversi rami.

Se utenti e gruppi sono sotto lo stesso nodo di un ramo LDAP, le impostazioni di utenti e gruppi per l'importazione delle voci contengono lo stesso DN di ramo. Ciò significa che quando importate utenti dovete usare un filtro per selezionare solo utenti e quando importate gruppi dovete usare un filtro per selezionare solo gruppi.

Se utenti e gruppi sono sotto diversi rami nella struttura, usate un DN di ramo che seleziona il ramo utente quando importate gli utenti e un DN di ramo che seleziona il ramo gruppo quando importate i gruppi.

Potete inoltre importare rami secondari per importare gli utenti di tutti i rami al di sotto di un determinato livello. Se desiderate ad esempio importare tutti i dipendenti del reparto vendite, potete usare il seguente DN di ramo:

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

Gli addetti alle vendite potrebbero tuttavia essere distribuiti in rami secondari. In questo caso, nella schermata Mappatura profilo utente impostate il parametro Ricerca nella sottostruttura su `true` per assicurare che vengano importati gli utenti dei rami secondari al di sotto di tale livello nella struttura.

Filtrare le voci selezionate

Un filtro specifica una condizione che una voce deve soddisfare affinché venga selezionata. Ciò limita la selezione delle voci in una parte determinata della struttura. Ad esempio, se il filtro specifica (`objectClass=organizationalPerson`), solo le voci con l'attributo `organizationalPerson` vengono selezionate per l'importazione.

Nota: l'attributo `objectClass` deve essere presente in tutte le voci di una directory LDAP.

Utenti e gruppi interni ed esterni

Gli utenti e i gruppi che create direttamente in Acrobat Connect Pro invece di importarli da una directory LDAP sono denominati utenti e gruppi *interni*. Gli utenti e i gruppi importati nel database di Acrobat Connect Pro da una directory LDAP sono denominati utenti e gruppi *esterni*.

Per assicurare che i gruppi importati siano sempre sincronizzati con la directory LDAP esterna, non potete aggiungere utenti e gruppi interni ai gruppi esterni. Potete tuttavia aggiungere utenti e gruppi esterni ai gruppi interni.

Se il valore del nome o del login di una voce di utente o gruppo importato corrisponde al login di un utente o gruppo interno esistente, la sincronizzazione delle directory modifica l'utente o il gruppo importato da interno a esterno e inserisce un avviso nel registro di sincronizzazione.

Integrare Acrobat Connect Pro con una directory LDAP

L'integrazione con un servizio di directory viene eseguita nella scheda Impostazioni servizio directory della console di gestione applicazione. Usate un account amministratore.

Potete configurare un server di directory per l'autenticazione degli utenti e la sincronizzazione LDAP. La configurazione può essere diretta a uno o più rami del servizio di directory.

1. Aprire la console di gestione applicazione.

Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Configura Connect Pro Server 7.

2. Immettere le impostazioni di connessione al server LDAP.

Selezionate la scheda Impostazioni servizio directory. Immettete valori nella schermata Impostazioni LDAP > Impostazioni di connessione e fate clic su Salva.

Quando fate clic su Salva, Acrobat Connect Pro esegue un test della connessione LDAP. Se il test ha esito negativo, compare il seguente messaggio: Le impostazioni sono state salvate correttamente ma non è stato possibile verificare la connettività LDAP. Verificate l'URL e la porta LDAP.

Campo	Valore predefinito	Descrizione
URL server LDAP	Nessun valore predefinito.	La sintassi standard è <code>ldap://[nomeserver:numeroporta]</code> . Se l'organizzazione usa un server LDAP protetto, usate <code>ldaps://</code> . Se non specificate una porta, Acrobat Connect Pro usa la porta standard LDAP (389) o LDAPS (636). LDAPS richiede certificati SSL. Se configurate Acrobat Connect Pro per una foresta Microsoft Active Directory in cui è attivato il catalogo globale, usate quest'ultimo (porta standard: 3268).
Metodo di autenticazione della connessione LDAP	Nessun valore predefinito.	Meccanismo di autenticazione delle credenziali (nome utente e password LDAP) dell'account del servizio LDAP per Acrobat Connect Pro (diritti amministrativi). Semplice (autenticazione standard; consigliato). Anonimo (nessuna password; il server LDAP deve essere configurato per consentire login anonimi). Digest MD5 (configurate il server LDAP per consentire l'autenticazione digest).
Nome utente connessione LDAP	Nessun valore predefinito.	Login amministrativo sul server LDAP.
Password connessione LDAP	Nessun valore predefinito.	Password amministrativa sul server LDAP.
Timeout query LDAP	Nessun valore predefinito.	Tempo in secondi allo scadere del quale la query viene annullata. Se lasciate vuoto questo campo, non viene impostato alcun timeout. Impostate questo valore su 120.
Limite dimensione pagina di query LDAP	Nessun valore predefinito.	La dimensione della pagina dei risultati restituiti dal server LDAP. Se la casella è vuota o impostata su 0, non viene usata alcuna dimensione di pagina. Usate questo campo per i server LDAP in cui è configurata una dimensione massima per i risultati. Impostate la dimensione della pagina su un valore inferiore alla dimensione massima dei risultati, in modo che i risultati vengano recuperati dal server in più pagine. Ad esempio, se provate a integrare una grande directory LDAP in grado di visualizzare solo 1000 utenti mentre gli utenti da importare sono 2000, l'integrazione non riesce. Se impostate la dimensione della pagina di query su 100, i risultati vengono restituiti in 20 pagine e tutti gli utenti vengono importati.

Di seguito è riportato un esempio di sintassi LDAP per le impostazioni di connessione:

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

3. Mappare i profili utente di Acrobat Connect Pro e della directory LDAP.

Scegliete la scheda Mappatura profilo utente, immettete i valori necessari e fate clic su Salva.

Campo	Valore predefinito	Descrizione
Login	Nessun valore predefinito.	L'attributo login del servizio di directory.
Nome	Nessun valore predefinito.	L'attributo nome del servizio di directory.
Cognome	Nessun valore predefinito.	L'attributo cognome del servizio di directory.
E-mail	Nessun valore predefinito.	L'attributo e-mail del servizio di directory.

Se avete definito campi personalizzati, questi vengono aggiunti alla schermata Mappatura profilo utente. In questo esempio, un profilo utente Acrobat Connect Pro viene mappato su un profilo utente LDAP Active Directory; NetworkLogin (accesso alla rete) è un campo personalizzato.

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

4. (Facoltativo) Aggiungere un ramo utente.

Fate clic su **Aggiungi** per aggiungere informazioni utente da un determinato ramo della società. Immettete valori nei campi relativi al ramo e al filtro e fate clic su **Salva**.

Per importare utenti da rami secondari, selezionate **True (Vero)** nel menu **Ricerca sottostruttura**; in caso contrario, selezionate **False (Falso)**.

Per ulteriori informazioni, consultate [“Informazioni sulla struttura di directory LDAP”](#) a pagina 30.

Campo	Valore predefinito	Note/attributo LDAP
DN ramo	Nessun valore predefinito.	DN (nome distinto) del nodo radice del ramo. Viene visualizzato un collegamento al ramo selezionato.
Filtro	Nessun valore predefinito.	La stringa di filtro della query.
Ricerca nella sottostruttura	True	True o False. Il valore True avvia la ricerca ricorsiva in tutte le sottostrutture del ramo.

5. Mappare i profili dei gruppi di Acrobat Connect Pro e della directory LDAP.

Selezionate la scheda **Mappatura profilo del gruppo**, immettete i valori necessari e fate clic su **Salva**.

***Nota:** i profili dei gruppi di Acrobat Connect Pro non supportano i campi personalizzati.*

Campo	Valore predefinito	Note/attributo LDAP
Nome gruppo	Nessun valore predefinito.	L'attributo nome gruppo del servizio di directory.
Membro del gruppo	Nessun valore predefinito.	L'attributo membro del gruppo del servizio di directory.

Di seguito è riportata la mappatura tra gli attributi per voci di gruppi LDAP e un profilo gruppo di Acrobat Connect Pro:

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

6. (Facoltativo) Aggiungere un ramo gruppo.

Fate clic su **Aggiungi** per aggiungere informazioni utente da un determinato ramo dell'organizzazione. Immettete valori nei campi relativi al ramo e al filtro e fate clic su **Salva**.

Per importare gruppi da rami secondari, selezionate **True (Vero)** nel menu **Ricerca sottostruttura**; in caso contrario, selezionate **False (Falso)**.

Per ulteriori informazioni, consultate [“Informazioni sulla struttura di directory LDAP”](#) a pagina 30.

Campo	Valore predefinito	Note/attributo LDAP
DN ramo	Nessun valore predefinito.	DN (nome distinto) del nodo radice del ramo. Ogni ramo dell'organizzazione ha un attributo DN LDAP specifico. Viene visualizzato un collegamento al ramo selezionato.
Filtro	Nessun valore predefinito.	La stringa di filtro della query.
Ricerca nella sottostruttura	True	Un valore booleano pari a <code>true</code> o <code>false</code> . Il valore <code>true</code> avvia la ricerca ricorsiva in tutte le sottostrutture del ramo.

Di seguito è riportato un esempio di sintassi LDAP per l'aggiunta di un ramo all'organizzazione e la definizione dei gruppi corrispondenti:

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

7. Immettere le impostazioni di autenticazione.

Selezionate la scheda Impostazioni autenticazione. Per autenticare gli utenti Acrobat Connect Pro rispetto al servizio directory dell'organizzazione, selezionate Abilita autenticazione directory LDAP. Se non la selezionate, Acrobat Connect Pro usa l'autenticazione nativa (le credenziali utenti registrate nel database Acrobat Connect Pro).

Se selezionate Abilita fall-back Connect Pro per autenticazione directory LDAP non riuscita, Acrobat Connect Pro usa l'autenticazione nativa.

***Nota:** questo risulta utile in caso di problemi temporanei di connessione LDAP in rete. Tuttavia, le credenziali LDAP possono essere diverse dalle credenziali presenti nel database Acrobat Connect Pro.*

Per aggiungere gli utenti che si collegano per la prima volta al server Connect Pro se l'autenticazione LDAP ha esito positivo, selezionate Crea account utente Acrobat Connect Pro dopo l'autenticazione della directory LDAP. Se tutti gli utenti presenti nel servizio directory possono usare Acrobat Connect Pro, lasciate questa opzione selezionata e, come tipo di account, selezionate Interno. Per ulteriori informazioni, consultate “[Utenti e gruppi interni ed esterni](#)” a pagina 31.

Per creare un ID di login in Acrobat Connect Pro e inserire gli utenti nei gruppi specificati al primo login in Acrobat Connect Pro, selezionate Abilita iscrizione di gruppo solo per il primo login. Immettete i gruppi nel campo dei Nomi gruppo.

8. Pianificare la sincronizzazione.

Selezionate la scheda Impostazioni sincronizzazione. Nella schermata Impostazioni sincronizzazione selezionate la casella di controllo Attiva sincronizzazione pianificata per pianificare la sincronizzazione una volta al giorno, alla settimana o al mese a una determinata ora. Per ulteriori informazioni, consultate “[Procedure consigliate per la sincronizzazione](#)” a pagina 35.

Potete inoltre eseguire la sincronizzazione manuale nella schermata Azioni sincronizzazione.

9. Impostare criteri per la password e criteri di eliminazione.

Selezionate la scheda Impostazioni criteri, scegliete i criteri di impostazione password e i criteri di eliminazione e quindi fate clic su Salva. Per ulteriori informazioni sui criteri per la password, consultate “[Gestire le password](#)” a pagina 35.

***Nota:** se durante la sincronizzazione selezionate l'opzione Elimina utenti e gruppi [...], tutti gli utenti esterni che sono stati eliminati dal server LDAP vengono eliminati anche dal server di Acrobat Connect Pro.*

10. Visualizzare l'anteprima della sincronizzazione.

Selezionate la scheda Azioni sincronizzazione. Nella sezione Anteprima sincronizzazione directory fate clic su Anteprima. Per ulteriori informazioni, consultate “[Procedure consigliate per la sincronizzazione](#)” a pagina 35.

Gestire le password

Se non abilitate l'autenticazione LDAP, dovete scegliere in che modo gli utenti vengono autenticati da Acrobat Connect Pro.

Quando Acrobat Connect Pro importa informazioni utente da una directory esterna, non importa la password di rete dell'utente. Dovete pertanto implementare un altro metodo per la gestione delle password degli utenti importati nella directory di Acrobat Connect Pro.

Notificare gli utenti per l'impostazione di una password

Nella schermata Impostazioni criteri della scheda Impostazioni sincronizzazione potete scegliere di inviare un messaggio e-mail agli utenti importati con un collegamento che consente loro di impostare una password.

Impostare la password su un attributo LDAP

Potete scegliere di impostare la password iniziale di un utente importato sul valore di un attributo nella voce di directory dell'utente. Ad esempio, se la directory LDAP include l'ID dipendente come campo, potete impostare la password iniziale degli utenti sul relativo ID dipendente. Dopo che gli utenti hanno eseguito l'accesso usando questa password, possono modificarla.

Procedure consigliate per la sincronizzazione

In qualità di amministratore potete sincronizzare Acrobat Connect Pro con la directory LDAP esterna in due modi:

- Potete pianificare la sincronizzazione in modo che venga eseguita a intervalli regolari.
- Potete eseguire una sincronizzazione manuale per sincronizzare immediatamente la directory di Acrobat Connect Pro con la directory LDAP dell'organizzazione.

Prima di importare utenti e gruppi in una sincronizzazione iniziale, è consigliabile usare un browser LDAP per verificare i parametri di connessione. I seguenti browser sono disponibili online: LDAP Browser/Editor e LDAP Administrator.

Importante: non riavviate il server LDAP o eseguite processi paralleli durante la sincronizzazione. Ciò potrebbe infatti causare l'eliminazione di gruppi e utenti da Acrobat Connect Pro.

Sincronizzazioni pianificate

Le sincronizzazioni pianificate sono consigliate perché garantiscono che Acrobat Connect Pro disponga di un quadro aggiornato degli utenti e dei gruppi importati dalla directory LDAP dell'organizzazione.

Se importate un numero elevato di utenti e gruppi, la sincronizzazione iniziale può richiedere notevoli risorse. In questo caso è consigliabile pianificare la sincronizzazione iniziale in modo che venga eseguita in un periodo di lavoro meno intenso, ad esempio di notte. (In alternativa, potete eseguire manualmente la sincronizzazione iniziale.)

Per configurare la sincronizzazione pianificata, usate la schermata Impostazioni sincronizzazione > Impostazioni pianificazione nella console di gestione applicazione.

Quando viene eseguita la sincronizzazione, Acrobat Connect Pro confronta le voci di directory LDAP con le voci di directory di Acrobat Connect Pro e importa solo le voci che contengono almeno un campo modificato.

Anteprima della sincronizzazione

Prima di importare utenti e gruppi in una sincronizzazione iniziale, Adobe consiglia di verificare le mappature mediante l'anteprima della sincronizzazione. Nell'anteprima gli utenti e i gruppi non vengono effettivamente importati ma eventuali errori vengono registrati. Potete quindi esaminare questi errori per diagnosticare i problemi di sincronizzazione.

Per accedere ai registri della sincronizzazione, usate la schermata Registri sincronizzazione. Ogni riga del registro indica un evento della sincronizzazione; la sincronizzazione genera almeno un evento per ogni entità (utente o gruppo) elaborata. Se durante l'anteprima vengono generati avvisi o errori, questi vengono elencati in un secondo registro di avvisi.

Valori del file di registro

I registri di sincronizzazione contengono valori in formato separato da virgole. Nelle seguenti tabelle con *principal* (entità) si fa riferimento a voci di utenti e gruppi. I seguenti valori sono inclusi nelle voci di registro:

Campo	Descrizione
Date	Il valore data-ora formattato, con indicazione dei millisecondi. Il formato è <i>yyyyMMdd'T'HHmms.SSS</i> .
Principal ID	Il nome del gruppo o di login.
Principal type	Un solo carattere: U per utente, G per gruppo.
Evento	L'azione intrapresa o la condizione rilevata.
Detail	Informazioni dettagliate sull'evento.

Nella seguente tabella vengono descritti i diversi tipi di evento che possono essere inclusi nei file di registro di sincronizzazione:

Evento	Descrizione	Dettagli
add	L'entità è stata aggiunta ad Acrobat Connect Pro.	Un pacchetto XML ridotto che descrive i campi aggiornati mediante una serie di coppie di tag nel formato <code><fieldname>value</fieldname></code> (ad esempio <code><first-name>Joe</first-name></code>). Il nodo padre e i campi non aggiornati vengono omissi.
update	L'entità è un utente esterno e alcuni campi sono stati aggiornati.	
update-members	L'entità è un gruppo esterno e le entità sono state aggiunte o rimosse dall'appartenenza al gruppo.	Un pacchetto XML ridotto che descrive i membri aggiunti e rimossi. Il nodo padre viene omissi: <code><add>ID list</add></code> <code><remove>ID list</remove></code> L'elenco di ID è una serie di pacchetti <code><id>principal ID</id></code> in cui <code>principal ID</code> è un ID che viene elencato nella colonna Principal ID, ad esempio un login utente o un nome di gruppo. Se non ci sono membri di un elenco di ID, il nodo padre viene riportato come <code><add/></code> o <code><remove/></code> .
delete	L'entità è stata eliminata da Acrobat Connect Pro.	
up-to-date	L'entità è un'entità esterna in Acrobat Connect Pro ed è già sincronizzata con la directory esterna. Non sono state apportate modifiche.	Un utente o un gruppo creato in Acrobat Connect Pro viene considerato come entità interna. Un utente o un gruppo creato dal processo di sincronizzazione viene considerato come entità esterna.

Evento	Descrizione	Dettagli
make-external	L'entità è un'entità interna in Acrobat Connect Pro ed è stata convertita in un'entità esterna.	Questo evento consente alla sincronizzazione di modificare o eliminare l'entità ed è in genere seguito da un altro evento che esegue l'una o l'altra operazione. Questo evento viene registrato nel registro di avvisi.
warning	Si è verificato un evento di livello avviso.	Un messaggio di avviso.
error	Si è verificato un errore.	Messaggio di eccezione Java.

Informazioni su LDAPS

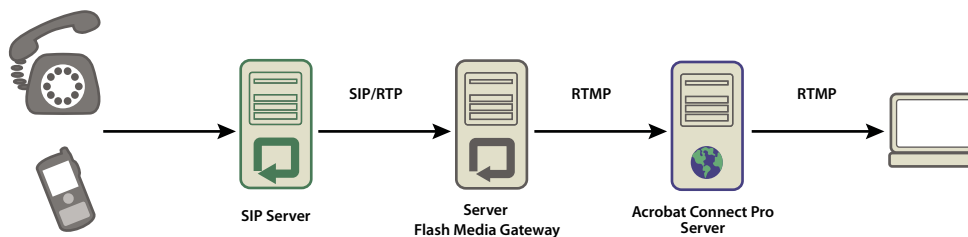
Acrobat Connect Pro supporta in modo nativo *LDAPS*, il protocollo sicuro LDAP. Il server di directory LDAP deve fornire connettività SSL. Per la connessione sicura a un server di directory LDAP, usate il protocollo LDAPS nell'URL della connessione, come segue: `ldaps://esempioServerDirectory:NumeroPorta`.

Implementazione di Universal Voice

Flusso di lavoro per l'implementazione di Universal Voice

Nota: Per un confronto tra Universal Voice e gli adattatori per telefonia integrata, consultate [“Opzioni di audioconferenza Connect Pro”](#) a pagina 13.

Connect Pro Universal Voice utilizza un componente denominato Flash Media Gateway per ricevere l'audio dai server SIP. L'audio fluisce in una sola direzione, da un server SIP alle stanze riunioni di Connect Pro. Installate Flash Media Gateway e configuratelo in modo da poter comunicare con un server SIP. Il server SIP può essere installato su un'infrastruttura della vostra azienda o di terzi. (I fornitori SIP sono denominati anche *fornitori VoIP*).



I flussi audio del telefono attraversano un server di audioconferenza (non nell'immagine), un server SIP e Flash Media Gateway, quindi raggiungono la stanza riunioni di Connect Pro.

Seguite questo flusso di lavoro per implementare la soluzione Universal Voice:

- 1 Per installare e configurare Universal Voice, dovete disporre dei seguenti elementi:
 - Connect Pro Server 7.5
 - Credenziali del fornitore SIP
- 2 Installate Flash Media Gateway.

Flash Media Gateway può essere installato sullo stesso computer di Connect Pro Server o su un computer dedicato. Potete implementare Flash Media Gateway su un solo computer oppure su un cluster di server. Il programma di installazione di Flash Media Gateway è compreso nel programma di installazione di Connect Pro Server. Consultate [“Esegui il programma di installazione”](#) a pagina 14.

3 Configurate Flash Media Gateway per la connessione a un server SIP.

Al termine dell'installazione, viene avviata la console di gestione applicazione. (Per accedere alla console di gestione applicazione potete utilizzare anche il sito <http://localhost:8510/console>.) Utilizzate la console per configurare Flash Media Gateway per la connessione a un server SIP. Consultate [“Configurazione di Acrobat Connect Pro con la procedura guidata della console di gestione applicazione”](#) a pagina 15.

4 Aprite le porte. Consultate [“Porte e protocolli Flash Media Gateway”](#) a pagina 38.

Se un firewall utilizza il NAT, consultate [“Configurazione di Flash Media Gateway per comunicare attraverso un firewall che usa NAT”](#) a pagina 39.

5 Per installare Flash Media Gateway su un cluster di computer, consultate [“Implementare Flash Media Gateway su un cluster di server”](#) a pagina 42.

6 Per creare una sequenza di composizione e testare la connessione audio, consultate www.adobe.com/go/learn_cnn_uvconfig_it.

7 Se in una riunione di Connect Pro l'audio non si stente, consultate [“Risoluzione dei problemi relativi a Universal Voice”](#) a pagina 43.

Porte e protocolli Flash Media Gateway

Nota: Per visualizzare un digramma del modo in cui fluiscono i dati tra fornitore SIP, Flash Media Gateway e Connect Pro Server, consultate [“Flusso di dati”](#) a pagina 7.

Flash Media Gateway riceve le richieste di Connect Pro Central Application Server sulla porta seguente:

Numero porta	Indirizzo di associazione	Protocollo
2222	*/Qualsiasi scheda	HTTP

Flash Media Gateway avvia una connessione con Flash Media Server come un normale client RTMP. Flash Media Server riceve Flash Media Gateway sulla porta seguente:

Numero porta	Indirizzo di associazione	Protocollo
8506	*/Qualsiasi scheda	RTMP

Flash Media Gateway comunica con il fornitore dell'audioconferenza mediante i protocolli SIP e RTP sulle porte seguenti:

Direzione	Regola
Da Flash Media Gateway a Internet	SRC-IP=<Server-IP>, SRC-PORT=5060, DST-IP=ANY, DST-PORT=5060
Da Internet a Flash Media Gateway	SRC-IP=ANY, SRC-PORT=5060, DST-IP=<Server-IP>, DST-PORT=5060
Da Flash Media Gateway a Internet	SRC-IP=<Server-IP>, SRC-PORT=5000_TO_6000, DST-IP=ANY, DST-PORT=ANY_HIGH_END
Da 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 indica qualunque porta prima della 1024. L'intervallo porte predefinito è compreso tra 5000 e 6000. Potete modificare questi valori nella console di gestione applicazione.

Configurazione di Flash Media Gateway per comunicare attraverso un firewall che usa NAT

Nota: Potrebbe non essere necessario eseguire questa operazione se il firewall utilizzato è SIP compatibile o SIP-aware. Inoltre, in alcuni casi il gateway a livello di applicazione (ALG) per SIP in un firewall può causare problemi. Se non riuscite a stabilire la comunicazione mediante l'ALG, disattivate l'ALG per SIP nel firewall e utilizzate la tecnica descritta in questa sezione.

