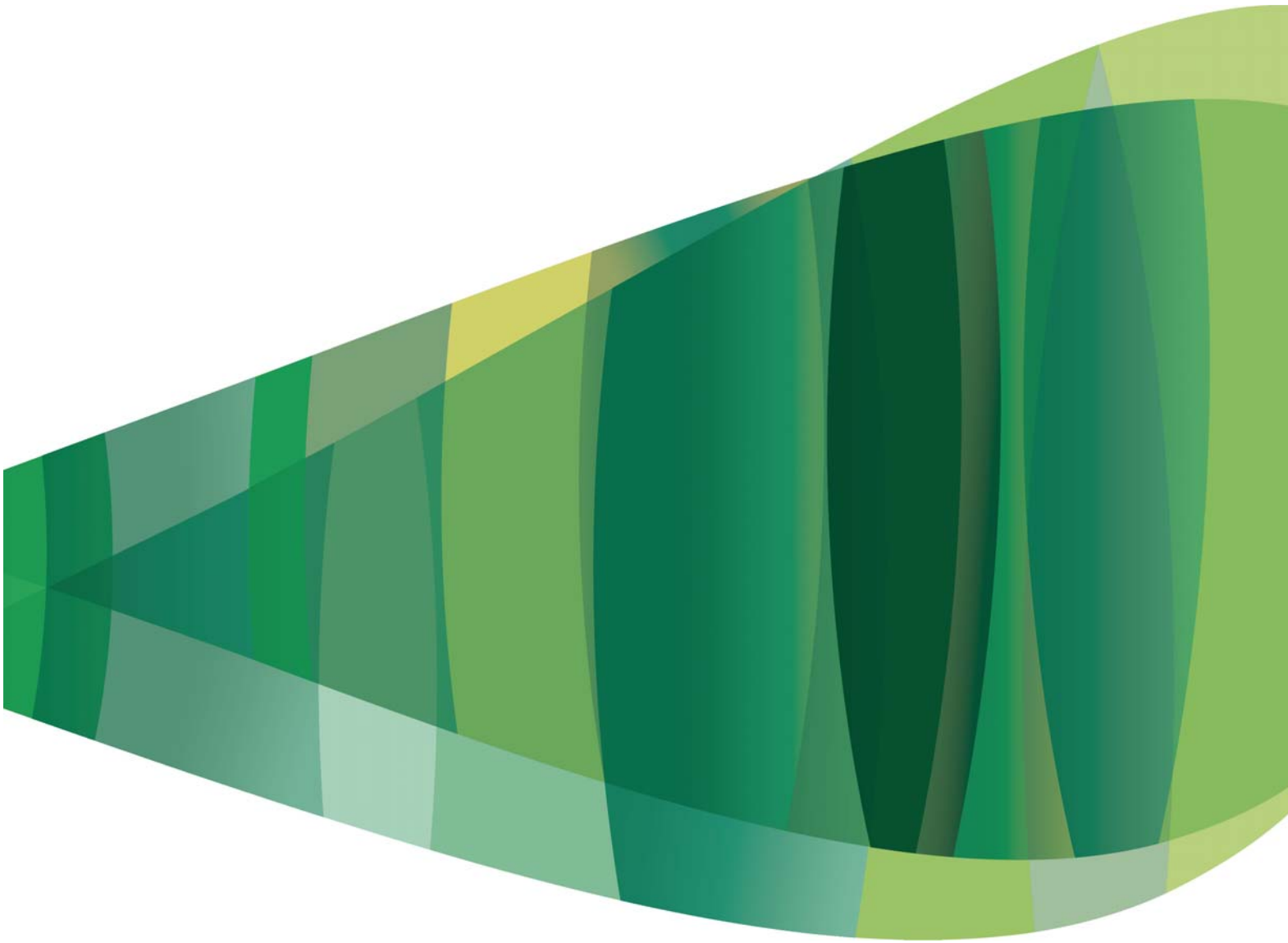
ADOBE® ACROBAT® CONNECT™ PRO 7

MIGRACIÓN, INSTALACIÓN Y CONFIGURACIÓN DE ADOBE ACROBAT CONNECT PRO SERVER 7



Adobe

Migration, installation et configuration d'Adobe® Acrobat® Connect™ Pro Server 7 pour Windows®

Adobe Systems Incorporated, 345 Park Avenue, San Jose, Californie 95110, Etats-Unis.

Sommaire

Chapitre 1 : Préparation de la migration, de l'installation et de la configuration

Lorsque vous vous préparez à concevoir et à installer un système Adobe® Acrobat® Connect™ Pro Server 7, vérifiez les conditions d'installation requises, les configurations prises en charge et la présentation technique. Si vous effectuez une mise à niveau vers Acrobat Connect Pro Server 7, suivez les instructions de sauvegarde des fichiers.