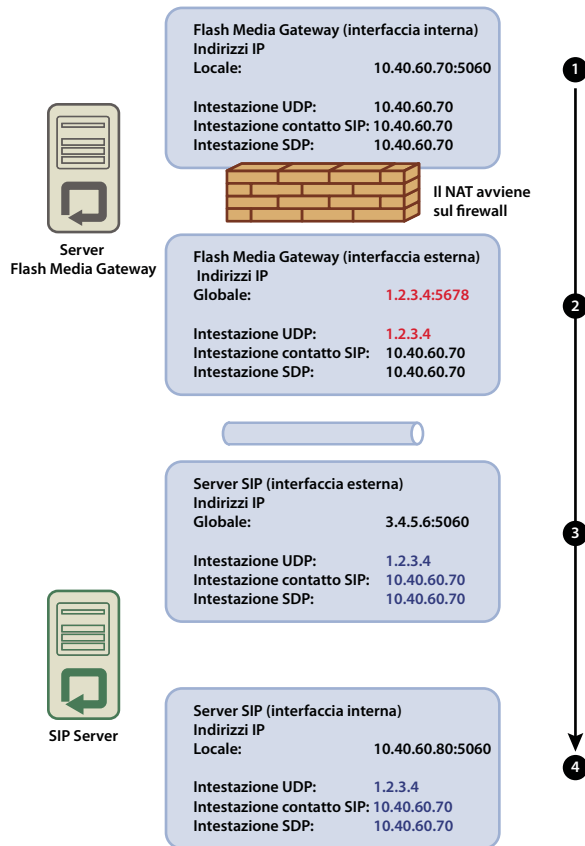
Il NAT (Network address translation, Traduzione degli indirizzi di rete) è un processo che consente alle reti di utilizzare un numero minore di indirizzi IP esterni e di oscurare quelli interni. Il NAT cambia l'indirizzo IP e il numero di porta dei pacchetti che escono da una rete. Gli indirizzi IP interni vengono modificati in indirizzi IP esterni. Il NAT inoltre cerca di indirizzare agli indirizzi IP corretti le risposte inviate all'indirizzo IP esterno.

Quando Flash Media Gateway è protetto da un firewall che utilizza il NAT, potrebbe non riuscire a ricevere i pacchetti provenienti dal server SIP. Il NAT modifica l'indirizzo IP locale e dell'intestazione UDP (origine del pacchetto) in modo che corrisponda all'indirizzo IP esterno.

L'indirizzo IP dell'intestazione UDP è uguale all'indirizzo IP esterno di Flash Media Gateway. Pertanto, se il server SIP utilizza l'indirizzo IP dell'intestazione UDP per inviare una risposta, quest'ultima riesce a trovare Flash Media Gateway.

L'indirizzo IP dell'intestazione del contatto è uguale all'indirizzo IP locale di Flash Media Gateway. Pertanto, se il server SIP utilizza l'indirizzo IP dell'intestazione del contatto per inviare una risposta, quest'ultima non riesce a trovare Flash Media Gateway. L'indirizzo IP locale è protetto da un firewall e non è visibile al server SIP.

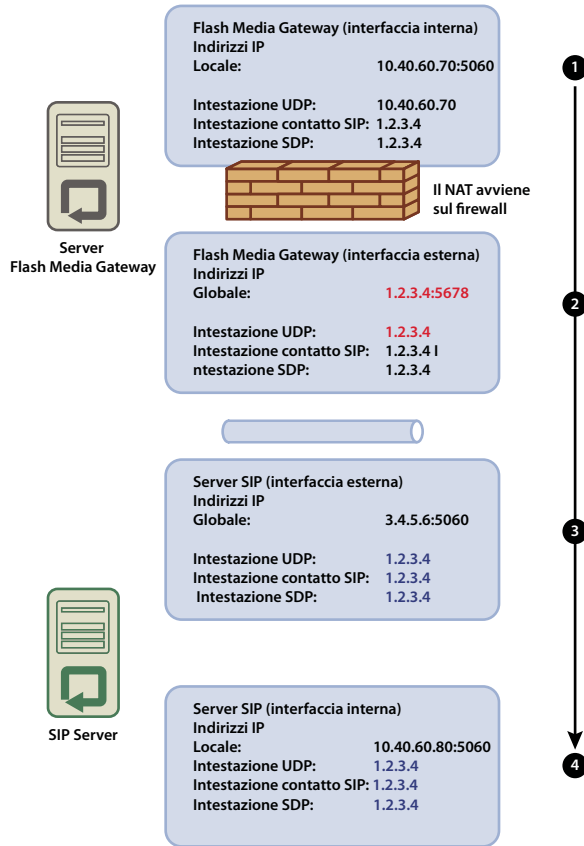
Nell'immagine seguente è mostrato come il NAT modifica gli indirizzi IP sul firewall:



Il NAT modifica l'indirizzo IP

- 1 Flash Media Gateway (interfaccia interna). L'intestazione UDP (indirizzo IP dell'origine del pacchetto) e l'indirizzo IP dell'intestazione del contatto SIP corrispondono all'indirizzo IP locale.
- 2 Flash Media Gateway (interfaccia esterna). Il NAT modifica l'indirizzo IP dell'intestazione UDP in indirizzo IP globale.
- 3 Server SIP (interfaccia esterna). Il pacchetto cerca l'interfaccia globale sul server SIP. Per raggiungere l'interfaccia interna, viene inoltrata direttamente la porta. Se la porta non viene inoltrata, il pacchetto si perde e le comunicazioni si interrompono.
- 4 Server SIP (interfaccia interna). Il pacchetto viene elaborato quando raggiunge l'interfaccia. Se il server SIP utilizza l'indirizzo IP dell'intestazione UDP per inviare una risposta, quest'ultima riesce a raggiungere Flash Media Gateway. Se il server SIP utilizza l'indirizzo IP dell'intestazione del contatto, la risposta non riesce a raggiungere Flash Media Gateway.

Nell'immagine seguente è mostrata una configurazione valida in cui l'indirizzo IP dell'intestazione del contatto SIP è lo stesso dell'indirizzo IP esterno di Flash Media Gateway. La modifica consente ai pacchetti di essere reinstradati dal server SIP a Flash Media Gateway.



Configurazione valida per le comunicazioni

Per verificare se Flash Media Gateway riesce a ricevere i pacchetti da un server SIP, effettuate quanto segue:

- 1 In Flash Media Gateway, aprite il file *RootInstallationFolder/conf/sip.xml* in un editor di testi. (La cartella di installazione principale predefinita è *C:\Program Files\Adobe\Flash Media Gateway*).
 - a Create un tag `<globalAddress>` sotto il tag `<Profile>`. Inserite l'indirizzo IP esterno di Flash Media Gateway, nel modo seguente:

```

...
<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>
...

```

In un cluster, è necessario che ciascun server Flash Media Gateway abbia un indirizzo IP esterno unico.

Importante: Se l'indirizzo IP esterno è dinamico, è necessario riconfigurare Flash Media Gateway ogni volta che l'indirizzo IP esterno cambia.

- b** Riavviate il servizio Flash Media Gateway. Consultate [“Avviare e arrestare Flash Media Gateway”](#) a pagina 89.
- 2** Sul firewall tra il server Flash Media Gateway e il server SIP, eseguite il tunneling direttamente dalla porta SIP (per impostazione predefinita 5060) e dalle porte vocali RTP (per impostazione predefinita da 5000 a 6000) al server Flash Media Gateway. Le porte aperte sul firewall devono corrispondere a quelle aperte sul server Flash Media Gateway.

Nota: i server possono comunicare senza tunneling. Tuttavia, senza questo, le chiamate potrebbero disconnettersi all'improvviso, specialmente dopo una durata prolungata.

Implementare Flash Media Gateway su un cluster di server

Per implementare un cluster di server, installate Flash Media Gateway e Connect Pro Server ognuno sui propri computer. Non installateli sugli stessi computer.

Quando Flash Media Gateway viene implementato su un cluster di server, Connect Pro Server è in grado di gestire il bilanciamento del carico e il failover. Connect Pro Edge Server non richiede altre configurazioni.

- 1** Eseguite il programma di installazione su ciascun server del cluster e selezionate l'installazione di Flash Media Gateway. Consultate [“Eseguire il programma di installazione”](#) a pagina 14.

Nota: Per informazioni sull'implementazione di Connect Pro Server in un cluster, consultate [“Implementare un cluster di server Acrobat Connect Pro”](#) a pagina 23.

- 2** Su un server Connect Pro, aprite la console di gestione applicazione all'indirizzo <http://localhost:8510/console>.
- 3** Selezionate Impostazioni Flash Media Gateway > Impostazioni host FMG e fate clic su Aggiungi per aggiungere altri server Flash Media Gateway e configurarli. Consultate [“Configurazione di Acrobat Connect Pro con la procedura guidata della console di gestione applicazione”](#) a pagina 15.

Nota: Utilizzate la console di gestione applicazione su un server per inserire i parametri di configurazione per tutti i server del cluster. La console di gestione applicazione invia le impostazioni a tutti i server del cluster.

Opzioni avanzate di configurazione Flash Media Gateway

Per le opzioni di configurazione avanzate, consultate la documentazione di [Flash Media Gateway](#).

Risoluzione dei problemi relativi a Universal Voice

Se in un'audioconferenza Universal Voice in una stanza riunioni l'audio non funziona, effettuate quanto segue:

- 1 Verificate che il volume sul computer sia attivato. Se utilizzate delle cuffie, verificate che siano connesse alla presa di uscita.
- 2 Eseguite una prova della sequenza di composizione. Consultate [Test della sequenza di composizione](#).
- 3 Verificate che Flash Media Gateway sia configurato correttamente:
 - a Aprite la console di gestione applicazione (<http://localhost:8510/console>) su Connect Pro Server e fate clic su Impostazioni di Flash Media Gateway > Impostazioni host FMG. Lo stato di ciascun Flash Media Gateway deve risultare "Attivo".
 - b In caso contrario, aprite il file *RootInstallationFolder/custom.ini*. Verificate che siano presenti le voci seguenti:

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

Se le voci non sono presenti, inseritele e riavviate Connect Pro Central Application Server.
- 4 Contattate il supporto Adobe visitando il sito Web all'indirizzo www.adobe.com/go/connect_licensed_programs_it.

Uso di adattatori per telefonia integrata

Installazione di adattatori per telefonia integrata

Gli adattatori per telefonia integrata sono estensioni Java che consentono a Connect Pro di connettersi a un bridge audio. Potete installare quanti adattatori per telefonia integrata desiderate. La guida all'installazione è disponibile nel [Centro di assistenza di Connect Pro](#). Gli adattatori per telefonia sono disponibili sul sito adobe.com.

Configurazione di Universal Voice per gli adattatori per telefonia integrata

Potete configurare Universal Voice per tutti gli adattatori per telefonia integrata installati su Connect Pro Server. Quando si configura un adattatore per telefonia integrata per Universal Voice, potete trasmettere l'audioconferenza ai partecipanti VoIP in una stanza riunioni.

- 1 Aprite il file *RootInstallationFolder\appserv\conf\telephony-settings.xml* in un editor di testo.
- 2 Nel file XML, definite la sequenza di composizione per il fornitore di audioconferenza. Nell'esempio seguente è utilizzata la sequenza di composizione per l'adattatore Premiere:

Nota: i parametri forniti dall'utente sono racchiusi tra parentesi quadre ([]), mentre quelli dell'adattatore tra parentesi graffe ({}).

```
<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>
```

Nell'esempio seguente è utilizzata la sequenza di composizione per l'adattatore 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	Descrizione
conf-num	Il numero di telefono per partecipare all'audioconferenza. È necessario che questo sia il primo elemento della sequenza di composizione. È consentito un solo elemento <conf-num>. Il valore tra parentesi graffe {} è fornito dall'adattatore.
delay	Un ritardo nella sequenza di composizione, in millisecondi.
dtmf	Un tono DTMF (dual-tone multi-frequency). Un valore DTMF può essere costituito da un qualunque numero o una lettera di una tastiera telefonica, inclusi * and #.

- 3 Convalidare e salvare il file XML.
- 4 Riavviate Connect Pro Central Application Server.

Per ulteriori informazioni sulla configurazione degli adattatori per telefonia, consultate *Usa degli adattatori per telefonia* nel [Centro di assistenza di Connect Pro](#).

Nascondere l'utente Flash Media Gateway nell'elenco dei partecipanti

Nota: Questa sezione è valida solo per gli adattatori per telefonia integrata configurati per Universal Voice.

Quando una stanza riunioni si connette con Flash Media Gateway, la connessione figura come utente nell'elenco dei partecipanti. Per nascondere l'utente Flash Media Gateway nell'elenco dei partecipanti, configurate il numero di audioconferenza nel file custom.ini. Utilizzate lo stesso numero per tutti i computer del cluster. Il numero di audioconferenza può essere richiesto al fornitore SIP. Oppure, se l'amministratore di account ha configurato un fornitore audio in Connect Pro Central, il numero si può rintracciare nella stanza riunioni.

1 Aprite il file \breeze\custom.ini in un editor di testo.

2 Aggiungete il seguente parametro:

```
UV_NUMBER={audio_conference_telephone_number}
```

```
// Example:
```

```
UV_NUMBER=4155551212
```

3 Salvate e chiudete il file custom.ini.

4 Per riavviare il server, procedete nel modo seguente:

- a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server > Arresta Connect Pro Central Application Server.
- b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server > Avvia Connect Pro Central Application Server.

Configurazione della memorizzazione condivisa

Informazioni sulla memorizzazione condivisa

Potete usare la console di gestione applicazione per configurare Acrobat Connect Pro in modo che usi periferiche NAS e SAN per la gestione della memorizzazione dei contenuti. Per “contenuto” si intende qualsiasi file pubblicato su Acrobat Connect Pro, ad esempio corsi, file SWF, PPT o PDF e registrazioni archiviate.

Di seguito sono riportate configurazioni possibili per la memorizzazione condivisa:

- Il contenuto viene copiato sulla periferica di memorizzazione esterna primaria, quindi trasferito alla cartella del contenuto di ogni server Acrobat Connect Pro quando necessario. Se necessario, i contenuti più vecchi vengono eliminati dalla cartella dei contenuti del server per fare posto ai contenuti più nuovi. Questa configurazione libera risorse sul server applicazioni e ciò è particolarmente utile in un cluster di grandi dimensioni. (Immettete un valore nelle caselle Memorizzazione condivisa e Dimensione cache contenuto.)
- Il contenuto viene copiato su tutti i server e sulla periferica di memorizzazione esterna primaria. Questa configurazione è consigliata per cluster di piccole dimensioni, a meno che non disponiate di grandi quantità di contenuto a cui gli utenti accedono in modo casuale. (Immettete un valore nella casella Memorizzazione condivisa e lasciate vuota la casella Dimensione cache contenuto.)

Nota: se avete un cluster Acrobat Connect Pro e non configurate periferiche di memorizzazione condivisa, il cluster funziona in modalità di mirroring totale (il contenuto pubblicato su Acrobat Connect Pro viene copiato su tutti i server) e il contenuto non viene mai rimosso automaticamente dai server.

Configurare la memorizzazione condivisa

Se state configurando la memorizzazione condivisa per un server Acrobat Connect Pro, seguite le istruzioni della prima attività. Se state configurando la memorizzazione condivisa per un cluster, seguite le istruzioni della prima attività per un computer del cluster e quindi le istruzioni della seconda attività per tutti gli altri computer del cluster.

Altri argomenti presenti nell’Aiuto

“[Periferiche di memorizzazione del contenuto supportate](#)” a pagina 4

“[Implementare un cluster di server Acrobat Connect Pro](#)” a pagina 23

Configurare la memorizzazione condivisa

Prima di iniziare Acrobat Connect Pro deve essere configurato senza memorizzazione condivisa ed eseguito su un server.


- 1 Configurate un volume condiviso su una periferica di memorizzazione esterna.

Se un volume condiviso ha nome utente e password, tutti i volumi condivisi devono usare lo stesso nome utente e la stessa password.

- 2 (Facoltativo) Se state aggiornando un server Acrobat Connect Pro esistente per l’uso di volumi di memorizzazione condivisa, dovete copiare il contenuto da uno dei server esistenti al volume condiviso.

- a Arrestate il server (Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server e Arresta Connect Pro Meeting Server).

- b Copiate la cartella `[root_install_dir]\content\7` sul volume condiviso creato al passaggio 1.

 *Alcuni computer di un cluster possono avere contenuto supplementare. Acrobat Connect Pro non può usare questi file, ma se desiderate copiarli sul volume condiviso a scopo di archiviazione, potete creare ed eseguire uno script che confronta il contenuto di ogni computer con il contenuto del volume condiviso.*

- c Avviate Acrobat Connect Pro (Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Meeting Server e Avvia Connect Pro Central Application Server).

- 3 In Acrobat Connect Pro, scegliete Start > Pannello di controllo > Strumenti di amministrazione > Servizi per aprire la finestra Servizi; selezionate Adobe Connect Enterprise Server ed eseguite le seguenti operazioni:

- a Fate clic con il pulsante destro del mouse e scegliete Proprietà.

- b Selezionate la scheda Connessione.

- c Selezionate Account e se il volume condiviso ha un nome utente e una password specificateli e fate clic su Applica.

- 4 Riavviate Acrobat Connect Pro (solo il server applicazione).

- a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.

- b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

- 5 Aprite la console di gestione applicazione (Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Configura Connect Pro Server 7).

- 6 Nella scheda Impostazioni applicazione selezionate la scheda Impostazioni server, andate alla sezione Impostazioni memorizzazione condivisa e immettete un percorso nella casella Memorizzazione condivisa (ad esempio `\\storage`).

Se la periferica di memorizzazione primaria è piena, potete aggiungere un’altra periferica alla posizione primaria. Separate i percorsi mediante punto e virgola (;): `\\new-storage;\\storage`.

Nota: la scrittura, ovvero la copia nella cartella di memorizzazione, viene eseguita solo per la prima cartella. La lettura, ovvero la copia dalla cartella di memorizzazione, viene eseguita in sequenza a partire dalla prima cartella finché non viene trovato il file.

- 7 (Facoltativo) Per configurare la cartella del contenuto su Acrobat Connect Pro in modo che funga da cache (gli elementi vengono rimossi automaticamente quando è necessario spazio e ripristinati su richiesta), immettete un valore nella casella Dimensione cache contenuto.

La dimensione della cache del contenuto è una percentuale dello spazio su disco da usare come cache. Adobe consiglia di impostare un valore compreso tra 15 e 50 perché la dimensione della cache può aumentare superando il valore impostato. Gli elementi della cache vengono eliminati solo dopo che il contenuto visualizzato è scaduto (24 ore dopo l'ultima visualizzazione).

- 8 Fate clic su Salva e chiudete la console di gestione applicazione.
- 9 Riavviate Acrobat Connect Pro (solo il server applicazione).
 - a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.
 - b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

Configurare la memorizzazione condivisa per altri server del cluster

- 1 Installate Acrobat Connect Pro ma non avviatelo. Se Acrobat Connect Pro è installato e già in esecuzione, arrestatelo.
- 2 In Acrobat Connect Pro, scegliete Start > Pannello di controllo > Strumenti di amministrazione > Servizi per aprire la finestra Servizi; selezionate Adobe Connect Enterprise Server ed eseguite le seguenti operazioni:
 - a Fate clic con il pulsante destro del mouse e scegliete Proprietà.
 - b Selezionate la scheda Connessione.
 - c Selezionate Account e se il volume condiviso ha un nome utente e una password specificateli e fate clic su Applica.
- 3 Avviate Acrobat Connect Pro.
 - a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Meeting Server.
 - b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.
- 4 (Facoltativo) Se state installando Acrobat Connect Pro per la prima volta, seguite i passaggi descritti in [“Implementare un cluster di server Acrobat Connect Pro”](#) a pagina 23.
- 5 Fate clic su Salva e chiudete la console di gestione applicazione.

Configurazione delle impostazioni di notifica dell'account

Aggiunta dei collegamenti Assistenza e Stato al menu Guida

Gli amministratori di account possono aggiungere dei collegamenti alla pagina Stato e alla pagina Assistenza nel menu Guida delle stanze riunioni. Tali collegamenti visualizzano le pagine HTML da voi indicate. La pagina Stato può fornire informazioni sullo stato attuale del sistema Acrobat Connect Pro, mentre la pagina Assistenza può offrire informazioni su come ottenere assistenza nell'uso di Acrobat Connect Pro. Se tali collegamenti non vengono definiti, non saranno disponibili nel menu Guida.

- 1 Aprite il file `RootInstallationFolder\custom.ini` in un editor di testo.
- 2 Per modificare il collegamento alla pagina Stato, impostate `STATUS_PAGE = "http://connect.mycompany.com/status.html"`.
- 3 Per modificare il collegamento alla pagina Assistenza, impostate `SUPPORT_PAGE="http://connect.mycompany.com/support.html"`.

Gli URL possono essere assoluti o relativi al server riunioni. Gli URL assoluti devono iniziare con "http://" o "https://". Gli URL relativi con "/".

- 4 Per riavviare Acrobat Connect Pro effettuate le operazioni seguenti:
 - a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.
 - b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

Impostare l'ora di invio dei rapporti mensili

Acrobat Connect Pro invia un messaggio e-mail al mese con informazioni sulla capacità dell'account. Per impostazione predefinita, i rapporti mensili sulla capacità dell'account vengono inviati alle ore 3:00 UTC. Per cambiare l'ora di invio, potete aggiungere parametri al file `custom.ini` e importare i valori desiderati.

Per ulteriori informazioni sulla configurazione delle notifiche dell'account in Connect Pro Central, consultate il capitolo "Amministrazione di Acrobat Connect Pro" nella guida *Utilizzo di Adobe Acrobat Connect Pro 7.5*, disponibile online all'indirizzo www.adobe.com/go/connect_documentation_it.

- 1 Aprite il file `CartellaPrincipaleInstallazione\custom.ini` e aggiungete i seguenti parametri con i valori desiderati:

THRESHOLD_MAIL_TIME_OF_DAY_HOURS L'ora UTC alla quale viene inviato il rapporto mensile riguardo le notifiche della capacità. Il valore deve essere un numero intero compreso tra 0 e 23. Questo parametro può essere impostato solo nel file `custom.ini`; non è possibile impostarlo in Connect Pro Central.

THRESHOLD_MAIL_TIME_OF_DAY_MINUTES I minuti dell'ora alla quale viene inviato il rapporto mensile riguardo le notifiche della capacità. Il valore deve essere un numero intero compreso tra 0 e 59. Questo parametro può essere impostato solo nel file `custom.ini`; non è possibile impostarlo in Connect Pro Central.

Nota: se i parametri precedenti non vengono specificati o se sono specificati in modo errato, il messaggio e-mail viene inviato alle 3:00 (UTC).

Seguono valori di esempio che possono essere aggiunti al file `custom.ini`:

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

- 2 Per riavviare Acrobat Connect Pro effettuate le operazioni seguenti:
 - a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.
 - b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

Impostare le soglie di capacità

Gli account amministratori di Acrobat Connect Pro possono impostare soglie di capacità in Connect Pro Central. Quando l'account supera tali soglie, viene inviata una notifica. È possibile aggiungere parametri al file custom.ini che definiscono le soglie di capacità predefinite per Connect Pro Central.

Per ulteriori informazioni sulla configurazione delle notifiche dell'account in Connect Pro Central, consultate il capitolo "Amministrazione di Acrobat Connect Pro" nella guida *Utilizzo di Adobe Acrobat Connect Pro 7.5*, disponibile online all'indirizzo www.adobe.com/go/connect_documentation_it.

- 1 Aprite il file *Cartella Principale Installazione\custom.ini* e aggiungete uno o più dei seguenti parametri con i valori desiderati:

THRESHOLD_NUM_OF_MEMBERS Percentuale di soglia predefinita per la quota di Autori e Ospitanti riunioni. Il valore deve essere un numero intero divisibile per 10 compreso tra 10 e 100. Se il valore non viene specificato o se è specificato in modo errato, il valore predefinito è 80.

THRESHOLD_CONC_USERS_PER_MEETING Percentuale di soglia predefinita per la quota di Utenti simultanei a riunione. Il valore deve essere un numero intero divisibile per 10 compreso tra 10 e 100. Se il valore non viene specificato o se è specificato in modo errato, il valore predefinito è 80.

THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT Percentuale di soglia predefinita per la quota di Partecipanti alla riunione per l'account. Il valore deve essere un numero intero divisibile per 10 compreso tra 10 e 100. Se il valore non viene specificato o se è specificato in modo errato, il valore predefinito è 80.

THRESHOLD_CONC_TRAINING_USERS Percentuale di soglia predefinita per la quota di Utenti in formazione simultanei. Il valore deve essere un numero intero divisibile per 10 compreso tra 10 e 100. Se il valore non viene specificato o se è specificato in modo errato, il valore predefinito è 80.

Seguono valori di esempio che possono essere aggiunti al file 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 Per riavviare Acrobat Connect Pro effettuate le operazioni seguenti:
 - a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.
 - b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

Configurazione della conversione da PDF a SWF

Conversione PDF

Utilizzate un contenitore Condivisione in una stanza riunioni Connect Pro per condividere i documenti PDF. Ospitanti e relatori hanno la possibilità di sincronizzare la navigazione di tutti i partecipanti e utilizzare la lavagna sovrapposta per le collaborazioni. Caricate i documenti PDF nel contenitore Condivisione dal desktop o dalla libreria dei contenuti di Connect Pro. La condivisione dei documenti nel contenitore Condivisione offre i seguenti vantaggi rispetto alla condivisione dello schermo:

- Ospitanti e relatori possono precaricare e organizzare i documenti nella stanza riunioni.
- Visualizzazione di migliore qualità per tutti i partecipanti.
- Meno requisiti di larghezza di banda per partecipanti e relatori.
- Maggiore facilità di cooperazione per i relatori.
- Collaborazione più semplice con la lavagna.

Quando i documenti PDF vengono condivisi in un contenitore Condivisione, Connect Pro li converte in formato Flash. In Connect Pro Server sono disponibili alcuni parametri di configurazione per il controllo della conversione dei PDF.

Configurare la conversione da PDF a SWF

- 1 Aprite il file `RootInstallationFolder\custom.ini` in un editor di testo.
- 2 Modificate i parametri di configurazione seguenti:

Parametro	Valore predefinito	Descrizione
ENABLE_PDF2SWF	true	Un valore booleano che specifica se è abilitata o meno la conversione da PDF a SWF per il server. Impostate questo parametro su false per disabilitare la conversione per problemi di prestazioni.
PDF2SWF_PAGE_TIMEOUT	5	Il valore di intervallo di attesa per pagina, in secondi.
PDF2SWF_CONVERTER_PORTS_START	4000	Il valore più basso dell'intervallo di porte utilizzate per le conversioni da PDF a SWF.
PDF2SWF_CONVERTER_PORTS_END	4030	Il valore più alto dell'intervallo di porte utilizzate per le conversioni da PDF a SWF.
PDF2SWF_CONCURRENCY_LIMIT	3	Il numero massimo di conversioni da PDF a SWF che possono aver luogo contemporaneamente su un server delle applicazioni. Se un server delle applicazioni riceve un numero maggiore di richieste, queste vengono messe in coda.
PDF2SWF_QUEUE_LIMIT	5	Il numero massimo di conversioni da PDF a SWF che possono rimanere in coda di attesa contemporaneamente. Se un server delle applicazioni riceve un numero maggiore di richieste, l'utente riceve il messaggio "Connect Pro non ha potuto convertire il file per la visualizzazione. Riprovate più tardi." Gli amministratori nel registro visualizzano il seguente messaggio: <status code="request-retry"><exception>java.lang.Exception: Conversion Load too much on server.
PDF2SWF_TIMEOUT_NUMBER_OF_PAGES	3	Il numero massimo di pagine consentite per l'intervallo di attesa, prima dell'interruzione della conversione.

- 3 Riavviate Connect Pro Central Application Server. Consultate “[Avviare e arrestare Acrobat Connect Pro Server](#)” a pagina 87.

Integrazione con Microsoft Live Communications Server 2005 e Microsoft Office Communications Server 2007

Flusso di lavoro per configurare l'integrazione della presenza

Se integrate Acrobat Connect Pro con un server di comunicazioni in tempo reale Microsoft, gli ospitanti delle riunioni potranno vedere la presenza LCS o OCS dei partecipanti registrati nell'Elenco partecipanti e avviare con gli utenti online conversazioni basate su testo.

Per ulteriori informazioni sull'Elenco partecipanti, consultate la guida *Utilizzo di Adobe Acrobat Connect Pro 7.5*, disponibile online all'indirizzo www.adobe.com/go/connect_documentation_it.

1. Devono essere installati sia Acrobat Connect Pro Server che un server per comunicazioni.

Installate e verificate l'installazione di Acrobat Connect Pro Server e di un server di comunicazione. Acrobat Connect Pro Server supporta l'integrazione con Microsoft Live Communications Server 2005 e Microsoft Office Communications Server 2007. Consultate “[Installare Connect Pro Server e Flash Media Gateway](#)” a pagina 14 e la documentazione del server di comunicazione.

2. Configurare il server di comunicazione.

Configurate il server di comunicazione per lo scambio di dati con Acrobat Connect Pro Server Consultate “[Configurare Live Communications Server 2005 o Office Communications Server 2007](#)” a pagina 51.

3. Arrestare Connect Pro Presence Service.

Acrobat Connect Pro Server comprende Connect Pro Presence Service. Arrestate questo servizio prima di configurare Acrobat Connect Pro. Consultate “[Avviare e arrestare Connect Pro Presence Service](#)” a pagina 56.

4. Configurare Connect Pro Presence Service.

Configurate Acrobat Connect Pro in modo che possa scambiare dati con il server di comunicazione. Il server di presenza è installato in `RootInstallationFolder\presserv`. Consultate “[Configurare Connect Pro Presence Service](#)” a pagina 53.

5. Avviare Connect Pro Presence Service.

Consultate “[Avviare e arrestare Connect Pro Presence Service](#)” a pagina 56.

6. Abilitare l'elenco invitati e il contenitore Chat in Connect Pro Central.

Accedete a Connect Pro Central come amministratore. Selezionate Amministrazione > Conformità e controllo > Gestione contenitori. Deselezionate l'opzione per disabilitare l'elenco invitati e il contenitore Chat.

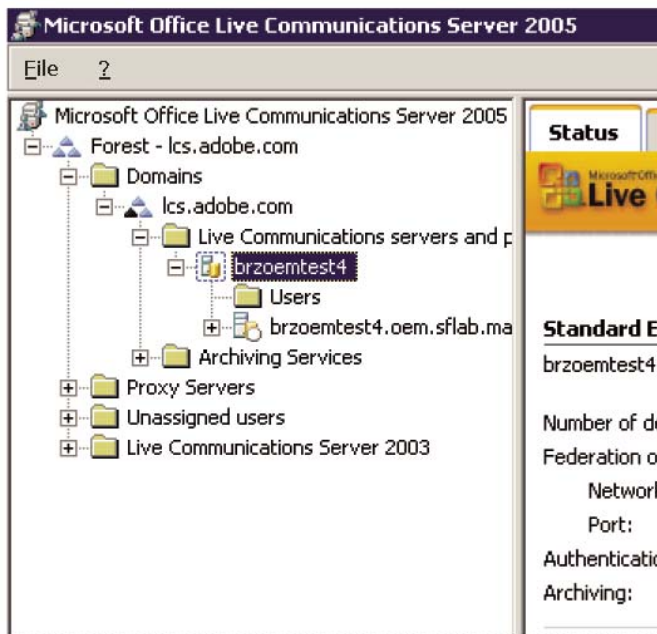
Configurare Live Communications Server 2005 o Office Communications Server 2007

- 1 Per aprire la console di configurazione, scegliete Start > Programmi > Strumenti di amministrazione > Live Communications Server 2005 o Office Communications Server 2007.

- 2 Fate clic con il pulsante destro del mouse sulla foresta, selezionate Proprietà ed effettuate le seguenti operazioni:
 - a Selezionate la scheda Federation (Federazione).
 - b Selezionate la casella Enable federation and public IM connectivity (Abilita federazione e connettività IM pubblica).
 - c Immettete l'indirizzo di rete di Acrobat Connect Pro.
 - d Immettete la porta 5072.

5072 è il numero di porta predefinito di Connect Pro Presence Service nel file \presserv\conf\lcs gw.xml.

- e Fate clic su OK.
- 3 Nel riquadro di sinistra della console di configurazione, espandete Domains, il vostro dominio, quindi i server e pool Live Communications.
- 4 Fate clic con il pulsante destro del mouse sul nome dell'host nel vostro pool e selezionate Properties (Proprietà).



- 5 Nella finestra di dialogo delle proprietà del server, effettuate una delle seguenti operazioni:
 - a Selezionate la scheda Host Authorization (Autorizzazione host). Aggiungete l'indirizzo IP di Acrobat Connect Pro. Verificate che Outbound Only (Solo in uscita) sia impostato su No, Throttle as Server (Limita come server) su Yes (Sì) e Treat as Authentication (Tratta come autenticazione) su Yes.
 - b Se davanti al server Acrobat Connect Pro è installato un sistema di bilanciamento del carico, aggiungete l'indirizzo IP di tale sistema.
 - c Fate clic su OK.
- 6 Nel riquadro di sinistra della console di configurazione, espandete il nome FQDN del vostro server e selezionate Applications (Applicazioni).

- 7 Effettuate le seguenti operazioni:
 - a Fate clic su IM URL Filter Application Setting (Impostazione filtro URL per IM). Nella finestra di dialogo delle proprietà, deselezionate Enable (Abilita). Se questa impostazione è abilitata, gli ospitanti di riunioni non possono inviare URL in messaggi immediati.
- 8 Chiudete la console di configurazione.

Configurare i client del server di comunicazione

L'integrazione di Acrobat Connect Pro con i server di comunicazione Microsoft funziona con client standard Microsoft Office Communicator 2005 (MOC 2005). I client non richiedono una particolare configurazione. Tuttavia, affinché sia possibile fare clic sugli URL delle riunioni Connect in MOC 2005, modificate la proprietà "Allow hyperlinks in an instant message" (Consenti collegamenti ipertestuali in messaggio immediato) del modello Communicator Administrative. Per ulteriori informazioni, consultate <http://technet.microsoft.com/it-it/library/bb963959.aspx>.

- 1 Selezionate Start > Esegui.
- 2 Digitate gpedit.msc nella casella Apri per aprire la finestra Group Policy (Criteri gruppo).
- 3 Fate clic per espandere Computer Configuration (Configurazione computer).
- 4 Fate clic per espandere Administrative Templates (Modelli amministrativi).
- 5 Fate clic con il pulsante destro del mouse su Microsoft Office Communicator Policy Settings (Impostazioni criteri di Microsoft Office Communicator).

***Nota:** se questo modello non è presente nella cartella Administrative Templates, aggiungetelo. Individuate Communicator.adm nel pacchetto client di Microsoft Office Communicator 2005 e copiatelo in C:\WINDOWS\inf\. Nella finestra Group Policy, fate clic con il pulsante destro del mouse su Administrative Templates, fate clic su Add/Remove Templates (Aggiungi/Rimuovi modelli), quindi su Add (Aggiungi), individuate il file e fate clic su Open (Apri).*

Configurare Connect Pro Presence Service

Completate le procedure seguenti per configurare Connect Pro Presence Service per lo scambio di dati con un server di comunicazione. Al termine, riavviate Connect Pro Central Application Server.

Definire il collegamento del gateway tra Connect Pro Presence Service e il server di comunicazione

- 1 Aprite il file `RootInstallationFolder\presserv\conf\lcs gw.xml` in un editor XML.
- 2 Modificate il file come segue, sostituendo i valori in grassetto con i valori richiesti:

```
<?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>
```

Parametro	Descrizione
<ospitante>	Dominio SIP degli utenti LCS o OCS
<bind>	Indirizzo IP del server LCS o OCS (o del sistema di bilanciamento del carico)
<area>	Dominio SIP degli utenti LCS o OCS

Configurare il file custom.ini

- 1 Aprite il file *RootInstallationFolder\custom.ini* in un editor di testo.
- 2 Immettete i seguenti parametri e valori:

Parametro	Valore
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Il valore fa distinzione tra maiuscole e minuscole.
OPN_HOST	Indirizzo di rete di Connect Pro Presence Service (ad esempio, localhost).
OPN_PORT	Porta interna usata tra Acrobat Connect Pro e Connect Pro Presence Service. Il valore predefinito (10020) deve corrispondere al valore nel file <i>RootInstallationFolder\presserv\conf\router.xml</i> . Non modificate questo valore.
OPN_PASSWORD	Token interno usato tra Acrobat Connect Pro e Connect Pro Presence Service. Il valore predefinito (segreto) deve corrispondere al valore nel file <i>RootInstallationFolder\presserv\conf\router.xml</i> . Non modificate questo valore.
OPN_DOMAIN	Nome del dominio del server Acrobat Connect Pro (server applicazione). Connect Pro Presence Service usa questo nome per identificare il server applicazione. In un cluster, ogni server applicazione deve avere il proprio nome di dominio.
MEETING_PRESENCE_POLL_INTERVAL	I client dell'host interrogano a intervalli regolare il server per recuperare lo stato degli invitati. Questo parametro imposta l'intervallo in secondi tra tali richieste. L'impostazione predefinita è 30. Non modificate questo valore.

Segue un esempio delle impostazioni:

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

Definire il gateway SIP in Connect Pro Presence Service

- 1 Aprite il file *RootInstallationFolder\presserv\conf\lcs gw.xml* in un editor XML.
- 2 Modificate il file come segue, sostituendo i valori in grassetto con i valori richiesti:

```
<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>
```

Nel tag `<bind>`, immettete l'indirizzo IP del computer host di Acrobat Connect Pro. Se vengono restituiti più indirizzi IP, selezionate l'indirizzo IP interno o esterno che il server remoto LCS o OCS dovrà usare per collegarsi ad Acrobat Connect Pro.

- 3 Riavviate Connect Pro Central Application Server.

Configurare Connect Pro Presence Service in un cluster

Se Connect Pro è in esecuzione in un cluster, eseguite Connect Pro Presence su un solo computer del cluster. Configurate invece Connect Pro Presence Service su tutti i computer del cluster in modo che i computer possano scambiarsi informazioni relative alla presenza.

- 1 Aprite *root_install\custom.ini* in un editor di testi.
- 2 Immettete i seguenti parametri e valori:

Parametro	Valore
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Il valore fa distinzione tra maiuscole e minuscole.
OPN_HOST	Il nome FQDN del computer su cui è in esecuzione Connect Pro Presence Service. Il valore del parametro OPN_HOST è uguale su tutti i computer del cluster.
OPN_PORT	Porta interna usata tra Acrobat Connect Pro e Connect Pro Presence Service. Il valore predefinito (10020) deve corrispondere al valore nel file <i>RootInstallationFolder\presserv\conf\router.xml</i> . Non modificate questo valore.
OPN_PASSWORD	Token interno usato tra Acrobat Connect Pro e Connect Pro Presence Service. Il valore predefinito (segreto) deve corrispondere al valore nel file <i>RootInstallationFolder\presserv\conf\router.xml</i> . Non modificate questo valore.
OPN_DOMAIN	Il dominio usato da Connect Pro Presence Service per identificare un server Connect Pro in un cluster. A ogni computer del cluster deve essere assegnato un ID univoco. Il parametro OPN_DOMAIN può avere qualsiasi valore (ad esempio, presence.connect1, presence.connect2, connect3) purché sia un valore univoco nel cluster.
MEETING_PRESENCE_POLL_INTERVAL	I client dell'host interrogano a intervalli regolare il server per recuperare lo stato degli invitati. Questo parametro imposta l'intervallo in secondi tra tali richieste. L'impostazione predefinita è 30. Non modificate questo valore.

Segue un esempio delle impostazioni:

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

3 Riavviate Connect Pro Central Application Server.

Avviare e arrestare Connect Pro Presence Service

Connect Pro Presence Service può essere avviato e arrestato dal menu Start o dalla finestra Servizi.

Avviare e arrestare Connect Pro Presence Service dal menu Start

❖ Effettuate una delle seguenti operazioni:

- Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Presence Service.
- Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Presence Service.

Avviare e arrestare Connect Pro Presence Service dalla finestra Servizi

- 1 Scegliete Start > Pannello di controllo > Strumenti di amministrazione > Servizi per aprire la finestra Servizi.
- 2 Selezionate Acrobat Connect Pro Presence Service e fate clic sul servizio Avvia il servizio, Sospendi il servizio o Riavvia il servizio.

Configurazione di SSO (Single Sign-On)

Informazioni su Single Sign-On

Single Sign-On è un meccanismo di autenticazione degli utenti per tutte le applicazioni di una rete per le quali gli utenti in questione dispongono dell'autorizzazione di accesso. Single Sign-On usa un server proxy per l'autenticazione degli utenti in modo che questi non debbano accedere ad Acrobat Connect Pro.

Acrobat Connect Pro supporta le seguenti soluzioni di Single Sign-On:

Autenticazione dell'intestazione HTTP Configurate un proxy di autenticazione per intercettare le richieste HTTP, analizzare le credenziali utente dall'intestazione e passare le credenziali ad Acrobat Connect Pro.

Autenticazione Microsoft NT LAN Manager (NTLM) Configurate Connect Pro in modo che tenti l'autenticazione automatica dei client che si connettono con il controller di dominio Windows mediante il protocollo NTLMv1. Microsoft Internet Explorer in Microsoft Windows è in grado di negoziare l'autenticazione NTLM senza richiedere le credenziali all'utente.

***Nota:** I client Mozilla Firefox potrebbero essere in grado di negoziare l'autenticazione senza richieste. Per informazioni sulla configurazione, consultate questo [documento Firefox](#).*

Potete inoltre creare un filtro di autenticazione personalizzato. Per ulteriori informazioni, contattate il supporto Adobe.

Configurare l'autenticazione dell'intestazione HTTP

Quando è configurata l'autenticazione dell'intestazione HTTP, le richieste di login di Acrobat Connect Pro vengono instradate a un agente posizionato tra il client e Acrobat Connect Pro. L'agente può essere un proxy di autenticazione o un'applicazione software che esegue l'autenticazione dell'utente, aggiunge un'altra intestazione alla richiesta HTTP e invia la richiesta ad Acrobat Connect Pro. In Acrobat Connect Pro dovete rimuovere il commento a un filtro Java e configurare un parametro nel file custom.ini che specifica il nome dell'intestazione HTTP aggiuntiva.

Altri argomenti presenti nell' Aiuto

“[Avviare e arrestare Acrobat Connect Pro Server](#)” a pagina 87

Configurare l'autenticazione dell'intestazione HTTP su Acrobat Connect Pro

Per attivare l'autenticazione dell'intestazione HTTP, configurate una mappatura di filtro Java e un parametro di intestazione nel computer in cui è installato Acrobat Connect Pro.

1 Aprite il file `[root_install_dir]\appserv\conf\WEB-INF\web.xml` ed eseguite le seguenti operazioni:

a Rimuovete il commento alla mappatura del filtro Java `HeaderAuthenticationFilter`.

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

b Aggiungete un commento alla mappatura del filtro Java `NtlmAuthenticationFilter`.

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

2 Arrestate Acrobat Connect Pro:

a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.

b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Meeting Server.

3 Aggiungete la seguente riga al file `custom.ini`:

```
HTTP_AUTH_HEADER=header_field_name
```

L'agente di autenticazione deve aggiungere un'intestazione alla richiesta HTTP inviata ad Acrobat Connect Pro. Il nome dell'intestazione deve essere `header_field_name`.

4 Salvate il file `custom.ini` e riavviate Acrobat Connect Pro:

a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Meeting Server.

b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

Scrivere il codice di autenticazione

Il codice di autenticazione deve autenticare l'utente, aggiungere un campo all'intestazione HTTP che contiene il login utente e inviare una richiesta ad Acrobat Connect Pro.

1 Impostate il valore del campo dell'intestazione `header_field_name` su un login utente di Acrobat Connect Pro.

2 Inviare una richiesta HTTP ad Acrobat Connect Pro al seguente URL:

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

Il filtro Java di Acrobat Connect Pro intercetta la richiesta, cerca l'intestazione `header_field_name`, quindi l'utente con l'ID passato nell'intestazione. Se l'utente viene individuato, viene autenticato e viene inviata una risposta.

3 Nel contenuto HTTP della risposta di Acrobat Connect Pro, individuate la stringa "OK" che indica l'esito positivo dell'autenticazione.

4 Nella risposta di Acrobat Connect Pro, verificate la presenza del cookie `BREEZESESSION`.

5 Reindirizzate l'utente all'URL richiesto su Acrobat Connect Pro e passate il cookie `BREEZESESSION` come valore del parametro `session`, come indicato di seguito:

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

Nota: dovete passare il cookie `BREEZESESSION` in tutte le richieste ad Acrobat Connect Pro durante la sessione client corrente.

Configurare l'autenticazione dell'intestazione HTTP con Apache

Nella seguente procedura viene descritto un esempio di implementazione di autenticazione dell'intestazione HTTP che usa Apache come agente di autenticazione.

1 Installate Apache come proxy inverso su un computer diverso da quello in cui è installato Acrobat Connect Pro.

2 Scegliete Start > Programmi > Apache HTTP Server > Configure Apache Server > Edit the Apache httpd.conf Configuration file ed eseguite le seguenti operazioni:

a Rimuovete il commento dalla seguente riga:

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

b Rimuovete il commento dalle seguenti tre righe:

```
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 Aggiungete le seguenti righe alla fine del file:

```
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 Arrestate Acrobat Connect Pro:

a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.

b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Meeting Server.

4 Sul computer in cui è installato Acrobat Connect Pro aggiungete le seguenti righe di codice al file `custom.ini` (che per impostazione predefinita si trova nella directory di installazione principale `c:\breeze`):

```
HTTP_AUTH_HEADER=custom-auth
```

Il parametro `HTTP_AUTH_HEADER` deve corrispondere al nome configurato nel proxy. (In questo esempio è stato configurato nella riga 1 del passaggio 2c.) Il parametro è l'instestazione HTTP aggiuntiva.

5 Salvate il file `custom.ini` e riavviate Acrobat Connect Pro:

- a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Meeting Server.
- b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

6 Aprite il file `[root_install_dir]\appserv\conf\WEB-INF\web.xml` ed eseguite le seguenti operazioni:

- a Rimuovete il commento alla mappatura del filtro `Java HeaderAuthenticationFilter`.

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

- b Aggiungete un commento alla mappatura del filtro `Java NtlmAuthenticationFilter`.

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

Configurare l'autenticazione NTLM

NTLMv1 è un protocollo di autenticazione utilizzato con il protocollo di rete SMB nelle reti Microsoft Windows. Potete utilizzare il protocollo NTLM per consentire a un utente di dimostrare la propria identità in un dominio Windows dopo essere stato autorizzato ad accedere a un'altra risorsa di rete come Connect Pro. Per stabilire le credenziali dell'utente, il suo browser esegue automaticamente un'autenticazione di tipo challenge/response con il controller del dominio attraverso Connect Pro. Se il meccanismo ha esito negativo, l'utente può accedere direttamente a Connect Pro. Solo Internet Explorer su Windows supporta l'accesso unico con l'autenticazione NTLMv1.

Nota: per impostazione predefinita, i controller del dominio di Windows Server 2003 richiedono una funzione di sicurezza denominata firme SMB. Le firme SMB non sono supportate con la configurazione predefinita del filtro di autenticazione NTLM. potete configurare il filtro in modo che funzioni con questo requisito. Per ulteriori informazioni su questa e altre opzioni di configurazione avanzate, consultate la [documentazione sull'autenticazione JCIFS NTLM HTTP](#).