Configuration requise pour l'installation

Configuration matérielle, logicielle et utilisateur

Pour connaître la configuration requise pour Acrobat Adobe Connect Pro Server 7 et Adobe Acrobat Connect Pro Edge Server 7, visitez le site www.adobe.com/go/connect_sysreqs_fr.

Configuration des ports

Le tableau suivant décrit les ports sur lesquels les utilisateurs doivent pouvoir établir des connexions TCP.

Remarque : *RTMP (Real-Time Messaging Protocol) est un protocole Adobe.*

Valeur numérique	Adresse de liaison	Accès	Protocole
80	*/Adaptateur quelconque	Public	HTTP, RTMP
443	*/Adaptateur quelconque	Public	HTTPS, RTMPS
1935	*/Adaptateur quelconque	Public	RTMP

Le tableau suivant décrit les ports ouverts à l'intérieur d'un cluster. Chaque serveur Acrobat Connect Pro d'un cluster doit pouvoir établir des connexions TCP vers tous les autres serveurs du cluster sur ces ports.

Remarque : *Ces ports ne doivent pas être ouverts au public, même si vous n'utilisez pas de cluster.*

Valeur numérique	Port source	Adresse de liaison	Accès	Protocole
8506	Valeur quelconque	*/Adaptateur quelconque	Privé	RTMP
8507	Valeur quelconque	*/Adaptateur quelconque	Privé	HTTP

Chaque serveur Acrobat Connect Pro d'un cluster doit pouvoir établir une connexion TCP vers le serveur de base de données sur le port suivant :

Valeur numérique	Port source	Accès	Protocole
1433	Valeur quelconque	Privé	TSQL

Le tableau suivant décrit les ports serveur utilisés par Acrobat Connect Pro pour communiquer en interne. Ces ports ne doivent pas être utilisés sur un serveur hébergeant Acrobat Connect Pro, sinon ce dernier risque de ne pas démarrer.

Valeur numérique	Adresse de liaison	Accès	Protocole
1111	127.0.0.1	Interne	RTMP
1434	127.0.0.1 Ce port n'est actif que si vous utilisez la base de données intégrée.	Interne	TSQL
2909	127.0.0.1	Interne	RMI
8510	127.0.0.1	Interne	HTTP

Configurations prises en charge

Configurations de bases de données/serveur prises en charge

Acrobat Connect Pro stocke les informations sur les utilisateurs et le contenu dans une base de données. Configurations d'Acrobat Connect Pro et de bases de données prises en charge :

Serveur unique avec moteur de base de données intégré Installez Acrobat Connect Pro sur un ordinateur et installez le moteur de base de données intégré (inclus dans le programme d'installation d'Acrobat Connect Pro) sur ce même ordinateur. Le moteur de base de données intégré est Microsoft® SQL Server 2005 Express Edition.

Remarque : *Cette configuration ne peut être utilisée que dans des environnements de test, pas dans des environnements de production.*

Serveur unique avec base de données SQL Server Installez Acrobat Connect Pro sur un seul ordinateur sur lequel vous installez également Microsoft® SQL Server 2005 Standard Edition.

Serveur unique avec base de données SQL Server externe Installez Acrobat Connect Pro sur un seul ordinateur et installez SQL Server 2005 Standard Edition sur un autre ordinateur.

Serveur unique avec bases de données SQL Server multiples externes Installez Acrobat Connect Pro sur un seul ordinateur et installez SQL Server 2005 Standard Edition sur plusieurs ordinateurs (autrement dit un cluster) externes à Acrobat Connect Pro.

Serveurs multiples avec base de données SQL Server externe Installez Acrobat Connect Pro sur plusieurs ordinateurs (autrement dit un cluster) et installez SQL Server 2005 Standard Edition sur un autre ordinateur.

Serveurs multiples avec bases de données SQL Server multiples externes Installez Acrobat Connect Pro sur plusieurs ordinateurs (autrement dit un cluster) et installez SQL Server 2005 Standard Edition dans un cluster distinct.

Remarque : *Microsoft SQL Server 2005 Standard Edition n'est pas fourni avec Acrobat Connect Pro Server 7 et doit être acheté séparément.*

Voir aussi

« Préparation de l'installation » à la page 6

« Installation d'Acrobat Connect Pro Server 7 » à la page 13

Serveurs d'annuaire LDAP pris en charge

Vous pouvez configurer l'authentification utilisateur sur le serveur d'annuaire LDAP de votre société et en importer les informations d'annuaire dans Acrobat Connect Pro. Vous trouverez la liste des serveurs d'annuaire LDAP pris en charge à l'adresse www.adobe.com/go/connect_sysreqs_fr.