Aggiungere parametri di configurazione

Effettuate le seguenti operazioni per ciascun host presente in un cluster Connect Pro:

- 1 Aprite il file `root_install_dir\custom.ini` in un editor di testo e aggiungete i seguenti parametri:

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

Il valore `[dominio]` è il nome del dominio Windows a cui appartengono gli utenti e con cui eseguono l'autenticazione, ad esempio, RETEAZIENDA. È possibile che sia necessario impostare questo valore nelle versioni precedenti a Windows 2000 del nome di dominio. Per ulteriori informazioni, consultate [TechNote 27e73404](#). Il valore viene mappato sulla proprietà del filtro `jcifs.smb.client.domain`. Se il valore viene impostato direttamente nel file `web.xml`, sostituisce anche il valore nel file `custom.ini`.

Il valore [WINS_server_IP_address] corrisponde all'indirizzo IP o a un elenco di indirizzi IP separati da virgole dei server WINS. Utilizzate l'indirizzo IP, il nome host non funziona. I server WINS vengono interrogati nell'ordine specificato per risolvere l'indirizzo IP di un controller di dominio specificato nel parametro NTLM_DOMAIN. (Il controller di dominio esegue l'autenticazione degli utenti). Inoltre potete specificare l'indirizzo IP del controller di dominio stesso, ad esempio 10.169.10.77, 10.169.10.66. Questo valore viene mappato sulla proprietà del filtro `jcifs.netbios.wins`. Se il valore viene impostato nel file `web.xml`, sostituisce anche il valore nel file `custom.ini`.

2 Salvate il file `custom.ini`.

3 Aprite il file `root_install_dir\appserv\conf\WEB-INF\web.xml` in un editor di testo ed effettuate quanto segue:

a Eliminate il commento da `NtlmAuthenticationFilter` mapping, nel modo seguente:

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

b Cancellate il commento da `HeaderAuthenticationFilter` filter mapping, nel modo seguente:

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

4 Salvate il file `web.xml`.

5 Riavviate Connect Pro.

a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Serve > Arresta Adobe Acrobat Connect Pro Server.

b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server > Avvia Adobe Acrobat Connect Pro Server.

Riconciliare i criteri di login

Connect Pro e NTLM hanno criteri di login diversi per l'autenticazione degli utenti. Questi criteri vanno conformati prima che gli utenti possano utilizzare un unico login.

A seconda dei criteri utilizzati, il protocollo NTLM usa un identificatore di login che può essere un nome utente (mrossi), un ID di dipendente (1234) o un nome crittografato. Per impostazione predefinita, Connect Pro usa un indirizzo e-mail (mrossi@azienda.com) come identificatore di login. Modificate i criteri di login di Connect Pro in modo che possa condividere un unico identificativo con NTLM.

1 Aprite Connect Pro Central.

Per aprire Connect Pro Central, aprite una finestra del browser e digitate il nome di dominio completo dell'host di Connect Pro (ad esempio `http://connect.esempio.com`). Il valore per l'host di Connect Pro è stato immesso nella schermata Impostazioni server della console di gestione applicazione.

2 Selezionate la scheda Amministrazione. Fate clic su Utenti e gruppi. Fate clic su Modifica criteri di login e password.

3 Nella sezione Criterio di login selezionate No per Usa indirizzo e-mail per il login.

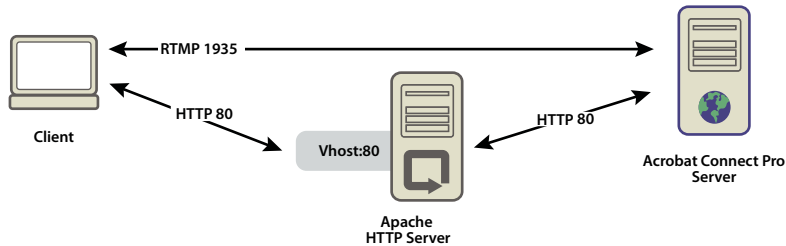
Configurazione di un proxy inverso davanti a Connect Pro Server

Uso di un proxy inverso

Davanti a Connect Pro Server potete configurare un proxy inverso. Il traffico passa attraverso il proxy inverso prima di raggiungere Connect Pro Server. Utilizzate questa configurazione per ottenere quanto segue:

- Tenere Connect Pro Server fuori dalla rete perimetrale.
Inserire il proxy inverso nella rete perimetrale e Connect Pro Server dietro il firewall aziendale.
- Eseguire l'autenticazione degli utenti prima che arrivino a Connect Pro Server.

Il proxy inverso esegue l'autenticazione con un altro sistema e autorizza gli utenti a connettersi a Connect Pro Server.



Il traffico HTTP passa attraverso il server Apache HTTP per arrivare a Connect Pro Server.

Configurare un proxy inverso

In questo esempio viene utilizzata l'installazione Windows (a 32 bit) del server Apache HTTP. La configurazione è la stessa per qualunque sistema operativo che Apache supporta. Nell'esempio non è utilizzata la codifica SOL; il traffico verso il server dell'applicazione di Connect Pro non è criptato.

Per forzare il passaggio di tutto il traffico HTTP attraverso il server Apache HTTP prima che arrivi a Connect Pro, effettuate quanto segue:

Nota: il traffico RTMP non passa attraverso il server Apache HTTP in questa configurazione.

- 1 Installate il server Apache HTTP.

Per impostazione predefinita, i file di configurazione Apache si trovano nella cartella `c:\Program Files\Apache Software Foundation\Apache2.2\conf\`.

- 2 Configurate Apache in modo che riceva tutto il traffico sulla porta 80.

Aprirete il file `c:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf` in un editor di testo e aggiungete quanto segue:

```
#  
# 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 Caricate il modulo richiesto per il funzionamento come proxy inverso.

Nello stesso file (httpd.conf), eliminate il commento dalle righe seguenti:

```
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 Collegate il file httpd.conf al file di configurazione che controlla le connessioni a Connect Pro.

Aggiungete la riga seguente alla fine del file httpd.conf:

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

- 5 Create un file di testo denominato httpd-connect.conf e salvatelo in c:\Program Files\Apache Software Foundation\Apache2.2\conf\extra.

- 6 Aggiungete le righe seguenti al file httpd-connect.conf file (inserite i vostri indirizzi IP e le porte dove è richiesto):

```
#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 Salvate il file e riavviate il servizio Apache.

- 8 Su Connect Pro Server, aprite la console di gestione applicazione in un browser: <http://localhost:8510/console/>

- 9 Nella schermata Impostazioni del server, effettuate quanto segue:

- Impostate l'host Connect Pro sul nome di dominio completo del server Apache HTTP.
- Impostate il nome esterno sul nome di dominio completo del computer su cui è installato Connect Meeting Server.

- 10 Riavviate Adobe Connect Pro Service (il server delle applicazioni) e il servizio Flash Media Server (FMS) (il server delle riunioni). Consultate “[Avviare e arrestare i server](#)” a pagina 87.

RTMP viene instradato su Connect Pro e HTTP attraverso Apache.

Hosting di Acrobat Connect Add-In

Informazioni su Acrobat Connect Add-In

Adobe Acrobat Connect Add-in è una versione di Flash Player che include funzioni avanzate per le riunioni di Acrobat Connect Pro.

Quando viene richiesto Acrobat Connect Add-In, questo viene scaricato automaticamente da un server Adobe in un processo invisibile per l'utente. Tuttavia, se la vostra organizzazione non consente ai dipendenti di scaricare software da server esterni, potete installare Acrobat Connect Add-in in un server dell'organizzazione.

I partecipanti alle riunioni, gli utenti registrati e i relatori devono scaricare Acrobat Connect Add-In se dispongono di una versione obsoleta e vengono promossi a ospitante o relatore oppure se vengono loro concessi diritti avanzati per il contenitore Condivisione.

Gli ospitanti di riunioni devono scaricare Acrobat Connect Add-In se questo non è installato sul computer in uso o se dispongono di una versione obsoleta.

Personalizzare la posizione di download di Acrobat Connect Add-In

Potete effettuare l'hosting di Acrobat Connect Add-In in un server dell'organizzazione e indirizzare gli utenti direttamente ai file eseguibili. Potete anche indirizzare gli utenti a una pagina con istruzioni per il download, con collegamenti verso i file eseguibili. Potete creare una pagina personalizzata con istruzioni per il download o usarne una fornita da Adobe. La pagina di Adobe è localizzata in tutte le lingue supportate.

Indirizzare gli utenti direttamente ai file eseguibili

- 1 Individuate il file XML della lingua di Acrobat Connect Pro sul server in cui è installato Acrobat Connect Pro. I file XML si trovano nelle due seguenti directory: `[root_install_dir]\appserv\web\common\intro\lang` e `[root_install_dir]\appserv\web\common\meeting\lang`.
- 2 Immettete un percorso per i file eseguibili per ogni piattaforma nella sezione `addInLocation` di ogni piattaforma in ciascun file della lingua:

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

Nota: questi sono i percorsi predefiniti dei file eseguibili del modulo Add-In. Potete modificare i percorsi sul server e cambiare di conseguenza i percorsi nella sezione `addInLocation`.

Indirizzare gli utenti alle pagine delle istruzioni per il download di Adobe

- 1 Individuate il file XML della lingua di Acrobat Connect Pro sul server in cui è installato Acrobat Connect Pro. I file XML si trovano nelle due seguenti directory: `[root_install_dir]\appserv\web\common\intro\lang` e `[root_install_dir]\appserv\web\common\meeting\lang`.
- 2 Immettete il percorso della pagina di istruzioni per il download nella sezione `addInLocation` di ogni piattaforma in ciascun file della lingua:

```
<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: il percorso include una stringa `#lang#` che Acrobat Connect Pro converte nella lingua della riunione in fase di runtime.

- 3 I file addindownload.htm contengono collegamenti verso i file eseguibili del modulo Add-In nei percorsi predefiniti in Acrobat Connect Pro (/common/addin/setup.exe e /common/addin/AcrobatConnectAddin.z). Se modificate il percorso dei file eseguibili, aggiornate i collegamenti nella pagina addindownload.htm di ogni lingua.

Indirizzare gli utenti alle pagine di istruzioni per il download create personalmente

- 1 Individuate il file XML della lingua di Acrobat Connect Pro sul server in cui è installato Acrobat Connect Pro. I file XML si trovano nelle due seguenti directory: [root_install_dir]\appserv\web\common\intro\lang e [root_install_dir]\appserv\web\common\meeting\lang.
- 2 Nella sezione addInLocation di ogni piattaforma in ciascun file della lingua, immettete il percorso della pagina di istruzioni che avete creato:

```
<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: potete decidere di creare pagine delle istruzioni distinte per ogni piattaforma.

- 3 Create una pagina di istruzioni in ogni lingua che desiderate supportare. Nella pagina di istruzioni, includete collegamenti verso i file eseguibili del modulo Add-In per ogni piattaforma.

Capitolo 4: Protezione

Proteggendo Adobe Acrobat Connect Pro Server proteggete la vostra organizzazione dalla perdita di proprietà e da azioni dannose. È importante proteggere l'infrastruttura della propria organizzazione, Acrobat Connect Pro Server e il server del database utilizzato da Acrobat Connect Pro.

SSL (Secure Sockets Layer)

Informazioni sul supporto di SSL

Acrobat Connect Pro Server è composto da due server: Adobe® Flash® Media Server e il server applicazione Acrobat Connect Pro. Flash Media Server è anche detto *server riunioni* perché rende accessibili le riunioni in tempo reale tramite una connessione RTMP al client. Il server dell'applicazione Acrobat Connect Pro gestisce la connessione HTTP tra il client e la logica dell'applicazione Acrobat Connect Pro.

Nota: nel menu Start, il server riunioni si chiama "Connect Pro Meeting Server" e il server applicazione si chiama "Connect Pro Central Application Server". Nella finestra Servizi, il server riunioni si chiama "Flash Media Server (FMS)" e il server applicazione si chiama "Adobe Connect Enterprise Service".

È possibile configurare SSL per il server dell'applicazione, il server riunioni o entrambi:

Soluzione basata su hardware Utilizzate un acceleratore SSL per una configurazione SSL più robusta.

Acquistate separatamente un acceleratore SSL. Adobe ha verificato che Acrobat Connect Pro funziona con i seguenti acceleratori hardware SSL: F5 Big-IP 1000, Cisco Catalyst 6590 Switch e Radware T100.

Soluzione basata su software Utilizzate il supporto nativo per SSL in Acrobat Connect Pro.

Nota: SSL non è supportato su Microsoft® Windows® 98.

Acrobat Connect Pro utilizza il metodo HTTP CONNECT per richiedere una connessione SSL. I server proxy devono permettere ai client di usare il metodo CONNECT. Se i client non possono usare il metodo CONNECT, le connessioni RTMP avvengono mediante HTTP/HTTPS.

Per informazioni sulla configurazione di SSL, contattate l'assistenza Adobe all'indirizzo www.adobe.com/go/connect_licensed_programs_it.

Utilizzo dei certificati

Un certificato SSL verifica l'identità del server per il client.

Per stabilire la connessione del server riunioni (RTMP) e del server dell'applicazione (HTTP), è necessario disporre di due certificati SSL: uno per ciascun server. Per configurare SSL per un cluster di computer per l'hosting di Acrobat Connect Pro, occorre un certificato SSL per ogni server riunioni. Tutti i server applicazione in un cluster possono condividere un unico certificato SSL.

Ad esempio, per proteggere le connessioni del server riunioni e del server applicazione su un unico server, sono necessari due certificati SSL. Per proteggere le connessioni del server riunioni e del server applicazione in un cluster di tre server, sono necessari quattro certificati SSL: uno condiviso dai server applicazione e tre per i server riunioni.

Ottenere i certificati

- ❖ Contattate un'autorità di certificazione, ossia una società indipendente affidabile che verifichi l'identità del richiedente. (I certificati di tipo self-signed non funzionano con Acrobat Connect Pro.)

L'autorità di certificazione chiederà di generare un file Certificate Signing Request (CSR) SSL. Inviare il file CSR all'autorità di certificazione, che provvederà a convertirlo in certificato SSL. Contiene informazioni sulla vostra organizzazione e sul FQDN (Fully Qualified Domain Name, nome di dominio pienamente qualificato) associato al certificato SSL. Per istruzioni sulla generazione di un CSR, contattate l'autorità di certificazione.

Importante: Memorizzate le password per i certificati SSL in un'ubicazione sicura e accessibile.

Installare i certificati

- ❖ Installate i file dei certificati SSL e delle chiavi private in formato PEM nella cartella di Acrobat Connect Pro, per impostazione predefinita, c:\breeze.

Se ricevete un file CRT da un'autorità di certificazione, potete rinominare il file in modo che la sua estensione sia .pem.

Nota: sono necessari due file per ciascuna connessione protetta: uno per il certificato pubblico e uno per la chiave privata. Il server invia il certificato pubblico al client, mentre la chiave privata rimane sul server.

Configurare SSL basato su software

Quando si configura SSL basato su software, è possibile stabilire una connessione con il server applicazione (HTTP), il server riunioni (RTMP) o entrambi. Il server DNS va configurato per primo, indipendentemente dalla configurazione scelta.

Configurare il server DNS

- ❖ Create voci DNS che definiscano un FQDN per ogni connessione protetta.

Il nome FQDN per il server applicazione è l'URL che gli utenti finali devono usare per connettersi ad Acrobat Connect Pro. Immettete questo FQDN per il valore Host di Connect Pro nella pagina Impostazioni server, nella console di gestione dell'applicazione. Ad esempio, potete usare un valore di tipo `connect.nomeazienda.com`

Gli utenti finali non vedono il nome FQDN del server riunioni. Tuttavia per condurre riunioni tramite una connessione protetta è necessario avere un nome FQDN anche per il server riunioni. Immettete questo FQDN per il valore Nome esterno nella pagina Impostazioni server, nella console di gestione dell'applicazione. Ad esempio, potete usare un valore di tipo `fms.nomeazienda.com`.

Nota: in un cluster di server, tutti i server applicazione possono condividere lo stesso certificato SSL. I server riunioni, invece, richiedono ciascuno un proprio certificato. Per proteggere sia le connessioni HTTP, ossia quelle del server applicazione, che le connessioni RTMP, ossia quelle del server riunioni, su un unico server, dovete disporre di un totale di due FQDN e due certificati SSL, uno per ciascun protocollo.

Proteggere il server riunioni e il server applicazione

- 1 Aprire il file `Adaptor.xml` ubicato in `[root_install_dir]\comserv\win32\conf_defaultRoot_` e salvare una copia di backup in un'altra ubicazione.
- 2 Inserire il seguente codice nel file `Adaptor.xml` originale all'interno dei tag `<Adaptor></Adaptor>` (sostituire il codice in corsivo con i propri valori):

```

<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>

```

Dovete disporre di due file per ciascuna connessione protetta: uno per il certificato SSL pubblico e uno per la chiave privata che appartiene al certificato. Specificate la posizione del certificato SSL pubblico nel tag `<SSLCertificateFile>` e quella della chiave privata nel tag `<SSLCertificateKeyFile>`. Il server invia il certificato SSL pubblico ai client, mentre la chiave privata rimane sul server.

3 Individuate la riga seguente nel file `Adaptor.xml`:

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

4 Sostituite il codice al punto 3 con quanto segue:

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

5 Salvate il file `Adaptor.xml`.

6 (Facoltativo) Aprite il file `Adaptor.xml` in un browser Web per convalidarne la sintassi.

Se il browser segnala un errore, correggetelo e riaprite il file in un browser Web. Ripetete questa procedura finché il file non risulti valido.

7 Aprite il file `custom.ini` presente nella directory di installazione principale (per impostazione predefinita, `c:\breeze`) e salvate una copia di backup in un'altra ubicazione.

8 Inserite il seguente codice nel file `custom.ini` senza sostituire né eliminare il testo esistente:

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

Nota: il file `custom.ini` fa distinzione tra lettere maiuscole e minuscole: usate lettere maiuscole per i nomi dei parametri e lettere minuscole per i relativi valori.

9 Salvate il file `custom.ini`.

10 Aprire il file VHost.xml ubicato in `[root_install_dir]\comserv\win32\conf_defaultRoot_defaultVHost_` e salvare una copia di backup in un'altra ubicazione.

11 Individuare la riga seguente nel file VHost.xml:

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

12 Sostituire la riga al punto 11 con il seguente codice:

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

13 Salvate il file VHost.xml.

14 (Facoltativo) Aprite il file VHost.xml in un browser Web per convalidarne la sintassi.

15 Riavviate Adobe Connect Pro Server 7:

- a** Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.
- b** Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Meeting Server.
- c** Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Meeting Server.
- d** Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

16 Aprite la console di gestione applicazione (<http://localhost:8510/console> oppure Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Configura Connect Pro Server 7).

17 Nella schermata Impostazioni applicazione, selezionate Impostazioni server e procedete come segue:

- a** Immettete il nome FQDN per l'account di Acrobat Connect Pro nella casella Host di Connect Pro. Il nome FQDN è l'URL che gli utenti finali devono usare per connettersi ad Acrobat Connect Pro.
- b** Immettete il nome FQDN per il server riunioni di Acrobat Connect Pro nella casella Nome esterno di Mappature host. Il server usa questo valore internamente.

Stabilire la connessione solo con il server dell'applicazione

1 Aprire il file Adaptor.xml ubicato in `[root_install_dir]\comserv\win32\conf_defaultRoot_` e salvare una copia di backup in un'altra ubicazione.

2 Inserire il seguente codice nel file Adaptor.xml originale all'interno dei tag `<Adaptor></Adaptor>` (sostituire il codice in corsivo con i propri valori):