Remarque : *Tout serveur d'annuaire LDAP v.3 peut s'intégrer à Acrobat Connect Pro Server 7. Cependant, seuls les serveurs d'annuaire testés par Adobe sont pris en charge.*

Voir aussi

« Intégration dans un service d'annuaire » à la page 28

Périphériques de stockage de contenu pris en charge

Vous pouvez configurer votre système Acrobat Connect Pro pour qu'il stocke le contenu sur des périphériques NAS (Network Attached Storage) et SAN (Storage Area Network). Vous trouverez la liste des périphériques NAS et SAN pris en charge à l'adresse www.adobe.com/go/connect_sysreqs_fr.

Voir aussi

« Configuration du stockage partagé » à la page 35

Préparation de la migration

Voies de migration

Exécutez le programme d'installation d'Adobe Acrobat Connect Pro Server 7 pour effectuer la mise à niveau d'Adobe Connect Enterprise 6 vers Acrobat Connect Pro Server 7 (unique chemin de mise à niveau). Les interfaces utilisateur graphiques du programme d'installation d'Acrobat Connect Pro et de la Console de gestion des applications vous guident tout au long de la mise à niveau.

Pour plus d'informations sur la mise à niveau, contactez l'assistance d'Adobe : www.adobe.com/go/connect_licensed_programs_fr.

Migration de Connect Enterprise 6 vers Acrobat Connect Pro Server 7

Procédez comme suit pour migrer de Connect Enterprise 6 vers Acrobat Connect Pro Server 7.

1. Testez la migration dans un environnement non destiné à la production.

Il est généralement conseillé de prendre un instantané de l'environnement de production actuel et de tester la migration dans un environnement de test avant de migrer l'environnement de production. Lorsque vous avez réussi la migration dans l'environnement test, passez à l'étape 2.

2. Informez les utilisateurs quant à la migration.

Reportez-vous à la section « Information des utilisateurs quant à la migration » à la page 4.

3. Arrêtez Connect Enterprise 6 et sauvegardez les fichiers.

Voir la section « Sauvegarde des fichiers » à la page 4.

4. Sauvegardez la base de données.

Voir la section « Sauvegarde de la base de données » à la page 4.

5. Exécutez le programme d'installation d'Adobe Acrobat Connect Pro Server 7.

Reportez-vous à la section « Installation d'Acrobat Connect Pro Server 7 » à la page 13.

6. Configurez Acrobat Connect Pro Server 7.

Reportez-vous à la section « Configuration d'Acrobat Connect Pro avec l'Assistant de la Console de gestion des applications » à la page 14.

7. Vérifiez votre installation.

Reportez-vous à la section « Vérification de votre installation » à la page 16.

Information des utilisateurs quant à la migration

Comme pour toute mise à niveau logicielle, et en particulier si elle affecte un groupe de travail, la communication et la planification sont importantes. Avant de démarrer la migration ou l'ajout de modules à Acrobat Connect Pro, Adobe vous suggère d'effectuer les opérations suivantes :

- Prévoyez suffisamment de temps pour assurer une migration réussie. Il est préférable d'effectuer la mise à niveau pendant la période de maintenance habituelle.
- Signalez à vos utilisateurs qu'ils ne pourront pas utiliser Acrobat Connect Pro pendant la migration.
- Informez-les également des types de changements auxquels ils doivent s'attendre (nouvelles fonctionnalités ou meilleures performances, par exemple) après la migration. Pour plus d'informations sur les nouvelles fonctionnalités, visitez le site www.adobe.com/go/learn_cnn_whatsnew_fr.

Sauvegarde des fichiers

1 Pour arrêter tous les services Connect Enterprise 6, procédez comme suit :

a Choisissez Démarrer > Programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Enterprise Server.

b Choisissez Démarrer > Programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Meeting Server.

2 Sauvegardez le répertoire de contenu.

L'emplacement par défaut est C:\breeze\content.

3 Sauvegardez le fichier custom.ini.

L'emplacement par défaut est c:\breeze\custom.ini.

Sauvegarde de la base de données

Vous devez sauvegarder la base de données avant de la migrer. Pour sauvegarder le moteur de base de données intégré, utilisez la fenêtre d'invite de commande car le moteur de base de données intégré ne dispose pas de sa propre interface utilisateur graphique.

Remarque : *Si vous avez accès à SQL Server Enterprise Manager, vous pouvez le configurer pour sauvegarder le moteur de base de données intégré. Consultez la TechNote d'Adobe : www.adobe.com/go/79895439_fr.*

Pour sauvegarder SQL Server , utilisez SQL Server Enterprise Manager.