```
<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>
```

Dovete disporre di due file: uno per il certificato SSL pubblico e uno per la chiave privata che appartiene al certificato. Specificate la posizione del certificato SSL pubblico nel tag `<SSLCertificateFile>` e quella della chiave privata nel tag `<SSLCertificateKeyFile>`. Il server invia il certificato SSL pubblico ai client, mentre la chiave privata rimane sul server.

3 Individuate la riga seguente nel file `Adaptor.xml`:

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

4 Aggiungete il seguente codice sotto la riga al punto 3:

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

5 Salvate il file `Adaptor.xml`.

6 (Facoltativo) Aprite il file `Adaptor.xml` in un browser Web per convalidarne la sintassi.

Se il browser segnala un errore, correggetelo e riaprite il file in un browser Web. Ripetete questa procedura finché il file non risulti valido.

7 Aprite il file `custom.ini` presente nella directory di installazione principale (per impostazione predefinita, `c:\breeze`) e salvate una copia di backup in un'altra ubicazione.

8 Inserite il seguente codice nel file `custom.ini` senza sostituire né eliminare il testo esistente:

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

Nota: il file `custom.ini` fa distinzione tra lettere maiuscole e minuscole: usate lettere maiuscole per i nomi dei parametri e lettere minuscole per i relativi valori.

9 Salvate il file `custom.ini`.

10 Riavviate Acrobat Connect Pro Server 7:

- a** Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.
- b** Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Meeting Server.
- c** Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Meeting Server.
- d** Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

Stabilire la connessione solo con il server della riunione

1 Aprire il file `Adaptor.xml` ubicato in `[root_install_dir]\comserv\win32\conf_defaultRoot_` e salvare una copia di backup in un'altra ubicazione.

2 Inserire il seguente codice nel file `Adaptor.xml` originale all'interno dei tag `<Adaptor></Adaptor>` (sostituire il codice in corsivo con i propri valori):

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

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

Dovete disporre di due file: uno per il certificato SSL pubblico e uno per la chiave privata che appartiene al certificato. Specificate la posizione del certificato SSL pubblico nel tag <SSLCertificateFile> e quella della chiave privata nel tag <SSLCertificateKeyFile>. Il server invia il certificato SSL pubblico ai client, mentre la chiave privata rimane sul server.

3 Individuate la riga seguente nel file Adaptor.xml:

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

4 Sostituite il codice al punto 3 con quanto segue:

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

5 Salvate il file Adaptor.xml.

6 (Facoltativo) Aprite il file Adaptor.xml in un browser Web per convalidarne la sintassi.

Se il browser segnala un errore, correggetelo e riaprite il file in un browser Web. Ripetere questa procedura finché il file è valido.

7 Aprire il file VHost.xml ubicato in [root_install_dir]\comserv\win32\conf_defaultRoot_defaultVHost_e salvare una copia di backup in un'altra ubicazione.

8 Individuare la riga seguente nel file VHost.xml:

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

9 Sostituite la riga al punto 8 con il seguente codice:

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

10 Salvate il file VHost.xml.

11 (Facoltativo) Aprite il file VHost.xml in un browser Web per convalidarne la sintassi.

12 Aprite il file custom.ini presente nella directory di installazione principale (per impostazione predefinita, c:\breeze) e salvatene una copia di backup in un'altra posizione.

13 Inserite il seguente codice nel file custom.ini senza sostituire né eliminare il testo esistente:

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

14 Salvate il file custom.ini.

15 Riavviate Acrobat Connect Pro Server 7:

- a** Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.
- b** Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Meeting Server.
- c** Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Meeting Server.

- d Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

Provare la configurazione

- 1 Se avete protetto il server applicazione, effettuate il login a Connect Pro Central. Nel browser compare l'icona del lucchetto.
- 2 Se avete protetto la connessione del server riunioni, entrate in una stanza riunioni di Acrobat Connect Pro. La spia della connessione presenta l'icona del lucchetto.

Configurare SSL basato su hardware

Quando si configura SSL basato su hardware, è possibile stabilire una connessione con il server dell'applicazione (HTTP), il server della riunione (RTMP) o entrambi. Il server DNS va configurato per primo, indipendentemente dalla configurazione scelta.

Per ulteriori istruzioni su come configurare l'acceleratore hardware, consultate la documentazione del fornitore.

Configurare il server DNS

- ❖ Creare voci DNS per il server per tutti i server da proteggere

Definite un FQDN per ciascun server protetto, ad esempio applicazione.esempio.com e riunioni1.esempio.com.

Nota: in un cluster di server, tutti i server applicazione possono condividere lo stesso certificato SSL. I server riunioni invece richiedono ciascuno un proprio certificato. Per proteggere sia le connessioni HTTP, ossia quelle del server applicazione, che le connessioni RTMP, ossia quelle del server riunioni, su un unico server, dovete disporre di un totale di due FQDN e due certificati SSL, uno per ciascun protocollo.

Configurare SSL per i server riunione e dell'applicazione

- 1 Configurare il dispositivo hardware in modo che possa effettuare le seguenti operazioni:
 - a Ascoltare esternamente sulla porta 443 per application.esempio.com.
 - b Inoltrare i dati non crittografati al server dell'applicazione sulla porta 8443.
 - c Ascoltare esternamente sulla porta 443 per meeting1.esempio.com.
 - d Inoltrare i dati non crittografati al server della riunione sulla porta 1935.
 - e (Facoltativo) Ascoltare esternamente sulla porta 80 per application.example.com e inoltrare i dati non crittografati al server dell'applicazione sulla porta 80. Il server applicazione reindirizzerà gli utenti alla porta 443.
- 2 Configurare il firewall in modo che possa effettuare le seguenti operazioni:
 - a Consentire il traffico sul server dell'applicazione sulla porta 443 (e sulla porta 80, se si è completata la fase 1e).
 - b Consentire il traffico al server della riunione sulla porta 443.
- 3 Scegliete Start > Programmi > Adobe Connect Pro Server 7 > Configura Connect Pro Server 7 per aprire la console di gestione applicazione. Nella schermata Impostazioni applicazione, selezionate Impostazioni server e procedete come segue:
 - a Immettete il nome FQDN del server applicazione (ad esempio, connect.esempio.com) nella casella Host di Connect Pro. Il nome FQDN è l'URL che gli utenti finali devono usare per connettersi ad Acrobat Connect Pro.
 - b Immettete il nome FQDN del server riunioni (ad esempio, fms.esempio.com) nella casella Nome esterno di Mappature host. Il server usa questo valore internamente.

4 Aprite il file custom.ini presente nella directory di installazione principale (per impostazione predefinita, c:\breeze) e salvatene una copia di backup in un'altra posizione.

5 Inserite il seguente codice nel file custom.ini senza sostituire né eliminare il testo esistente:

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

Nota: il file custom.ini fa distinzione tra lettere maiuscole e minuscole: usate lettere maiuscole per i nomi dei parametri e lettere minuscole per i relativi valori.

6 Salvate il file custom.ini.

7 Riavviate Acrobat Connect Pro Server 7:

a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.

b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

Configurare SSL solo per il server riunioni

1 Configurate il dispositivo hardware in modo che possa effettuare le seguenti operazioni:

a Ascoltare esternamente sulla porta 443 per meeting1.example.com.

b Inoltrare i dati non crittografati al server della riunione sulla porta 1935.

2 Configurare il firewall per consentire il traffico al server della riunione sulla porta 443.

3 Aprite il file custom.ini presente nella directory di installazione principale (per impostazione predefinita, c:\breeze) e salvatene una copia di backup in un'altra posizione.

4 Inserite il seguente codice nel file custom.ini senza sostituire né eliminare il testo esistente:

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

5 Salvate il file custom.ini.

Configurare SSL solo per il server dell'applicazione

1 Configurate il dispositivo hardware in modo che possa effettuare le seguenti operazioni:

a Ascoltare esternamente sulla porta 443 per application.esempio.com.

b Inoltrare i dati non crittografati al server dell'applicazione sulla porta 8443.

c (Facoltativo) Ascoltare esternamente sulla porta 80 per application.example.com e inoltrare i dati non crittografati al server dell'applicazione sulla porta 80. Il server applicazione reindirizzerà gli utenti alla porta 443.

2 Configurate il firewall per consentire il traffico sul server dell'applicazione sulla porta 443 (e sulla porta 80, se si è completata la fase 1c).

3 In Acrobat Connect Pro, aggiungete quanto segue al file custom.ini nella cartella di installazione principale (per impostazione predefinita, c:\breeze):

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

Nota: il file custom.ini fa distinzione tra lettere maiuscole e minuscole: usate lettere maiuscole per i nomi dei parametri e lettere minuscole per i relativi valori.

4 Riavviate Acrobat Connect Pro Server 7:

- a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.
- b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

Provare la configurazione

- 1 Se avete protetto il server applicazione, effettuate il login a Connect Pro Central. Nel browser compare l'icona del lucchetto.
- 2 Se avete protetto la connessione del server riunioni, entrate in una stanza riunioni di Acrobat Connect Pro. La spia della connessione presenta l'icona del lucchetto.

Configurare SSL basato su software per un server periferico

Se sul server di origine è configurato SSL basato su software, questo va configurato anche per tutti i server periferici da proteggere.

Come un server di origine, un server periferico è composto da due servizi: un servizio riunioni e un servizio applicazione. Per configurare SSL per entrambi questi servizi, sono necessari due nomi FQDN e due indirizzi IP. Potete condividere il nome FQDN del servizio applicazione con il server di origine, ma il servizio riunioni deve avere un proprio FQDN. Il nome FQDN del server applicazione è l'URL che gli utenti finali devono usare per connettersi ai propri account Acrobat Connect Pro.

Ad esempio, se avete un server periferico e un server di origine, occorrono tre nomi FQDN e tre certificati SSL: uno per ogni servizio riunione e uno condiviso tra i servizi applicazione. Sono necessari quattro indirizzi IP, uno per ogni servizio riunione e uno per ogni servizio applicazione.

In questa configurazione di esempio, il server di origine ha i seguenti indirizzi IP e nomi FQDN:

10.192.37.11 = connect.yourcompany.com
10.192.37.10 = meeting1.yourcompany.com

Il server periferico ha i seguenti indirizzi IP e nomi FQDN:

10.192.37.100 = connect.yourcompany.com
10.192.37.101 = edge1.yourcompany.com

Nota: se state installando per la prima volta sia il server periferico che il server di origine, impostateli entrambi senza SSL e verificate che possano comunicare tra di loro. Una volta determinato che i server periferico e di origine possono comunicare, potete configurare l'SSL per entrambi.

Altri argomenti presenti nell' Aiuto

["Implementazione di Acrobat Connect Pro Edge Server"](#) a pagina 27

["Informazioni sul supporto di SSL"](#) a pagina 65

Configurare il server periferico

- 1 Nel server di origine, aprite il file c:\breeze\comserv\win32\conf_defaultRoot_\Adaptor.xml e copiate tutta la sezione <SSL></SSL>, come segue:

```

<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: è possibile che il codice contenga valori diversi, ma deve contenere gli stessi elementi XML.

- 2 Nel server periferico, aprite il file c:\breeze\edgeserver\win32\conf_defaultRoot_\Adaptor.xml e incollate il blocco di codice <SSL></SSL> copiato dal server di origine dopo il tag <Adaptor>.
- 3 Effettuate le seguenti operazioni per configurare il servizio applicazione e il servizio riunione sul server periferico:
 - a Il servizio applicazione corrisponde al tag <Edge name="applicationserver"> nel blocco <SSL>. Il servizio applicazione usa lo stesso nome FQDN del servizio applicazione sul server di origine. Copiate il certificato e i file chiave .pem dal server di origine alla stessa posizione sul server periferico. In questo esempio, il nome FQDN è 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 Il servizio riunione corrisponde al tag <Edge name="meetingserver"> nel blocco <SSL>. Modificate l'XML in modo che il servizio riunione punti a file di certificato e chiave univoci per il suo nome FQDN univoco. In questo esempio, il nome FQDN è 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 Nel file Adaptor.xml sul server periferico, individuate la riga `<HostPort name="edge1">${FCS.HOST_PORT}</HostPort>`. Dopo tale riga, aggiungete le due seguenti righe:

```
<HostPort name="meetingserver" ctl_channel=":19354">206.192.37.100:-443</HostPort>
<HostPort name="applicationserver" ctl_channel=":19355">206.192.37.101:-443</HostPort>
```

Questo codice vincola gli indirizzi IP interni del server periferico alla porta protetta 443. In questo esempio, gli indirizzi IP interni sono 206.192.37.100 e 206.192.37.101. Nel vostro codice, usate gli indirizzi IP interni del vostro server periferico.

5 Salvate il file Adaptor.xml.

6 Aprite il file Adaptor.xml in un browser Web per verificare la validità dell'XML.

In caso di errori di sintassi, il browser Web presenta un messaggio di errore. Correggete gli errori XML e verificate nuovamente il file.

7 Sul server periferico, aprite il file `c:\breeze\edgeserver\win32\conf_defaultRoot_defaultVHost_Vhost.xml`.

Individuate il tag `<RouteEntry></RouteEntry>` e sostituitelo con quanto segue:

```
<RouteEntry protocol="rtmp">*:*;10.192.37.11:8506</RouteEntry>
```

Questo codice fa sì che il server periferico indirizzi le connessioni RTMP da qualsiasi indirizzo IP e qualsiasi porta al server di origine, mediante la porta 8506. In questo esempio viene usato l'indirizzo IP 10.192.37.11. Nel vostro codice, usate l'indirizzo IP del servizio applicazione del vostro server di origine.

8 Salvate il file VHost.xml.

9 Aprite il file VHost.xml in un browser Web per verificare la validità dell'XML.

In caso di errori di sintassi, il browser Web presenta un messaggio di errore. Correggete gli errori XML e verificate nuovamente il file.

10 Sul server periferico, aprite il file `c:\breeze\edgeserver\custom.ini`.

11 Immettete il parametro `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` e impostatelo sull'indirizzo IP o sul nome FQDN del server di origine, come segue:

```
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
```

Per configurare il sistema per la connessione solo tramite SSL, aggiungete un marcatore di commento davanti al parametro `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT`, come segue:

```
# FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

Nota: se il server periferico non riesce a risolvere il nome FQDN del server di origine, usate l'indirizzo IP.

12 Nel server di origine, aprite il file C:\breeze\edgeserver\win32\conf\HttpCache.xml e aggiornate il tag <HostName>, come segue:

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

13 Salvate il file HttpCache.xml.

14 Aprite il file HttpCache.xml in un browser Web per verificare la validità dell'XML.

In caso di errori di sintassi, il browser Web presenta un messaggio di errore. Correggete eventuali errori XML e verificate nuovamente il file.

Configurare il server di origine

1 Configurate il server di origine per SSL. Per ulteriori informazioni, consultate “[SSL \(Secure Sockets Layer\)](#)” a pagina 65.

2 Sul server di origine, aprite il file c:\breeze\custom.ini e immettete quanto segue per vincolare il server periferico al server di origine:

```
edge.FCS_EDGE_CLUSTER_ID=1
```

Usate il valore per il parametro `FCS_EDGE_CLUSTER_ID` impostato nel file custom.ini del server periferico. In questo esempio, il valore è `sanfran` e il codice è quindi `edge.sanfran=1`.

Nota: il valore 0 è riservato e non può essere usato.

3 Riavviate Connect Pro Central Application Server e Connect Pro Meeting Server.

4 Scegliete Start > Programmi > Adobe Connect Pro Server 7 > Configura Connect Pro Server 7 per aprire la console di gestione applicazione. Effettuate le seguenti operazioni:

a Fate clic su Impostazioni server.

b Nella casella Nomi esterni, potete vedere il nome FQDN del server periferico e una casella vuota alla sua destra. Se non vedete il nome FQDN, attendete qualche minuto e aggiornate la finestra del browser.

c Immettete il nome FQDN del server periferico nella casella vuota e fate clic su Salva. In questo modo il server periferico viene registrato presso il server di origine.

5 Impostate il server DNS locale affinché indirizzi al server periferico gli utenti che richiedono un URL di Acrobat Connect Pro.

Configurare SSL basato su hardware per un server periferico

Se sul server di origine è configurato un SSL basato su hardware, questo va configurato anche per tutti i server periferici da proteggere.

Come un server di origine, un server periferico è composto da due servizi: un servizio riunioni e un servizio applicazione. Per configurare SSL per entrambi questi servizi, sono necessari due nomi FQDN e due indirizzi IP. Potete condividere il nome FQDN del servizio applicazione con il server di origine, ma il servizio riunioni deve avere un proprio FQDN. Il nome FQDN del server applicazione è l'URL che gli utenti finali devono usare per connettersi ai propri account Acrobat Connect Pro.

Ad esempio, se avete un server periferico e un server di origine, occorrono tre nomi FQDN e tre certificati SSL: uno per ogni servizio riunione e uno condiviso tra i servizi applicazione. Sono necessari quattro indirizzi IP, uno per ogni servizio riunione e uno per ogni servizio applicazione.

In questa configurazione di esempio, il server di origine ha i seguenti indirizzi IP e nomi FQDN:

```
10.192.37.11 = connect.yourcompany.com  
10.192.37.10 = meeting1.yourcompany.com
```

Il server periferico ha i seguenti indirizzi IP e nomi FQDN:

```
10.192.37.100 = connect.yourcompany.com  
10.192.37.101 = edge1.yourcompany.com
```

Nota: se state installando per la prima volta sia il server periferico che il server di origine, impostateli entrambi senza SSL e verificate che possano comunicare tra di loro. Una volta determinato che i server periferico e di origine possono comunicare, potete configurare SSL per entrambi.

Altri argomenti presenti nell’Aiuto

“Implementazione di Acrobat Connect Pro Edge Server” a pagina 27

“Informazioni sul supporto di SSL” a pagina 65

Configurare il server periferico

- 1 Sul server periferico, aprite il file `c:\breeze\edgeserver\custom.ini`.
- 2 Immettete il parametro `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` e impostatelo sull’indirizzo IP o sul nome FQDN del server di origine, come segue:

```
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
```

Per configurare il sistema per la connessione solo tramite SSL, aggiungete un marcatore di commento davanti al parametro `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT`, come segue:

```
# FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

Nota: se il server periferico non riesce a risolvere il nome FQDN del server di origine, usate l’indirizzo IP.

- 3 Nel server di origine, aprite il file `C:\breeze\edgeserver\win32\conf\HttpCache.xml` e aggiornate il tag `<HostName>`, come segue:

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

- 4 Salvate il file `HttpCache.xml`.
- 5 Aprite il file `HttpCache.xml` in un browser Web per verificare la validità dell’XML.

In caso di errori di sintassi, il browser Web presenta un messaggio di errore. Correggete eventuali errori XML e verificate nuovamente il file.

Configurare il server di origine

- 1 Configurate il server di origine per SSL. Per ulteriori informazioni, consultate “SSL (Secure Sockets Layer)” a pagina 65.
- 2 Sul server di origine, aprite il file `c:\breeze\custom.ini` e immettete quanto segue per vincolare il server periferico al server di origine:

```
edge.FCS_EDGE_CLUSTER_ID=1
```

Usate il valore per il parametro `FCS_EDGE_CLUSTER_ID` impostato nel file `custom.ini` del server periferico. In questo esempio, il valore è `sanfran` e il codice è quindi `edge.sanfran=1`.

Nota: il valore 0 è riservato e non può essere usato.

- 3 Riavviate Connect Pro Central Application Server e Connect Pro Meeting Server.
- 4 Scegliete Start > Programmi > Adobe Connect Pro Server 7 > Configura Connect Pro Server 7 per aprire la console di gestione applicazione. Effettuate le seguenti operazioni:
 - a Fate clic su Impostazioni server.
 - b Nella casella Nomi esterni, potete vedere il nome FQDN del server periferico e una casella vuota alla sua destra. Se non vedete il nome FQDN, attendete qualche minuto e aggiornate la finestra del browser.
 - c Immettete il nome FQDN del server periferico nella casella vuota e fate clic su Salva. In questo modo il server periferico viene registrato presso il server di origine.
- 5 Impostate il server DNS locale affinché indirizzi al server periferico gli utenti che richiedono un URL di Acrobat Connect Pro.

Tag XML per SSL

Tag	Valore predefinito	Descrizione
SSLCertificateFile	Nessun valore predefinito.	L'ubicazione del file di certificato da inviare al client. Se non viene specificato un percorso assoluto, si suppone che il certificato sia relativo alla directory Adaptor.
SSLCertificateKeyFile	Nessun valore predefinito.	L'ubicazione del file di chiave privato per il certificato. Se non viene specificato un percorso assoluto, si suppone che il file di chiave sia relativo alla directory Adaptor. Se il file di chiave è crittografato, la frase di autorizzazione deve essere specificata nel tag <code>SSLPassPhrase</code> . L'attributo <code>tipo</code> specifica il tipo di codifica utilizzata per il file di chiave del certificato. Il tipo può essere <code>PEM</code> o <code>ASN1</code> .
SSLCipherSuite	Vedere la descrizione.	L'algoritmo di cifratura. L'algoritmo consiste di elementi delimitati da due punti (:). Possono essere algoritmi di scambio chiave, metodi di autenticazione, metodi di cifratura, tipi di digest oppure uno degli alias selezionati per i raggruppamenti comuni. Per un elenco dei componenti, consultate la documentazione di Flash Media Server. Questo tag ha la seguente impostazione predefinita: <code>ALL: !ADH: !LOW: !EXP: !MD5: @STRENGTH</code> Prima di modificare le impostazioni predefinite, contattate l'assistenza tecnica di Adobe.
SSLPassPhrase	Nessun valore predefinito.	La frase di autorizzazione da utilizzare per decrittografare il file di chiave privata. Se il file di chiave privata non è crittografato, lasciate vuoto questo tag.
SSLSessionTimeout	5	Il tempo durante il quale una sessione attivata da SSL resta valida, in minuti.

Parametri di configurazione SSL

Parametro	Valore predefinito	Descrizione
ADMIN_PROTOCOL	http://	Il protocollo utilizzato dal server dell'applicazione. Impostare su https:// per configurare SSL.
DEFAULT_FCS_HOSTPORT	:1935	La porta utilizzata da Flash Media Server per comunicare utilizzando il protocollo RTMP. Impostare su:-443,1935 per configurare SSL.
HTTPS_PORT	Nessun valore predefinito.	La porta sulla quale il server dell'applicazione ascolta le richieste HTTPS. Di solito questo parametro è impostato su 443 o 8443 per configurare SSL.
SSL_ONLY	no	Impostare su yes se il server supporta solo le connessioni sicure. Questa impostazione forza tutti gli URL di Acrobat Connect Pro a utilizzare HTTPS.
RTMP_SEQUENCE	Nessun valore predefinito.	I server di origine, i server periferici e le porte utilizzati per connettersi a Flash Media Server (il server riunioni).

PKI (Public Key Infrastructure)

Informazioni su PKI (Public Key Infrastructure)

Potete configurare un'infrastruttura a chiave pubblica (PKI) per gestire le credenziali di identificazione come parte dell'architettura di protezione di Acrobat Connect Pro per i client. Nel più familiare protocollo SSL il server deve dimostrare la propria identità al client, mentre nell'infrastruttura PKI è il client che deve dimostrare la propria identità al server.

Una terza parte affidabile, detta autorità di certificazione, verifica l'identità del client e vincola un certificato al client. Il certificato (o *chiave pubblica*) è in formato X.509. Quando il client si connette ad Acrobat Connect Pro, un proxy negozia la connessione per l'infrastruttura PKI. Se il client dispone di un cookie di una sessione precedente o di un certificato valido, viene connesso ad Acrobat Connect Pro.

Per ulteriori informazioni sull'infrastruttura PKI, consultate il centro per la tecnologia PKI Microsoft.

Requisiti utente per l'infrastruttura PKI

Per partecipare a una riunione che richiede l'autenticazione PKI, gli utenti devono usare Windows XP o Windows 2003 e disporre di un certificato client valido installato sul computer locale. Quando un utente partecipa a una riunione, viene visualizzata una finestra di dialogo in cui dovrà scegliere un certificato client valido tra quelli installati sul computer.

È consigliabile che i client usino Adobe Acrobat Connect Add-in per partecipare a una riunione che richiede l'autenticazione PKI. Prima di partecipare a una riunione, occorre installare il componente aggiuntivo sul client mediante il programma di installazione autonomo.

I client possono inoltre usare la versione più recente di Adobe Flash Player nel browser per partecipare alle riunioni. Il supporto per PKI di Flash Player non è tuttavia tanto completo quanto quello del componente aggiuntivo. Per visualizzare gli archivi delle riunioni, i client devono tuttavia disporre della versione più recente di Flash Player.

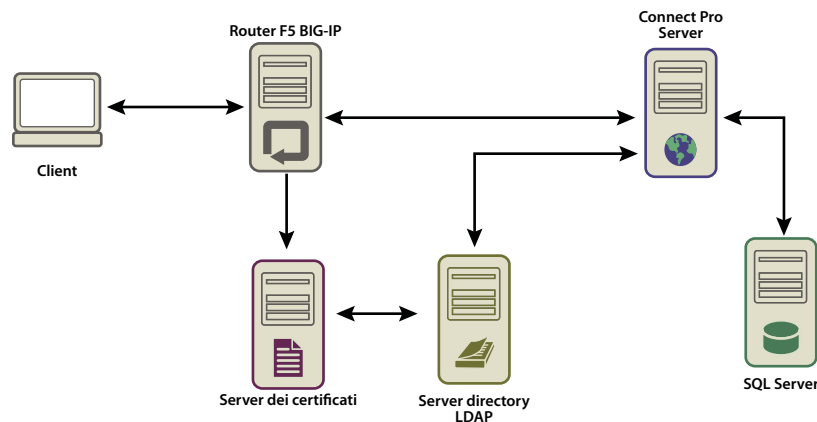
Potete progettare un sistema PKI che richieda l'autenticazione solo delle connessioni HTTP o delle connessioni HTTP ed RTMP. Se decidete di richiedere i certificati client sia per le connessioni HTTP sia per le connessioni RTMP, agli utenti viene richiesto di scegliere il certificato ogni volta che viene stabilita una nuova connessione server. Vengono ad esempio visualizzate due richieste per accedere a una riunione, una volta per HTTP e una volta per RTMP. Poiché non è possibile stabilire una connessione RTMP senza l'autenticazione HTTP, potete scegliere di richiedere l'autenticazione client solo per la connessione HTTP.

Implementazione di PKI

Nella seguente procedura viene descritta un'implementazione di riferimento di infrastruttura PKI configurata con un router F5 BIG-IP LTM 9.1.2 (build 40.2) come proxy. Usate le sezioni più importanti per creare la vostra soluzione con un router F5 o un'altra periferica.

Questa implementazione di riferimento rispetta severi standard di protezione, richiede infatti un certificato client sia per le connessioni HTTP (server applicazioni) sia per le connessioni RTMP (server riunioni).

Nota: Adobe consiglia vivamente di creare un criterio di protezione prima di implementare un'infrastruttura PKI. Nell'infrastruttura PKI vengono usate diverse tecnologie e l'implementazione di un criterio di protezione è fondamentale quando tali sistemi interagiscono.



Flusso di dati in un'infrastruttura a chiave pubblica (PKI)

In questo esempio si parte dai seguenti presupposti:

- Acrobat Connect Pro è installato.
- Acrobat Connect Pro è integrato con un servizio di directory LDAP.
- Un utente importato dal servizio di directory LDAP può partecipare a una riunione gestita da Acrobat Connect Pro.
- È installato un router F5.

1. Configurare il server di directory LDAP.

Per ogni utente dovete specificare un attributo `email` LDAP che viene aggiunto al campo dell'oggetto del certificato client.

La regola iRule F5 cerca in `X.509::subject` l'indirizzo e-mail e ne inserisce il valore nell'intestazione HTTP. Acrobat Connect Pro usa l'intestazione HTTP per autenticare l'utente.

Nota: in questo esempio viene usato l'attributo `email`. Potete usare un qualsiasi identificatore esposto dal formato `X.509`, con un massimo di 254 caratteri e condiviso dal servizio directory LDAP e Acrobat Connect Pro.

2. Configurare il criterio di login di Acrobat Connect Pro.

Acrobat Connect Pro deve usare un indirizzo e-mail per il login utente. In Connect Pro Central, selezionate la scheda Amministrazione, fate clic su Utenti e gruppi e quindi su Modifica criteri di login e password.

3. Configurare un server CA.

Il server CA (autorità di certificazione) gestisce le richieste di certificati, verifica le identità dei client, emette certificati e gestisce un elenco di revoca dei client (CRL, Client Revocation List).

In questa implementazione il server CA fa riferimento al server di directory LDAP per ottenere un certificato client. Il server CA esegue una query nel server LDAP alla ricerca delle informazioni sul client che, se esistenti e non revocate, vengono inserite in un certificato.

Verificate che il certificato client sia installato e utilizzabile analizzando il campo dell'oggetto. Si presenta come segue:

```
E = adavis@asp.sflab.macromedia.com
CN = Andrew Davis
CN = Users
DC = asp
DC = sflab
DC = macromedia
DC = com
```

4. Configurare Acrobat Connect Pro per l'uso dell'autenticazione dell'intestazione HTTP.

Nel file `[root_install_dir]\appserv\conf\WEB-INF\web.xml` rimuovete il commento dal seguente codice:

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

Arrestate il server riunioni e il server applicazione. Nel file `custom.ini` nella directory di installazione principale aggiungete la seguente riga:

```
HTTP_AUTH_HEADER=hah_login
```

Salvate il file `custom.ini` e riavviate Acrobat Connect Pro.

5. Configurare la logica dell'applicazione di F5.

La logica dell'applicazione in F5 cerca l'indirizzo e-mail nel campo oggetto del certificato del client. La logica passa l'indirizzo e-mail ad Acrobat Connect Pro in un'altra intestazione HTTP.

I client senza certificato vengono rifiutati. Se i client dispongono di un certificato, questo deve essere autenticato. Il protocollo OCSP (Online Certification Status Protocol) e la ricerca LDAP sono esempi di meccanismi di autenticazione.

Dopo che il certificato è stato autenticato, analizzatelo alla ricerca di un identificatore univoco noto ad Acrobat Connect Pro. In questo esempio un certificato valido viene analizzato alla ricerca di un indirizzo e-mail.

Una richiesta che include la stringa `session` o ha un cookie `BREEZESSESSION` può passare senza autenticazione perché il client è già stato autenticato. (Acrobat Connect Pro verifica questi argomenti tramite una query nel database.)

Se la richiesta non include la stringa `session` o il cookie `BREEZESSESSION`, l'utente deve accedere ad Acrobat Connect Pro. Per far accedere un utente, inserite l'identificatore univoco (in questo caso l'indirizzo e-mail) nel campo `HTTP_AUTH_HEADER` e reindirizzate la richiesta alla pagina di login di Acrobat Connect Pro.

Il seguente codice è una regola iRule F5 inserita nel profilo HTTPS che gestisce le richieste:

```

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]]
}

```

Altri argomenti presenti nell’Aiuto

“[Avviare e arrestare Acrobat Connect Pro Server](#)” a pagina 87

Protezione dell’infrastruttura

Protezione della rete

Per le comunicazioni Acrobat Connect Pro si avvale di diversi servizi TCP/IP privati. Tali servizi aprono diverse porte e canali che devono essere protetti dagli utenti esterni. Per Acrobat Connect Pro è necessario proteggere le porte più delicate mediante un firewall, che supporti l’ispezione del contenuto dei pacchetti e non solo i filtri pacchetti). Tale firewall deve essere dotato di un’opzione che neghi tutti i servizi per impostazione predefinita, ad eccezione di quelli consentiti in modo esplicito. Il firewall deve inoltre avere due o più interfacce di rete. Questa architettura consente di impedire che utenti non autorizzati scavalchino la protezione del firewall.

La soluzione più semplice per proteggere Acrobat Connect Pro consiste nel bloccare tutte le porte sul server, ad eccezione delle porte 80, 1935 e 443. Un dispositivo firewall hardware esterno offre un livello di protezione da eventuali carenze nel sistema operativo. Potete configurare livelli di firewall hardware per creare reti perimetrali. Se il server viene aggiornato regolarmente dal reparto IT con le più recenti patch di protezione Microsoft, potete configurare un firewall software per garantire un’ulteriore protezione.

Accesso dalla rete intranet

Affinché gli utenti possano accedere ad Acrobat Connect Pro dalla rete intranet, i server e il database di Acrobat Connect Pro devono risiedere in una subnet distinta, separata da un firewall. Per ostacolare l'indirizzamento (da parte di un utente malintenzionato) del traffico a un IP pubblico e dall'IP interno decodificato dell'indirizzo di rete, il segmento di rete interno in cui è installato Acrobat Connect Pro deve usare indirizzi IP privati (10.0.0.0/8, 172.16.0.0/12 o 192.168.0.0/16). Per ulteriori informazioni, consultate RFC 1918. Questa configurazione del firewall deve tenere conto di tutte le porte di Acrobat Connect Pro e se tali porte sono configurate per il traffico in ingresso o in uscita.

Protezione del server del database

Sia che il database risieda sullo stesso server di Acrobat Connect Pro o su un server diverso, accertatevi che sia protetto. I computer su cui risiede un database devono trovarsi in una posizione fisicamente protetta. Di seguito sono riportate alcune precauzioni supplementari da prendere:

- Installate il database nell'area protetta dell'Intranet dell'organizzazione.
- Non collegate mai il database direttamente a Internet.
- Eseguite regolarmente il backup dei dati e archiviate le copie in un luogo protetto fuori sede.
- Installate le patch più recenti per il server del database.
- Utilizzate connessioni SQL affidabili.

Per informazioni sulla protezione di SQL Server, consultate il sito Web sulla protezione di Microsoft SQL.

Creare account di servizio

La creazione di un account di servizio per Acrobat Connect Pro vi consente di eseguire Acrobat Connect Pro in modo più sicuro. Adobe consiglia di creare un account di servizio e un account di servizio SQL Server 2005 Express Edition per Acrobat Connect Pro. Per ulteriori informazioni, consultate gli articoli 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" (Come modificare l'account di servizio di SQL Server o SQL Server Agent senza usare SQL Enterprise Manager in SQL Server 2000 o Gestione configurazione SQL Server in SQL Server 2005) e "The Services and Service Accounts Security and Planning Guide" (Guida alla pianificazione e alla protezione di servizi e account di servizio).

Creare un account di servizio

- 1 Create un account locale denominato ConnectService che non includa gruppi predefiniti.
- 2 Impostate il servizio Adobe Connect Enterprise Service, il servizio Flash Media Administration Server e il servizio Flash Media Server (FMS) su questo nuovo account.
- 3 Impostate "Controllo completo" per la seguente chiave del Registro di sistema:
HKLM\SYSTEM\ControlSet001\Control\MediaProperties\PrivateProperties\Joystick\Winmm
- 4 Impostate "Controllo completo" per le cartelle NTFS nella cartella principale di Acrobat Connect Pro (per impostazione predefinita, c:\breeze).

Le sottocartelle e i file devono avere le stesse autorizzazioni. Per i cluster modificate i percorsi corrispondenti su ogni nodo di computer.

- 5 Impostate i seguenti diritti di accesso per l'account ConnectService:

Accesso come servizi: SeServiceLogonRight

Creare un account di servizio SQL Server 2005 Express Edition

- 1 Create un account locale denominato ConnectSqlService che non includa gruppi predefiniti.
- 2 Modificate l'account di servizio SQL Server 2005 Express Edition LocalSystem in ConnectSqlService.
- 3 Impostate "Controllo completo" per ConnectSqlService per le seguenti chiavi del Registro di sistema:

```
HKEY_LOCAL_MACHINE\Software\Clients\Mail  
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\80  
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\[databaseInstanceName]
```

Per i cluster eseguite questa operazione su ogni nodo del cluster. L'autorizzazione Controllo completo viene applicata a tutte le chiavi figlio di un'istanza di database denominata.

- 4 Impostate "Controllo completo" per ConnectSqlService per le cartelle del database. Le sottocartelle e i file devono avere le stesse autorizzazioni. Per i cluster modificate i percorsi corrispondenti su ogni nodo di computer.
- 5 Impostate i seguenti diritti utente per il servizio ConnectSqlService:

Agisci come parte del sistema operativo: SeTcbPrivilege. Ignorare il controllo incrociato: SeChangeNotify. Blocco di pagine in memoria: SeLockMemory. Accesso come processo batch: SeBatchLogonRight. Accesso come servizio: SeServiceLogonRight. Sostituzione di token a livello di processo: SeAssignPrimaryTokenPrivilege.

Proteggere le installazioni su un solo server

Il seguente flusso di lavoro riepiloga il processo relativo all'installazione e alla protezione di Acrobat Connect Pro su un solo computer. Si parte dal presupposto che il database venga installato sullo stesso computer e che gli utenti accedano ad Acrobat Connect Pro su Internet.

1. Installare un firewall.

Poiché consentite agli utenti di accedere ad Acrobat Connect Pro da Internet, il server è facilmente accessibile anche da parte di utenti malintenzionati. L'uso di un firewall vi consente di bloccare l'accesso al server e controllare le comunicazioni che avvengono tra Internet e il server.

2. Configurare il firewall.

Dopo che avete installato il firewall, configuratelo nel modo seguente:

- Porte in ingresso (da Internet): 80, 443, 1935.
- Porte in uscita (verso il server di posta elettronica): 25.
- Usate solo il protocollo TCP/IP.

Poiché il database si trova sullo stesso server in cui è installato Acrobat Connect Pro, non dovete aprire la porta 1434 sul firewall.

3. Installare Acrobat Connect Pro.

4. Verificare il funzionamento delle applicazioni Acrobat Connect Pro.

Dopo avere installato Acrobat Connect Pro, verificate che funzioni correttamente sia da Internet sia dalla rete locale.

5. Verificare il firewall.

Dopo che avete installato e configurato il firewall, dovete verificare che funzioni correttamente. Verificate il firewall provando a usare le porte bloccate.

Proteggere i cluster

I sistemi cluster (con più server) sono più complessi delle configurazioni a server unico. Un cluster di Acrobat Connect Pro può essere ubicato in un centro dati o distribuito geograficamente in più centri operativi di rete. Potete installare e configurare i server sui cui risiede Connect Pro in diverse ubicazioni e quindi sincronizzarli attraverso la replica del database.

Nota: I cluster devono utilizzare Microsoft SQL Server 2005 Standard Edition, non il motore del database incorporato.

Di seguito sono riportati consigli importanti per proteggere i cluster:

Reti private La soluzione più semplice per i cluster in una singola ubicazione consiste nel creare una subnet supplementare per il sistema Acrobat Connect Pro. Questo approccio offre un livello elevato di protezione.

Firewall software locali Nel caso di server di Acrobat Connect Pro inclusi in un cluster e che condividono una rete pubblica con altri server, è consigliabile installare un firewall software su ogni singolo server.

Sistemi VPN Nel caso di installazioni con più server in cui i computer su cui è installato Acrobat Connect Pro si trovano in diverse posizioni fisiche, è consigliabile usare un canale crittografato per comunicare con i server remoti. Numerosi fornitori di software e hardware offrono tecnologia VPN per proteggere le comunicazioni con i server remoti. Acrobat Connect Pro si basa su questa soluzione di protezione esterna se il traffico di dati deve essere crittografato.

Risorse e consigli per la protezione

Procedure consigliate per la protezione

Il seguente elenco di controllo descrive le procedure migliori per proteggere il sistema Acrobat Connect Pro:

Usare SSL per proteggere il traffico di rete Potete proteggere la connessione al server riunioni, al server dell'applicazione o a entrambi.

Eseguire solo i servizi necessari Non eseguite applicazioni quale un controller di dominio, un server Web o un server FTP sullo stesso computer in cui è in esecuzione Acrobat Connect Pro. Per ridurre il rischio che un'altra applicazione possa essere usata per compromettere il server, riducete il numero di applicazioni e servizi in esecuzione sul computer in cui è installato Acrobat Connect Pro.

Aggiornare la protezione del sistema operativo Controllate regolarmente la disponibilità di aggiornamenti critici che risolvono problemi di protezione e applicate le patch necessarie. Un firewall elimina alcuni di tali problemi di protezione. In generale, accertatevi che sui server siano sempre installati i più recenti aggiornamenti di protezione approvati da Microsoft e dagli altri fornitori della vostra piattaforma.

Proteggere i sistemi host Se sui server memorizzate informazioni riservate, è importante conoscere la protezione fisica dei sistemi che usate. Acrobat Connect Pro si avvale della protezione del sistema host contro gli utenti malintenzionati. I server che contengono dati riservati devono pertanto essere protetti. Acrobat Connect Pro è progettato per sfruttare le funzioni dell'ambiente nativo quale la crittografia del file system.

Usare password complesse Una password complessa è efficiente nella protezione dei dati. Gli amministratori di Acrobat Connect Pro possono configurare criteri di login e password in Connect Pro Central. Le installazioni di Acrobat Connect Pro usano spesso Microsoft SQL Server 2005 Standard Edition, che richiede anch'esso una protezione mediante password complessa.

Usare l'autenticazione LDAP o Single Sign On È consigliabile utilizzare LDAP o Single Sign On per l'autenticazione di Connect Pro. Se utilizzate un'autenticazione diversa, assicuratevi che gli utenti utilizzino per Connect Pro una password diversa da quella utilizzata per i sistemi aziendali.

Eseguire regolarmente controlli della protezione Controllate periodicamente i sistemi per garantire che tutte le funzioni di protezione funzionino nel modo appropriato. Potete ad esempio usare un analizzatore di porte per verificare il firewall.

Riferimenti e risorse per la protezione

Le seguenti risorse vi possono essere d'aiuto per proteggere i server:

Protezione della rete Il SANS (System Administration, Networking, and Security) Institute è un'organizzazione di ricerca e formazione che conta sulla collaborazione di amministratori di sistema, professionisti nel campo della protezione e amministratori di rete. Offre corsi sulla protezione delle rete nonché la certificazione nella protezione della rete.

Protezione di SQL Server Le pagine delle risorse relative alla protezione di Microsoft SQL disponibili nel sito Web Microsoft offrono informazioni sulla protezione di SQL Server.

Strumenti Nmap è un programma avanzato di analisi delle porte che indica quali porte sono usate da un sistema. È disponibile gratuitamente grazie alla licenza GPL (General Public License) di GNU.

***Nota:** l'efficacia delle misure di protezione adottate dipende da vari fattori, ad esempio dalle misure di protezione fornite dal server e dal software di protezione installato. Il software Acrobat Connect Pro non garantisce la protezione del server o delle informazioni in esso archiviate. Per ulteriori informazioni, consultate la dichiarazione di non responsabilità di garanzia inclusa nel contratto di licenza di Acrobat Connect Pro.*

Capitolo 5: Amministrazione di Connect Pro Server

L'amministrazione di Acrobat Connect Pro Server implica le seguenti attività:

- Gestione e monitoraggio dei file di registro per evitare tempi di inattività
- Gestione dello spazio su disco
- Backup dei dati
- Creazione e generazione dei rapporti di utilizzo

Avviare e arrestare i server

Avviare e arrestare Acrobat Connect Pro Server

Potete avviare o arrestare Acrobat Connect Pro dal menu Start, dalla finestra Servizi o dalla riga di comando. Verificate che il database sia in esecuzione prima di avviare Connect Pro Server.

Arrestare Acrobat Connect Pro dal menu Start

- 1 Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Application Server.
- 2 Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Meeting Server.

Avviare Acrobat Connect Pro dal menu Start

- 1 Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Meeting Server.
- 2 Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Application Server.

Arrestare Acrobat Connect Pro dalla finestra Servizi

- 1 Scegliete Start > Pannello di controllo > Strumenti di amministrazione > Servizi per aprire la finestra Servizi.
- 2 Arrestate il servizio Adobe Connect Enterprise Service .
- 3 Arrestate il servizio Flash Media Server (FMS).
- 4 Arrestate il servizio Flash Media Administration Server.

Avviare Acrobat Connect Pro dalla finestra Servizi

- 1 Scegliete Start > Pannello di controllo > Strumenti di amministrazione > Servizi per aprire la finestra Servizi.
- 2 Avviate il servizio Flash Media Server (FMS).
- 3 Avviate il servizio Flash Media Server Administration Server.
- 4 Avviate il servizio Adobe Connect Enterprise Service .

Arrestare Acrobat Connect Pro dalla riga di comando

- 1 Scegliete Start > Esegui per aprire la finestra Esegui. Digitate **cmd** per aprire un prompt dei comandi.
- 2 Andate alla directory breeze\appserv\win32.
- 3 Digitate il comando seguente per arrestare Acrobat Connect Pro:

```
net stop ConnectPro
```

- 4 Digitate il testo seguente per arrestare Flash Media Server:

```
net stop FMS
```

- 5 Digitate il testo seguente per arrestare Flash Media Server Administration Server:

```
net stop FMSAdmin
```

Avviare Acrobat Connect Pro dalla riga di comando

- 1 Scegliete Start > Esegui per aprire la finestra Esegui. Digitate **cmd** per aprire un prompt dei comandi.
- 2 Andate alla directory breeze\appserv\win32.
- 3 Digitate il testo seguente per avviare Flash Media Server:

```
net start FMS
```

- 4 Digitate il testo seguente per avviare Flash Media Server Administrator Server:

```
net start FMSAdmin
```

- 5 Digitate il testo seguente per avviare Acrobat Connect Pro:

```
net start ConnectPro
```

Avviare e arrestare Connect Pro Presence Service

Connect Pro Presence Service può essere avviato e arrestato dal menu Start o dalla finestra Servizi. Avviate Connect Pro Presence Service solo se il sistema Acrobat Connect Pro è integrato con Microsoft Live Communications Server or Office Communications Server.

Altri argomenti presenti nell’Aiuto

“[Integrazione con Microsoft Live Communications Server 2005 e Microsoft Office Communications Server 2007](#)” a pagina 51

Arrestare il servizio di presenza dal menu Start

- ❖ Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Presence Service.

Avviare il servizio di presenza dal menu Start

- ❖ Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Presence Service.

Arrestare, avviare o riavviare il servizio di presenza dalla finestra Servizi

- 1 Scegliete Start > Pannello di controllo > Strumenti di amministrazione > Servizi per aprire la finestra Servizi.
- 2 Selezionate Acrobat Connect Pro Presence Service.
- 3 Scegliete Avvia, Arresta o Riavvia il servizio.

Avviare e arrestare Flash Media Gateway

Potete avviare o arrestare Flash Media Gateway dalla finestra Servizi o dalla riga di comando. Prima di avviare Flash Media Gateway, verificate che Connect Pro Server sia in esecuzione.

Avviare e arrestare Flash Media Gateway dalla finestra Servizi

- 1 Scegliete Start > Pannello di controllo > Strumenti di amministrazione > Servizi per aprire la finestra Servizi.
- 2 Selezionate Flash Media Gateway Service.
- 3 Scegliete Avvia, Arresta o Riavvia il servizio

Avviare e arrestare Flash Media Gateway dalla riga di comando

- 1 Scegliete Start > Esegui per aprire la finestra Esegui. Digitate **cmd** per aprire un prompt dei comandi.
- 2 Digitate il testo seguente per avviare Flash Media Gateway:

```
net start fmg
```

- 3 Digitate il testo seguente per arrestare Flash Media Gateway:

```
net stop fmg
```

Avviare e arrestare Acrobat Connect Pro Edge Server

Potete avviare o arrestare Acrobat Connect Pro Edge Server 7 dal menu Start, dalla finestra Servizi e dalla riga di comando.

Arrestare Acrobat Connect Pro Edge Server 7 dal menu Start

- ❖ Scegliete Start > Programmi > Adobe Acrobat Connect Pro Edge Server 7 > Arresta Connect Pro Edge Server.

Avviare Acrobat Connect Pro Edge Server 7 dal menu Start

- ❖ Scegliete Start > Programmi > Adobe Acrobat Connect Edge Server 7 > Avvia Connect Pro Edge Server.

Arrestare Acrobat Connect Pro Edge Server 7 dalla finestra Servizi

- 1 Scegliete Start > Impostazioni > Pannello di controllo > Strumenti di amministrazione > Servizi per aprire la finestra Servizi.
- 2 Arrestate il servizio Flash Media Server (FMS).
- 3 Arrestate il servizio Flash Media Server Administration Server.

Avviare Acrobat Connect Pro Edge Server dalla finestra Servizi

- 1 Scegliete Start > Impostazioni > Pannello di controllo > Strumenti di amministrazione > Servizi per aprire la finestra Servizi.
- 2 Avviate il servizio Flash Media Server Administration Server.
- 3 Avviate il servizio Flash Media Server (FMS).

Arrestare Acrobat Connect Pro Edge Server dalla riga di comando

- 1 Scegliete Start > Esegui per aprire la finestra Esegui. Digitate **cmd** per aprire un prompt dei comandi.
- 2 Digitate il testo seguente per arrestare Flash Media Server:

```
net stop FMS
```

3 Digitate il testo seguente per arrestare Flash Media Server Administrator Server:

```
net stop FMSAdmin
```

Avviare Acrobat Connect Pro Edge Server dalla riga di comando

1 Scegliete Start > Esegui per aprire la finestra Esegui. Digitate **cmd** per aprire un prompt dei comandi.

2 Digitate il testo seguente per avviare Flash Media Server Administrator Server:

```
net start FMSAdmin
```

3 Digitate il testo seguente per avviare Flash Media Server:

```
net start FMS
```

Gestione e monitoraggio dei registri

I file di registro

I file di registro di Acrobat Connect Pro Server consentono di visualizzare informazioni sugli eventi che si verificano durante le operazioni. Potete usare le informazioni presenti nei file di registro per creare meccanismi e rapporti di monitoraggio e per risolvere i problemi. I file di registro forniscono informazioni sulle attività dell'utente e sulle prestazioni del server. Ad esempio, i file di registro possono indicare il motivo per cui a un utente è stato negato l'accesso quando ha tentato di eseguire il login, oppure il motivo per cui una connessione telefonica si è interrotta.

Acrobat Connect Pro Server include 5 file di registro nella cartella *RootInstallationFolder\logs*. Usate i file di registro *access.log* ed *error.log* per monitorare Acrobat Connect Pro. Gli altri 3 file di registro sono interni e non sono necessari per utilizzare il sistema.

access.log Contiene informazioni su tutti i tentativi di accesso al server.

breeze.log Contiene informazioni sull'avvio o meno dell'applicazione *ConnectPro.exe*.

error.log Contiene informazioni su problemi del sistema.

service-err.log Contiene informazioni sugli errori dell'applicazione e sull'avvio.

service-out.log Contiene i messaggi *STDOUT* e *STDERR* generati dalla macchina virtuale Java.

Voce di file di registro di esempio

La seguente voce di esempio del file *access.log* include un'intestazione, un elenco dei campi utilizzati nella voce di registro e i dati specifici per tale voce di 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=breezxn5pquysyshfgttt, ip=138.1.21.100} GET http://joeuser.macromedia.com&mode=xml 0
20/5 0
```

La tabella seguente spiega la voce di esempio:

Campo	Dati	Descrizione
date	2006-10-30	La data in cui si è verificato l'evento registrato.
time	18:12:50	L'ora in cui si è verificato l'evento registrato.
x-comment	Login non eseguito.	Indica che un utente non è stato in grado di eseguire il login al server dell'applicazione.
x-module	PRINCIPAL	L'evento si è verificato nel modulo Principal nel server dell'applicazione.
x-status	NO_ACCESS_NO_LOGIN	Indica che l'utente non è stato in grado di eseguire il login.
x-severity	W	Identifica la gravità dell'evento come avviso (W).
x-category	A	Indica che l'evento è un problema di accesso (A) (segnalato nel file access.log).
x-user	PUBLIC	L'utente corrente; in questo caso, un ospite non identificato o un utente pubblico.
x-access-request	http://joeuser.macromedia.com&mode=xml	Origine della richiesta.
time-taken	0	Per l'elaborazione di questa richiesta è stato necessario un tempo pari a zero.
db-logical-io	20/5	Sono state necessarie 20 letture del database e sono state restituite 5 righe di dati.
db-transaction-update-count	0	Durante l'elaborazione di questa richiesta non è stata aggiornata nessuna riga di database.

Rotazione dei file di registro

Potete ruotare i file access.log ed error.log. Modificate i valori predefiniti dei seguenti parametri nel file custom.ini (per impostazione predefinita, si trovano in *RootInstallationFolder\custom.ini*) per specificare con quale frequenza vengono ruotati i file di registro.

```
ACCESS_LOG_ROTATE_DAYS=1.0
ACCESS_LOG_ROTATE_KEEP=7
ERROR_LOG_ROTATE_DAYS=1.0
ERROR_LOG_ROTATE_KEEP=7
```

I parametri `*_DAYS` determinano la frequenza con la quale i file di registro vengono ruotati, in giorni. Usate il valore 0.5 per mezza giornata.

I parametri `*_KEEP` determinano per quanti giorni vengono conservati i file di registro prima di essere eliminati. Per impostazione predefinita, i file di registro vengono conservati per una settimana.

Dopo aver modificato il file custom.ini, riavviate Connect Pro Central Application Server.

Formato dei file di registro

I file di registro utilizzano il formato di file registro esteso W3C, leggibile con qualsiasi editor di testo.

Campi di registro nei file access.log e error.log

Ciascuna voce di registro contiene 11 campi di registro, i quali forniscono informazioni sul tipo di evento verificatosi, sul punto in cui si è verificato, sulla sua gravità e altri dati pertinenti:

Campo	Formato	Descrizione
date	AAAA/MM/GG	Data in cui è stata completata la transazione
time	OO:MM:SS	Ora del computer locale in cui è stata completata la transazione
x-comment	Stringa	Contiene informazioni leggibili dall'utente sulla voce di registro. Questo campo si trova sempre all'estrema sinistra.
x-module	Stringa	Indica dove si è verificato l'errore.
x-status	Stringa	Indica quale evento si è verificato.
x-severity	Testo (un carattere)	Indica se l'evento registrato è critico (C), un errore (E), un avviso (W) o un'informazione (I).
x-category	Testo (un carattere)	Indica se la voce di registro rappresenta un evento di accesso (A) o di sistema (S).
x-user	Stringa	Testo che rappresenta l'utente corrente. Applicabile solo se x-category è un accesso (A); altrimenti il campo viene impostato su un singolo trattino (-) a indicare un campo inutilizzato.
x-access-request	Stringa	Testo che rappresenta la richiesta di accesso. Questo testo può essere un nome di URL o di API con i parametri trasmessi. Applicabile solo se x-category è un accesso (A); altrimenti questo campo viene impostato su un singolo trattino (-) a indicare un campo inutilizzato.
time-taken	Numero	Tempo necessario per l'elaborazione della richiesta (in secondi). Applicabile solo se x-category è un accesso (A); altrimenti questo campo viene impostato su un singolo trattino (-) a indicare un campo inutilizzato.
db-logical-io	Stringa	Numero di letture del database necessarie per elaborare la richiesta e numero di righe restituite nel formato <reads>/<rows>.
db-transaction-update-count	Stringa	Numero di righe aggiornate nelle transazioni durante l'elaborazione delle richieste. Se la richiesta utilizza più di una transazione, questo valore è la somma di tutti gli aggiornamenti.

Voci dei campi modulo

Un modulo è un componente del server che gestisce alcuni insiemi di operazioni correlate. Ciascun modulo appartiene o al server dell'applicazione o al server della riunione. Il campo x-module indica se l'evento del registro si è verificato:

Voce di registro per il campo x-module	Descrizione	Server
ACCESS_KEY	Gestisce le chiavi di accesso.	Server applicazioni
ACCOUNT	Gestisce le operazioni con gli account.	Server applicazioni
ACL	Gestisce le operazioni relative ad ACL.	Server applicazioni
AICC	Gestisce tutte le comunicazioni AICC tra il server e il contenuto.	Server applicazioni
BUILDER	Esegue le build SCO.	Server applicazioni
Client	Metodi del client	Server riunioni
CLUSTER	Gestisce tutte le operazioni relative al cluster.	Server applicazioni
CONSOLE	Gestisce tutte le operazioni relative alla console.	Server applicazioni
Content	Contenitore Condivisione	Server riunioni
DB	Rappresenta il database.	Server applicazioni
EVENT	Gestisce tutte le operazioni relative all'evento.	Server applicazioni
HOSTED_MANAGER	Gestisce gli account del sistema (creazione, aggiornamento, eliminazione, impostazioni e così via).	Server applicazioni

Voce di registro per il campo x-module	Descrizione	Server
MEETING	Gestisce tutte le operazioni relative alla riunione.	Server applicazioni
Misc	Modulo vario.	Server riunioni
NOTIFICATION	Gestisce tutte le operazioni relative alle e-mail.	Server applicazioni
PERMISSION	Gestisce tutte le operazioni relative alle autorizzazioni.	Server applicazioni
Poll	Contenitore Sondaggio	Server riunioni
PLATFORM_FRAMEWORK	Rappresenta il framework della piattaforma.	Server applicazioni
PRINCIPAL	Gestisce tutte le operazioni relative ai principali.	Server applicazioni
REPORT	Rappresenta i rapporti.	Server applicazioni
Room	Gestisce l'apertura e la chiusura della stanza riunioni.	Server riunioni
RTMP	Rappresenta il gestore RTMP	Server applicazioni
SCO	Gestisce tutte le operazioni relative agli SCO.	Server applicazioni
SEARCH	Gestisce tutte le operazioni relative alla ricerca.	Server applicazioni
START_UP	Rappresenta il componente di avvio.	Server applicazioni
TELEPHONY	Gestisce tutte le operazioni relative alla telefonia.	Server applicazioni
TRACKING	Gestisce tutte le operazioni relative alla trascrizione.	Server applicazioni
TRAINING	Gestisce tutte le operazioni relative alla formazione.	Server applicazioni

Voci dei campi commento e stato

I campi x-comment e x-status indicano quale tipo di evento si è verificato. Il campo x-status fornisce un codice per ciascun evento registrato. Il campo x-comment fornisce una descrizione leggibile di ciascun evento registrato.

Nella seguente tabella sono elencati i codici di stato, il commento associato a ciascun codice di stato e una spiegazione di ciascun evento registrato:

Voce di registro per il campo x-status	Voce di registro per il campo x-comment	Descrizione
ACCESS_DENIED	Client trying to access protected method. Access is denied. {1}	Registrato quando il cliente tenta di accedere al metodo protetto.
BECAME_MASTER	Server {1} has been designated the master.	Registrato quando il pianificatore esce e questo server diventa il pianificatore.
CLUSTER_CON_BROKEN	Server {1} unable to reach {2} on port {3} to perform cluster operations.	Registrato quando Acrobat Connect Pro non è in grado di raggiungere un altro server nel cluster.
CLUSTER_FILE_TRANSFER_ERROR	Unable to transfer {1} from server {2}.	Registrato quando viene restituito un errore durante il trasferimento di un file.
CONNECT	New client connecting: {1}	Registrato quando si connette un nuovo client.

Voce di registro per il campo x-status	Voce di registro per il campo x-comment	Descrizione
CONNECT_WHILE_GC	Connecting while the application is shutting down - forcing shutdown.	Registrato quando il client tenta di connettersi durante la chiusura dell'applicazione.
DB_CONNECTION_ERROR	Unable to connect to database {1}.	Registrato quando Acrobat Connect non riesce a raggiungere il database.
DB_CONNECTION_TIME_OUT	Timed out waiting for database connection.	Registrato quando la connessione del database richiede un tempo eccessivo.
DB_VERSION_ERROR	Database {1} is incompatible with the current version of Acrobat Connect Pro.	Registrato quando il database non è aggiornato.
DISCONNECT	A client is leaving. Details: {1}	Registrato quando il client si disconnette.
EXT_ERROR	External error thrown by a third party.	Registrato quando il codice esterno ha restituito un errore.
FMS_CON_BROKEN	Health check failed due to broken FMS service connection.	Registrato quando la connessione del servizio viene interrotta.
FMS_NOT_FOUND	Unable to connect to FMS at startup.	Registrato quando Acrobat Connect non è in grado di stabilire la connessione del servizio all'avvio.
INTERNAL_ERROR	Internal error occurred.	Registrato quando viene restituito un errore interno.
INVALID	-	Registrato quando viene tentata l'esecuzione di un'operazione non valida.
INVALID_DUPLICATE	Value {1} is a duplicate in the system.	Registrato quando il valore immesso duplica un valore nel sistema.
INVALID_FORMAT	Field {1} of type {2} is invalid.	Il valore specificato non è valido per questo campo.
INVALID_ILLEGAL_OPERATION	Illegal operation performed.	L'operazione richiesta non è consentita.
INVALID_ILLEGAL_PARENT	-	Registrato quando un ACL ha una cartella principale non valida. Ad esempio, se la cartella A si trova all'interno della cartella B, la cartella B non può trovarsi nella cartella A.
INVALID_MISSING	Field {1} of type {2} is missing.	Valore obbligatorio mancante per questo campo.
INVALID_NO_SUCH_ITEM	Value {1} is an unknown in the system.	L'elemento richiesto non esiste.
INVALID_RANGE	The specified value must be between {1} and {2}.	Registrato quando il valore immesso non è compreso nell'intervallo.
INVALID_TELEPHONY_FIELD	Telephony authentication values were not validated by the service provider.	Il fornitore del servizio non è in grado di convalidare l'account di telefonia.
INVALID_VALUE_GTE	The specified value must be greater than or equal to {1}.	Registrato quando il valore immesso non è compreso nell'intervallo.
INVALID_VALUE_LTE	The specified value must be less than or equal to {1}.	Registrato quando il valore immesso non è compreso nell'intervallo.
KILLING_LONG_CONNECTION	Client has been in the room for 12 hours, disconnecting.	Registrato quando la connessione del client viene interrotta dopo il raggiungimento del limite.

Voce di registro per il campo x-status	Voce di registro per il campo x-comment	Descrizione
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.	Registrato quando il cliente utilizza Acrobat Connect Pro durante il periodo di uso gratuito e l'accesso sta per essere disattivato.
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.	Registrato quando la licenza scadrà dopo 15 giorni o meno.
MASTER_THREAD_TIMED_OUT	Master thread has not reported progress in {1} milliseconds.	Thread del pianificatore non in esecuzione.
MEETING_BACKUP_END	Server {1} is no longer the backup for room {2}.	Il backup della riunione è finito.
MEETING_BACKUP_START	Server {1} is now the backup for room {2}.	Il backup della riunione è iniziato.
MEETING_FAILOVER	Meeting {1} failed over to {2}.	Registrato quando una riunione genera un errore su questo server.
MEETING_TMP_READ	Meeting template {1} read for room {2}.	Modello letto dalla riunione.
MEETING_TMP_WRITTEN	Meeting template {1} written to room {2}.	Modello scritto nella riunione.
NO_ACCESS_ACCOUNT_EXPIRED	Your account has expired.	L'account sul quale avete eseguito l'accesso è scaduto.
NO_ACCESS_DENIED	Permission check failed.	Errore di controllo dell'autorizzazione.
NO_ACCESS_LEARNER	No permission to take courses.	Per seguire il corso è necessario essere membri del gruppo di utenti.
NO_ACCESS_LEARNING_PATH_BLOCKED	You have not fulfilled a prerequisite or preassessment.	Errore di prerequisito o valutazione preliminare.
NO_ACCESS_NO_EXTERNAL_USER_MODIFICATION	External users cannot be modified.	All'utente non è concesso modificare gli utenti LDAP.
NO_ACCESS_NO_LICENSE_FILE	Your license file has not been uploaded.	File della licenza non trovato.
NO_ACCESS_NO_LOGIN	Not logged in.	Errore restituito quando l'utente non ha eseguito il login.
NO_ACCESS_NO_QUOTA	A {1} quota error occurred for account {2} with limit {3}.	La quota ha superato il limite.
NO_ACCESS_NO_RETRY	You have reached the max limit and can not take the course again.	L'utente ha superato il numero massimo di tentativi consentiti per il corso.
NO_ACCESS_NO_SERVER	Server not available	Il server richiesto non è disponibile.
NO_ACCESS_NOT_AVAILABLE	The requested resource is unavailable.	Registrato quando la risorsa richiesta non è disponibile.
NO_ACCESS_NOT_SECURE	SSL request made on a non-SSL server.	Richiesta sicura effettuata su server non sicuro.
NO_ACCESS_PASSWORD_EXPIRED	Your password has expired.	Registrato quando la password di un utente è scaduta.
NO_ACCESS_PENDING_ACTIVATION	Your account has not been activated yet.	L'account non è ancora attivato.
NO_ACCESS_PENDING_LICENSE	Your account activation is pending a license agreement.	L'account non può essere utilizzato fino a quando non verrà letto il contratto di licenza.

Voce di registro per il campo x-status	Voce di registro per il campo x-comment	Descrizione
NO_ACCESS_SCO_EXPIRED	The course you tried to access is no longer available.	La data finale del corso è trascorsa.
NO_ACCESS_SCO_NOT_STARTED	Course is not open yet.	La data iniziale del corso non è stata raggiunta.
NO_ACCESS_WRONG_ZONE	Content accessed from wrong zone.	Restituito quando il contenuto o l'utente accede a un server nella zona sbagliata.
NO_DATA	Permission check failed.	La query non ha restituito nessun dato.
NO_DISKSPACE	Health check failed due to lack of disk space.	Registrato quando sul disco non vi è spazio sufficiente per l'account.
NOT_AVAILABLE	Requested resource is not available.	Errore restituito quando la risorsa non è disponibile.
OK	-	Richiesta elaborata con successo.
OPERATION_SIZE_ERROR	Operation too large to complete.	Registrato quando l'operazione non può essere completata a causa delle dimensioni.
REQUEST_RETRY	Unable to process request. Please try again.	Errore nella richiesta.
RESPONSE_ABORTED	Client that made request is not available to receive response.	Registrato quando l'utente chiude il browser prima che il server riesca a restituire la risposta.
RTMP_SVC_BLOCKED	Acrobat Connect Pro service request blocked from {1} because the server has not fully started up yet.	La connessione del servizio è stata richiesta per l'oggetto SCO, ma il server si sta ancora avviando.
RTMP_SVC_CLOSED	Acrobat Connect Pro service connection closed for {1}.	Connessione del servizio chiusa per l'oggetto SCO.
RTMP_SVC_REQUEST	Acrobat Connect Pro service request received from {1}.	Connessione del servizio richiesta dallo SCO.
RTMP_SVC_START	Acrobat Connect Pro service connection established with {1}.	Connessione del servizio stabilita con lo SCO.
SCRIPT_ERROR	Run-Time Script Error. Details: {1}	Registrato quando viene rilevato un errore dello script.
SERVER_EXPIRED	Health check failed due to server expiry (expiry date={1}, current time={2}).	Registrato quando il server non trasmette il controllo del funzionamento prima del timeout.
SOME_ERRORS_TERMINATED	Some actions terminated with an error.	Registrato quando un errore provoca l'interruzione di alcune azioni.
START_UP_ERROR	Start up error: {1}.	Registrato quando viene restituita un'eccezione durante l'avvio.
START_UP_ERROR_UNKNOWN	Unable to start up server. Acrobat Connect Pro might already be running.	Registrato quando viene restituito un errore durante l'avvio. JRUN stampa un errore.
TEL_CONNECTION_BROKEN	Telephony connection {1} was unexpectedly broken.	Registrato quando la connessione di telefonia si interrompe.
TEL_CONNECTION_RECOVERY	Telephony connection {1} was reattached to conference {2}.	Registrato quando Acrobat Connect ripristina una connessione alla conferenza.

Voce di registro per il campo x-status	Voce di registro per il campo x-comment	Descrizione
TEL_DOWNLOAD_FAILED	Unable to download {1} for archive {2}.	Registrato quando si verifica un timeout durante lo scaricamento dei file audio di telefonia.
TOO_MUCH_DATA	Multiple rows unexpectedly returned.	Registrato quando un'operazione restituisce più dati del previsto.
UNKNOWN_TYPE	{1}	Registrato quando il tipo di variabile è sconosciuto.

Nota: nella tabella precedente, {1} e {2} sono delle variabili che vengono sostituite con un valore nella voce di registro.

Voci del campo gravità

Il campo x-severity indica il livello di gravità di una condizione, facilitando l'identificazione del livello di risposta appropriato.

Voce di registro per il campo x-severity	Significato	Azione suggerita	Esempio
C	Critico	Configurate gli strumenti di monitoraggio di terze parti per avvisare i cercapersone quando si presenta una voce di registro con questo livello di gravità.	Impossibile contattare il database. Impossibile avviare o terminare un processo. Nel sistema si è verificato un errore.
E	Errore	Configurate gli strumenti di monitoraggio di terze parti per inviare un'e-mail quando si presenta una voce di registro con questo livello di gravità.	Impossibile contattare Adobe® Premiere®. Conversione non riuscita. Si è verificato un errore relativamente all'utente o all'account, ma non all'intero sistema.
W	Avviso	Generate ed esaminate rapporti periodici per identificare possibili miglioramenti operativi e del prodotto.	L'uso del disco o della memoria ha superato la soglia specificata.
I	Informazioni	Esaminate le voci di registro a fini di auditing o RCA.	Server avviato, interrotto o riavviato.

Voci del campo categoria

Il campo x-category indica se l'evento si riferisce a problemi di accesso (A) o a problemi generici del sistema (S). Tutte le voci della categoria A sono presenti nel file access.log e tutte le voci della categoria S sono presenti nel file error.log.

Voce di registro per il campo x-category	Significato	Descrizione
A	Accesso	Il codice di stato si riferisce ai problemi di accesso. Registrato nel file access.log.
S	Sistema	Il codice di stato si riferisce ai problemi generali del sistema. Registrato nel file error.log.

Gestione dello spazio su disco

La gestione dello spazio su disco

Il sistema Acrobat Connect Pro richiede almeno 1 GB di spazio libero su disco. Acrobat Connect Pro non dispone di strumenti integrati per il controllo dello spazio su disco; l'amministratore deve controllare lo spazio su disco mediante le utility del sistema operativo o strumenti di terzi.

Il contenuto può essere memorizzato sul server che ospita Acrobat Connect Pro, su volumi di memorizzazione condivisi esterni o su entrambi.

Altri argomenti presenti nell' Aiuto

“[Configurazione della memorizzazione condivisa](#)” a pagina 45

Gestione dello spazio su disco sui server Acrobat Connect Pro

❖ Effettuate una delle operazioni seguenti:

- Usate Connect Pro Central per eliminare il contenuto inutilizzato. Vedete [Eliminare un file o una cartella](#).
- Sostituite il disco del vostro server con un disco più grande.

Nota: se lo spazio disponibile sul disco del server scende al di sotto di 1 GB, il server si interrompe.

Gestione dello spazio su disco sui dispositivi di memorizzazione condivisa

❖ Controllate il dispositivo di memorizzazione condiviso principale per verificare lo spazio disponibile e i nodi del file system disponibili. Se uno dei due elementi scende al di sotto del 10%, aggiungete altro spazio di memorizzazione al dispositivo oppure un altro dispositivo di memorizzazione condiviso.

Nota: è consigliabile un valore pari al 10%. Inoltre, se state usando uno spazio di memorizzazione condiviso, impostate un valore massimo per le dimensioni di una cache nella console di gestione dell'applicazione, altrimenti la cache può riempire il disco.

Cancellare la cache di Edge Server

Adobe consiglia di creare un'attività pianificata settimanale per svuotare la cache del server periferico. È buona norma eseguire l'attività negli orari a traffico ridotto, ad esempio la domenica mattina presto.

- 1 Create un file cache.bat per eliminare la directory della cache. Per i dati immessi in questo file dovete usare la seguente sintassi:

```
del /Q /S [cache directory]\*.*
```

La directory predefinita della cache è C:\breeze\edgeserver\win32\cache\http. Per eliminare la cache, usate il seguente comando:

```
del /Q /S c:\breeze\edgeserver\win32\cache\http\*.*
```

- 2 Selezionate Start > Programmi > Adobe Connect Pro Edge Server 7 > Arresta Adobe Connect Pro Edge Server.
- 3 Eseguite il file cache.bat e verificate che esso elimini i file nella directory della cache.

Nota: la struttura delle directory viene mantenuta e gli eventuali file bloccati dal server periferico non vengono eliminati.

- 4 Selezionate Start > Programmi > Adobe Connect Pro Edge Server 7 > Avvia Adobe Connect Pro Edge Server.
- 5 Selezionate Start > Pannello di controllo > Attività pianificate > Aggiungi attività pianificata.

- 6 Selezionate `cache.bat` come nuovo file da eseguire.
- 7 Ripetete questa procedura per ciascun server periferico.

Backup dei dati

Il backup dei dati

Esistono tre tipi di dati di cui dovete eseguire il backup a intervalli regolari: contenuto (qualsiasi file memorizzato nelle librerie), impostazioni di configurazione e dati del database.

Se non state utilizzando dispositivi di memorizzazione condivisi, tutto il contenuto delle librerie viene memorizzato nella cartella `RootInstallationFolder\content`, per impostazione predefinita `C:\breeze\content`. Le impostazioni di configurazione sono memorizzate nel file `custom.ini`, nella cartella di installazione principale, che per impostazione predefinita è `C:\breeze`.

Un backup del database crea un duplicato dei dati presenti nel database. I backup del database pianificati regolarmente possono consentire il ripristino in caso di numerosi guasti, compresi quelli dei supporti, gli errori dell'utente e la perdita permanente di un server. Eseguire il backup del database ogni giorno.

Potete anche usare i backup per copiare un database da un server all'altro. Potete ricreare l'intero database da un backup in un'unica operazione, ripristinando il database. Il processo di ripristino sovrascrive il database esistente o lo crea, se esso non esiste. Lo stato del database ripristinato è identico a quello che esso aveva al momento dell'esecuzione del backup, tranne eventuali transazioni non confermate.

Potete creare backup sui dispositivi di backup, quali un disco o un nastro. Per configurare i backup potete utilizzare un'utility SQL Server. Ad esempio, potete sovrascrivere i backup non aggiornati o aggiungere nuovi backup al supporto di backup.

Durante il backup del database, adottate le migliori pratiche:

- Pianificate un backup notturno.
- Conservate i backup in un luogo sicuro, preferibilmente in un luogo diverso da quello in cui si trovano i dati.
- Conservate le vecchie copie di backup per un determinato periodo di tempo, nel caso in cui il backup più recente sia danneggiato, distrutto o perso.
- Definite un sistema per sovrascrivere i backup, riutilizzando per primo quello più vecchio. Per impedirne la sovrascrittura, utilizzate le date di scadenza riportate sui backup.
- Applicate delle etichette ai supporti di backup per identificare i dati e impedire la sovrascrittura delle copie di backup di importanza fondamentale.

Per eseguire il backup del database, utilizzate le utility di SQL Server:

- Transact-SQL
- SQL Distributed Management Objects
- Procedura guidata Create Database Backup
- SQL Server Management Studio

Eseguire il backup dei file del server

Eseguite il backup e proteggete i dati del sistema allo stesso modo in cui proteggete tutte le preziose risorse della vostra organizzazione.

È buona norma eseguire questa procedura di notte.

- 1 Per arrestare Acrobat Connect Pro effettuate le operazioni seguenti:
 - a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Central Service.
 - b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Arresta Connect Pro Meeting Service.
- 2 Eseguite una copia di backup della directory del contenuto.

Il percorso predefinito è C:\breeze.

- 3 Eseguite una copia di backup del file custom.ini.

Il percorso predefinito è C:\breeze\.

- 4 Per avviare Acrobat Connect Pro, effettuate le operazioni seguenti:
 - a Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Meeting Service.
 - b Scegliete Start > Programmi > Adobe Acrobat Connect Pro Server 7 > Avvia Connect Pro Central Service.

Eseguire il backup del database

Per eseguire il backup di tutte le edizioni di Microsoft SQL Server, potete utilizzare Microsoft SQL Server Management Studio o la finestra Prompt dei comandi.

L'edizione di SQL Server installata con Connect Pro Server non include SQL Server Management Studio, ma potete scaricare [Microsoft SQL Server Management Studio Express](#) dal sito Microsoft.

Utilizzare SQL Server Management Studio per il backup di SQL Server

Importante: non disinstallate il database.

- 1 In Windows, selezionate Start > Programmi > Microsoft SQL Server 2005 > SQL Server Management Studio.
- 2 Nel riquadro della struttura della finestra Object Explorer, fate clic con il pulsante destro del mouse sul database (denominato "breeze," per impostazione predefinita) e selezionate Operazioni > Backup...

Nota: per istruzioni dettagliate su come eseguire il backup e il ripristino del database SQL Server, visitate il sito del supporto tecnico Microsoft.

Utilizzare la finestra Prompt dei comandi per il backup di SQL Server

Per accedere alle informazioni della Guida relative ai comandi di database, digitate `osql ?` sul prompt del DOS e premete Invio.

Importante: non disinstallate il database.

- 1 Accedete al server in cui è installato Connect Pro Server.
- 2 Create una cartella in cui memorizzare i file di backup del database.

In questo esempio viene usata la cartella c:\Connect_Database.

- 3 Scegliete Start > Esegui, digitate **cmd** nella casella Apri e fate clic su OK.
- 4 Al prompt passate alla directory in cui è installato il database. Per impostazione predefinita, la directory è C:\Program Files\Microsoft SQL Server90\Tools\Binn.

- 5 Al prompt , digitate **osql -E** per accedere al motore database, quindi premete Invio.
- 6 Digitate **BACKUP DATABASE nome-database TO DISK = 'C:\Connect_Database\nome-database.bak'** per eseguire una utility Microsoft SQL per il backup del database di Connect, quindi premete Invio.
Il nome predefinito del database è *breeze*.
- 7 Al prompt digitate **go**, quindi premete Invio.
Nella finestra del comando compaiono messaggi riguardo lo stato del backup.
- 8 Al prompt digitate **quit**, quindi premete Invio.
- 9 Per verificare se il backup ha avuto esito positivo, controllate che il file breeze.bak sia incluso nella directory c:\Connect_Database.
- 10 Per riavviare il database, dal desktop di Windows scegliete Start > Pannello di controllo > Strumenti di amministrazione > Servizi. Nella finestra Servizi fate clic con il pulsante destro del mouse su SQL Server (MSSQLSERVER) e scegliete Avvia dal menu di scelta rapida.

Creazione di rapporti personalizzati

Creare rapporti personalizzati usando le visualizzazioni dello schema a stella

Acrobat Connect Pro usa un database per memorizzare informazioni su utenti, contenuto, corsi e riunioni. L'attività dell'utente popola il database. Potete usare strumenti come Adobe® ColdFusion® Studio e Business Objects Crystal Reports per eseguire una query sulle visualizzazioni dello schema a stella e visualizzare i dati. Potete anche usare strumenti basati su SQL come SQL Query Analyzer.

Le seguenti applicazioni di Acrobat Connect Pro possono inviare i dati ai rapporti:

Acrobat Connect Pro Meeting Partecipanti alla riunione, durata e contenuto della riunione.

Adobe Presenter Visualizzazioni del contenuto, visualizzazioni delle diapositive e visualizzazioni delle presentazioni.

Acrobat Connect Pro Training Informazioni sulla gestione del corso, come le statistiche sui partecipanti al corso, statistiche sulla visualizzazione dei contenuti e risultati dei questionari.

Nota: inoltre, potete eseguire rapporti dall'applicazione *Web Connect Pro Central* e visualizzarli o scaricarli in formato CSV. Per ulteriori informazioni, vedete [Generazione di rapporti in Connect Pro Central](#).

Fatto SCO

Colonna	Descrizione
dim_sco_details_sco_id	ID SCO
dim_sco_details_sco_version	Versione SCO
max_retries	Numero massimo di tentativi
owner_user_id	ID utente del proprietario dello SCO
disk_usage_kb	Uso del disco in kilobyte
passing_score	Valutazione superamento
max_possible_score	Valutazione massima possibile
views	Numero di visualizzazioni

Colonna	Descrizione
unique_viewers	Numero di utenti univoci che hanno visualizzato lo SCO
slides	Numero di diapositive
questions	Numero di domande
max_score	Valutazione massima
min_score	Valutazione minima
average_score	Valutazione media
average_passing_score	Valutazione superamento media
total_registered	Valutazione non superamento media
total_participants	Utenti registrati totali
account_id	Partecipanti totali

Dimensioni dei dettagli dello SCO

Colonna	Descrizione
sco_id	ID SCO
sco_version	Versione SCO
sco_name	Nome
sco_description	Descrizione
sco_type	Tipo di SCO
sco_int_type	Tipo di numero intero
is_content	Lo SCO è uno SCO di contenuto?
url	URL
parent_name	Nome dello SCO principale
parent_sco_id	ID dello SCO principale
parent_type	Tipo di SCO principale
date_sco_created	Data di creazione
date_sco_modified	Data modifica
sco_start_date	Data di inizio
sco_end_date	Data di fine
version_start_date	Data di inizio versione
version_end_date	Data di fine versione
sco_tag_id	ID del tag
passing_score	Valutazione superamento
max_possible_score	Valutazione massima possibile
linked_sco_id	ID di uno SCO collegato

Colonna	Descrizione
linked_type	Tipo di SCO collegato
owner_user_id	ID utente proprietario
storage_bytes_kb	Byte memorizzazione in kilobyte
account_id	ID account

Fatto Attività

Colonna	Descrizione
dim_activity_details_activity_id	ID attività
score	Valutazione
passed	Superato
completed	Completato
peak_session_users	Picco utenti sessione
number_correct	Numero corretto
number_incorrect	Numero errato
number_of_questions	Numero di domande
number_of_responses	Numero di risposte
account_id	ID account

Dimensioni dei dettagli dell'attività

Colonna	Descrizione
activity_id	ID attività
dim_sco_details_sco_id	ID SCO
dim_sco_details_sco_version	Versione SCO
dim_users_user_id	ID utente
dim_sco_details_parent_sco_id	ID SCO principale
score	Valutazione
passed	Superato
completed	Completato
activity_type	Tipo attività
role	Ruolo
date_activity_started	Data di inizio
date_activity_finished	Data di fine
dim_cost_center_id	ID centro costi
cost_center_audit_id	ID auditing
session_start_date	Data inizio sessione

Colonna	Descrizione
session_end_date	Data fine sessione
attendance_activity	Viene registrata la presenza?
session_id	ID sessione
account_id	ID account

Dimensioni dei test-out del programma

Colonna	Descrizione
dim_sco_details_curriculum_sco_id	ID colonna
dim_sco_details_curriculum_sco_version	Versione programma
test_out_subject_sco_id	ID SCO oggetto
test_out_target_sco_id	ID SCO di destinazione
test_out_type	Tipo test-out
account_id	ID account

Dimensioni dei prerequisiti del programma

Colonna	Descrizione
dim_sco_details_curriculum_sco_id	ID colonna
dim_sco_details_curriculum_sco_version	Versione programma
pre_requisite_subject_sco_id	ID SCO oggetto
pre_requisite_target_sco_id	ID SCO di destinazione
pre_requisite_type	Tipo prerequisito
account_id	ID account

Dimensioni dei requisiti di completamento del programma

Colonna	Descrizione
dim_sco_details_curriculum_sco_id	ID colonna
dim_sco_details_curriculum_sco_version	Versione programma
completion_subject_sco_id	ID SCO oggetto
completion_target_sco_id	ID SCO di destinazione
completion_requirement_type	Tipo requisito di completamento
account_id	ID account

Fatto Visualizzazioni delle diapositive

Colonna	Descrizione
dim_slide_view_details_slide_view_id	ID visualizzazione diapositiva

Colonna	Descrizione
dim_activity_details_activity_id	ID attività
slide_view_display_sequence	Sequenza di visualizzazione
account_id	ID account

Dimensioni dei dettagli delle visualizzazioni delle diapositive

Colonna	Descrizione
slide_view_id	ID visualizzazione diapositiva
date_slide_viewed	Data visualizzazione diapositiva
slide_name	Nome diapositiva
slide_description	Descrizione diapositiva
account_id	ID account

Fatto Risposte

Colonna	Descrizione
dim_answer_details_answer_id	ID risposta
dim_activity_details_activity_id	ID attività
dim_question_details_question_id	ID domanda
answer_display_sequence	Sequenza di visualizzazione
answer_score	Valutazione?
answer_correct	È corretta?
account_id	ID account

Dimensioni dei dettagli della risposta

Colonna	Descrizione
answer_id	ID risposta
date_answered	Data risposta
response	Risposta
account_id	ID account

Fatto Domanda

Colonna	Descrizione
dim_sco_details_sco_id	ID SCO
dim_sco_details_sco_version	Versione SCO
dim_question_details_question_id	ID domanda
number_correct	Numero di risposte corrette

Colonna	Descrizione
number_incorrect	Numero di risposte errate
total_responses	Risposte totali
high_score	Valutazione elevata
low_score	Valutazione bassa
average_score	Valutazione media
account_id	ID account

Dimensioni dei dettagli della domanda

Colonna	Descrizione
question_id	ID domanda
question_display_sequence	Sequenza di visualizzazione
question_description	Descrizione
question_type	Tipo domanda
account_id	ID account

Dimensioni delle risposte alla domanda

Colonna	Descrizione
dim_question_details_question_id	ID domanda
response_display_sequence	Sequenza delle visualizzazioni della risposta
response_value	Valore
response_description	Descrizione
account_id	ID account

Dimensioni dei gruppi

Colonna	Descrizione
group_id	ID gruppo
group_name	Nome gruppo
group_description	Descrizione gruppo
group_type	Tipo gruppo
account_id	ID account

Dimensioni dei gruppi di utenti

Colonna	Descrizione
user_id	ID utente
group_id	ID gruppo

Colonna	Descrizione
group_name	Nome gruppo
account_id	ID account

Dimensioni degli utenti

Colonna	Descrizione
user_id	ID utente
Login	Login
first_name	Nome
last_name	Cognome
email	Indirizzo e-mail
user_description	Descrizione utente
user_type	Tipo utente
most_recent_session	Sessione più recente
session_status	Stato sessione
manager_name	Nome manager
disabled	Disattivato
account_id	ID account
custom_field_1	Valore campo personalizzato 1
custom_field_2	Valore campo personalizzato 2
custom_field_3	Valore campo personalizzato 3
custom_field_4	Valore campo personalizzato 4
custom_field_5	Valore campo personalizzato 5
custom_field_6	Valore campo personalizzato 6
custom_field_7	Valore campo personalizzato 7
custom_field_8	Valore campo personalizzato 8
custom_field_9	Valore campo personalizzato 9
custom_field_10	Valore campo personalizzato 10

Dimensioni dei nomi dei campi personalizzati

Colonna	Descrizione
dim_column_name	Nome colonna campo personalizzato
custom_field_name	Nome campo personalizzato
account_id	ID account

Dimensioni dei centri costi

Colonna	Descrizione
cost_center_id	ID centro costi
cost_center_name	Nome centro costi
cost_center_description	Descrizione cento costo

Creazione di rapporti personalizzati dalle visualizzazioni dei database precedenti

Nota: Acrobat Connect Pro Server 7 introduce visualizzazioni dello schema a stella sulle quali potete eseguire query per creare rapporti personalizzati. Le visualizzazioni dei database precedenti sono comunque supportate, ma le visualizzazioni dello schema a stella sono più standardizzate e robuste.

Acrobat Connect Pro usa un database per memorizzare informazioni su utenti, contenuto, corsi e riunioni. L'attività dell'utente popola il database. Potete usare strumenti come Adobe® ColdFusion® Studio e Business Objects Crystal Reports per eseguire una query sul database e visualizzare i dati. Potete anche usare strumenti basati su SQL come SQL Query Analyzer.

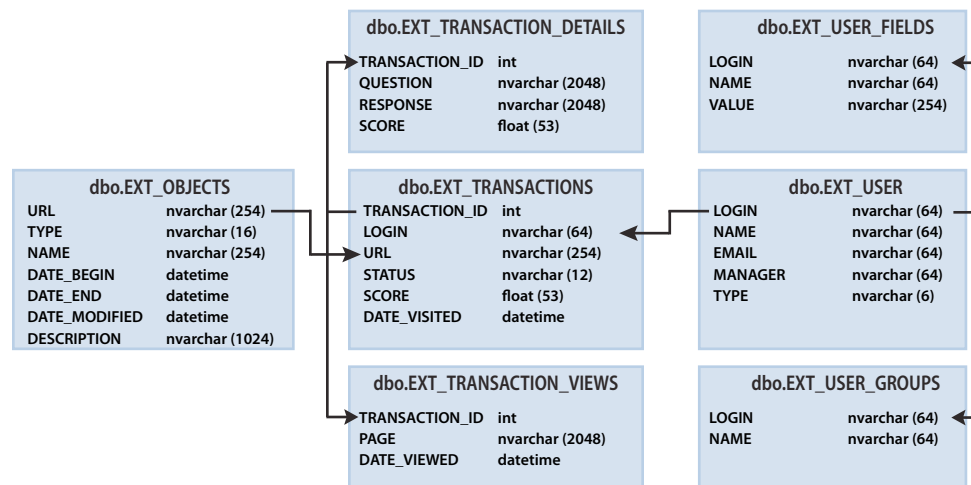
Le seguenti applicazioni di Acrobat Connect Pro possono inviare i dati ai rapporti:

Acrobat Connect Pro Meeting Partecipanti alla riunione, durata e contenuto della riunione.

Adobe Presenter Visualizzazioni del contenuto, visualizzazioni delle diapositive e visualizzazioni delle presentazioni.

Acrobat Connect Pro Training Informazioni sulla gestione del corso, come le statistiche sui partecipanti al corso, statistiche sulla visualizzazione dei contenuti e risultati dei questionari.

Visualizzare le relazioni tra diverse visualizzazioni database



Le frecce rappresentano i rapporti delle entità tra le sette visualizzazioni dei rapporti.

Nota: le seguenti funzioni non sono supportate: visualizzazioni non identificate in questo documento, alterazione delle visualizzazioni identificate in questo documento, accesso diretto allo schema del database sottostante.

- ❖ Usate uno strumento per la creazione di diagrammi che si connetta al database per visualizzare i rapporti tra le visualizzazioni del database.

EXT_TRANSACTIONS

Un ID di transazione univoco viene generato ogni volta che un utente interagisce con un oggetto. La visualizzazione EXT_TRANSACTIONS restituisce i dati elencati nella tabella seguente:

Colonna	Tipo dati	Descrizione
TRANSACTION_ID	INT	ID univoco per la transazione.
LOGIN	NVARCHAR	Nome dell'utente che ha eseguito questa transazione.
URL	NVARCHAR	Oggetto con cui ha interagito l'utente.
STATUS	NVARCHAR	Puo essere: superato, non superato, completato o in corso.
SCORE	FLOAT	La valutazione ottenuta dall'utente.
DATE_VISITED	DATETIME	Data in cui questa transazione è stata eseguita o visualizzata.

Query e dati di esempio La seguente query restituisce i dati della tabella seguente:

```
select * from ext_transactions where url = '/p63725398/' order by login, date_visited asc;
```

TRANSACTION_ID	LOGIN	URL	STATUS	SCORE	DATE_VISITED
10687	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:56:16.500
10688	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:56:16.500
10693	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:58:23.920
10714	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:09:20.810
10698	test2-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:00:49.483
10723	test3-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:11:32.153
10729	test3-lnagaraj@test.enang.com	/p63725398/	completed	20.0	2006-12-15 01:12:09.700

Note sulla query La visualizzazione EXT_TRANSACTIONS restituisce tutte le transazioni esistenti per un determinato utente e la sessione di formazione. Per visualizzare la transazione più recente, controllate il valore massimo di DATE_VISITED.

Potete applicare un filtro nei campi STATUS e URL per ottenere un elenco di utenti che hanno superato una sessione di formazione specifica, ad esempio:

```
select * from ext_transactions where url = '/p31102136/' and status = 'user-passed' order by login, date_visited asc;
```

Generazione di dati Azioni dell'utente che generano i dati in questa visualizzazione:

- Partecipazione a una riunione
- Visualizzazione di una parte del contenuto
- Seguire una sessione di formazione (un corso o un programma)

Dati esclusi •Numero di certificato, che non è presente nel database

- Valutazione massima, spesso non disponibile

EXT_TRANSACTIONS_VIEWS

La visualizzazione EXT_TRANSACTIONS_VIEWS recupera i dati sulle diapositive o sulle pagine visualizzate dagli utenti.

Colonna	Tipo dati	Descrizione
TRANSACTION_ID	INT	ID univoco ID per questa transazione (può essere unito a TRANSACTION_DETAILS per riepilogare l'URL).
PAGE	NVARCHAR	Numero della diapositiva o della pagina che è stata visualizzata.
DATE_VIEWED	DATETIME	Data in cui ha avuto luogo questa visualizzazione.

Query e dati di esempio La seguente query restituisce i dati della tabella seguente:

```
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

Generazione di dati I dati vengono generati in questa visualizzazione ogni volta che un utente visualizza contenuto o una sessione di formazione.

EXT_USERS

La visualizzazione EXT_USERS elenca gli utenti e gli attributi del profilo associato:

Colonna	Tipo dati	Descrizione
LOGIN	NVARCHAR	Identificatore univoco dell'utente.
NAME	NVARCHAR	Nome univoco dell'utente.
EMAIL	NVARCHAR	Indirizzo e-mail univoco.
MANAGER	NVARCHAR	Il login del manager. Il manager è sempre impostato su NULL in Breeze 5.1.
TYPE	NVARCHAR	Utente o ospite. Il tipo è sempre impostato sull'utente nella versione 5.1.

Query e dati di esempio La seguente query restituisce i dati della tabella seguente:

```
select * from ext_users;
```

LOGIN	NAME	EMAIL	MANAGER	TYPE
test4-lnagaraj@test.enang.com	test4 laxmi	test4-lnagaraj@test.enang.com	NULL	user
test7-lnagaraj@test.enang.com	TEST7 laxmi	test7-lnagaraj@test.enang.com	NULL	user

Generazione di dati I dati vengono aggiornati in questa visualizzazione ogni volta che un ospite o un utente viene creato, aggiornato o eliminato.

Dati esclusi • Password, che non è memorizzata in testo normale.

- Fuso orario e lingua, che non sono disponibili in un formato di lettura naturale, ad esempio PST è 323.
- Ultimo login, il cui calcolo risulta troppo intensivo per le risorse. Usate invece una query `max(date_visited)` dalla visualizzazione EXT_TRANSACTIONS per recuperare questi dati.

- Sessione attiva, ossia i dati provenienti dalla visualizzazione EXT_TRANSACTION. Usate invece un'interrogazione STATUS='IN-PROGRESS' per recuperare questi dati.
- Gli utenti eliminati non appaiono nella visualizzazione EXT_USERS. Gli utenti eliminati continuano a essere presenti nella visualizzazione EXT_TRANSACTION.
- I dati sui gruppi non sono inclusi in questa visualizzazione.
- I dati nei campi personalizzati dell'utente nuovi e predefiniti. Queste informazioni sono disponibili per ciascun utente nella visualizzazione EXT_USER_FIELDS.

EXT_USER_FIELDS

La visualizzazione EXT_USER_FIELDS elenca i campi personalizzati nuovi e predefiniti per un utente specifico. Elenca anche i campi personalizzati per gli utenti che sono stati convertiti in ospiti.

Colonna	Tipo dati	Descrizione
LOGIN	NVARCHAR	Identificatore univoco dell'utente.
NAME	NVARCHAR	Campo del nome, come ad esempio il numero di telefono.
VALUE	NVARCHAR	Valore del campo, come ad esempio 415.555.1212.

Query e dati di esempio La seguente query restituisce i dati della tabella seguente:

```
select * from ext_user_fields where login = 'test4-lnagaraj@test.enang.com';
```

LOGIN	NAME	VALUE
test4-lnagaraj@test.enang.com	{email}	test4-lnagaraj@test.enang.com
test4-lnagaraj@test.enang.com	{first-name}	test4
test4-lnagaraj@test.enang.com	{last-name}	laxmi
test4-lnagaraj@test.enang.com	{x-job-title}	sw engr 4
test4-lnagaraj@test.enang.com	{x-direct-phone}	NULL
test4-lnagaraj@test.enang.com	{x-direct-phone-key}	NULL
test4-lnagaraj@test.enang.com	SSN	777

Generazione di dati Le azioni che generano dati in questa visualizzazione: aggiunta, creazione o aggiornamento di campi personalizzati nuovi o predefiniti per uno o più utenti.

EXT_USER_GROUPS

La visualizzazione EXT_USER_GROUPS elenca i dati sui gruppi e i relativi membri dei gruppi. La visualizzazione EXT_USER_GROUPS usa i dati elencati nella tabella seguente:

Colonna	Tipo dati	Descrizione
LOGIN	NVARCHAR	Nome dell'utente.
NAME	NVARCHAR	Nome del gruppo.

Query e dati di esempio La seguente query restituisce i dati della tabella seguente:

```
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

Note sulla query La nidificazione di più gruppi è supportata nella versione 5.1 e nelle versioni successive. Ad esempio, se il gruppo A contiene il gruppo B e l'utente si trova nel gruppo B, l'utente viene elencato come membro di A.

I gruppi predefiniti, come il gruppo Amministratori, usano i nomi dei codici dello schema, come ad esempio nella seguente query SQL: `SELECT * FROM EXT_USER_GROUPS where group='{admins}`. Il nome del codice distingue i gruppi predefiniti dai gruppi definiti dall'utente.

Generazione di dati Azioni dell'utente che generano i dati in questa visualizzazione:

- Creazione, aggiornamento o eliminazione di un gruppo
- Cambiamento dell'appartenenza a un gruppo

EXT_OBJECTS

La visualizzazione EXT_OBJECTS elenca tutti gli oggetti del sistema (come riunioni, contenuto, corsi e così via) e i relativi attributi.

Colonna	Tipo dati	Descrizione
URL	NVARCHAR	Identificatore univoco dell'oggetto.
TYPE	NVARCHAR	Presentazione, corso, file FLV, file SWF, immagine, archivio, riunione, programma, cartella o evento.
NAME	NVARCHAR	Nome dell'oggetto che appare nell'elenco del contenuto.
DATE_BEGIN	DATETIME	Data pianificata per l'inizio dell'oggetto.
DATE_END	DATETIME	Data pianificata per la fine dell'oggetto.
DATE_MODIFIED	DATETIME	Data in cui l'oggetto è stato modificato.
DESCRIPTION	NVARCHAR	Informazioni riassuntive sull'oggetto immesse alla creazione di una riunione, contenuto, corso o un altro tipo di oggetto

Query e dati di esempio La seguente query SQL restituisce i dati della tabella seguente:

```
select * from ext_objects order by type asc;
```

URL	TYPE	NAME	DATE_BEGIN	DATE_END	DATE_MODIFIED	DESCRIPTION
/p79616987/	course	test api	2006-12-08 23:30:00.000	NULL	2006-12-08 23:36:55.483	NULL
/p47273753/	curriculum	test review curric	2006-12-14 21:00:00.000	NULL	2006-12-14 21:00:30.060	NULL
/tz1/	meeting	{default-template}	2006-12-12 19:15:00.000	2006-12-12 20:15:00.000	2006-12-12 19:25:07.750	release presentation
/p59795005/	presentation	ln-QUIZ-TEST1	NULL	NULL	2006-12-15 00:43:19.797	managers meeting

Note sulla query Potete ottenere tutti gli oggetti di un tipo specifico applicando un filtro al campo TYPE. Ad esempio, la seguente query SQL applica i filtri per i corsi e i programmi:

```
select * from ext_objects where type in ('course', 'curriculum');
```

Usate la seguente query SQL per restituire un elenco dei tipi di sistemi disponibili:

```
select DISTINCT (type) from ext_objects;
```

Generazione di dati Azioni dell'utente che generano i dati in questa visualizzazione:

- Creazione o aggiornamento di una riunione, un corso o un programma
- Caricamento o aggiornamento del contenuto

Dati esclusi •Durata, utilizzabile con `date_end - date_begin` per eseguire il calcolo.

- Dimensioni su disco, che rivelano le regole aziendali relativamente alla differenza tra copie e originali.
- ID cartella
- Gli oggetti eliminati non appaiono nella visualizzazione EXT_OBJECTS. Gli oggetti eliminati sono presenti nella visualizzazione EXT_TRANSACTION.