Important : *Ne désinstallez pas la base de données.*

Sauvegarde de la base de données SQL Server

Si vous utilisez une version achetée de Microsoft SQL Server, vous pouvez utiliser SQL Server Enterprise Manager pour sauvegarder votre base de données.

Important : *Ne désinstallez pas la base de données.*

1 Sous Windows, choisissez Démarrer > Programmes > Microsoft SQL Server > Enterprise Manager.

2 Dans l'arborescence de la fenêtre Enterprise Manager, sélectionnez la base de données (nommée « breeze » par défaut).

3 Sélectionnez Outils > Sauvegarder la base de données.

Remarque : *Pour des instructions complètes sur la sauvegarde et le rétablissement de la base de données SQL Server, consultez le site du support technique de Microsoft.*

Sauvegarde de la base de données intégrée

Si vous utilisez la base de données intégrée, procédez comme suit pour créer une sauvegarde.

Pour accéder aux informations d'aide pour les commandes de base de données, tapez `osql ?` à l'invite DOS et appuyez sur Entrée.

Important : *Ne désinstallez pas la base de données.*

1 Connectez-vous au serveur hébergeant Connect Enterprise Server 6.

2 Créez un dossier pour stocker les fichiers de sauvegarde de la base de données.

Cet exemple utilise le dossier C:\Connect_Database.

3 Sélectionnez Démarrer > Exécuter, tapez **cmd** dans la zone Ouvrir, puis cliquez sur OK.

4 A l'invite, indiquez le répertoire dans lequel vous avez installé la base de données. Par défaut, le répertoire est c:\MSSQL\Binn.

Remarque : *Il s'agit du répertoire par défaut pour Connect Enterprise Server 6. Le répertoire par défaut pour Acrobat Connect Pro Server 7 est c:\Program Files\Microsoft SQL Server\90\Tools\Binn.*

5 A l'invite MSSQL\Binn, entrez **osql -E** pour vous connecter au moteur de base de données et appuyez ensuite sur Entrée.

6 Entrez **BACKUP DATABASE nom de la base de données TO DISK = 'C:\Connect_Database\Nom_base de données.bak'** pour exécuter un utilitaire Microsoft SQL qui sauvegarde la base de données Connect, puis appuyez sur Entrée.

Le nom de la base de données par défaut est *breeze* .

7 A l'invite, tapez **go** et appuyez sur Entrée.

Le fenêtre de commande affiche des messages relatifs à la sauvegarde.

8 A l'invite, tapez **quit** et appuyez sur Entrée.

9 Pour vérifier que la sauvegarde a réussi, assurez-vous que le fichier breeze.bak est bien présent dans le répertoire C:\Connect_Database.

10 Pour redémarrer votre base de données, depuis le bureau de Windows, choisissez Démarrer > Panneau de configuration > Outils d'administration > Services. Dans la fenêtre Services, cliquez avec le bouton droit sur SQL Server (MSSQLSERVER) et choisissez Démarrer dans le menu contextuel.

Pour plus d'informations sur la sauvegarde du moteur de base de données intégré, consultez l'article de Microsoft « Comment faire pour sauvegarder une base de données Microsoft Data Engine à l'aide de Transact-SQL ».

Migration de la base de données intégrée vers SQL Server

Procédez comme suit pour migrer de l'utilisation de la base de données intégrée à celle de SQL Server 2005 Standard Edition sur un autre ordinateur.

Remarque : *Vous pouvez effectuer cette migration lorsque vous migrez de Connect Enterprise 6 vers Acrobat Connect Pro Server 7. Sinon, vous pouvez également le faire à tout moment après avoir installé Acrobat Connect Pro Server 7.*

1. Installez SQL Server 2005 Standard Edition.

Suivez les instructions fournies par Microsoft pour installer SQL Server.

2. Sauvegardez la base de données intégrée.

Voir la section « Sauvegarde de la base de données » à la page 4.

Remarque : *La base de données intégrée est limitée à la version de SQL Server.*

3. Copiez le fichier .bak du serveur Acrobat Connect Pro sur le serveur qui héberge SQL Server.

Lorsque vous sauvegardez la base de données intégrée, un fichier nommé *breeze*.bak est créé (où *breeze* correspond au nom de la base de données).

4. Rétablissez la base de données sur le serveur qui héberge SQL Server 2005 Standard Edition.

Pour plus d'informations sur le rétablissement de SQL Server, consultez Microsoft TechNet.

5. Entrez les informations relatives à la base de données SQL Server dans la Console de gestion des applications sur le serveur qui héberge Acrobat Connect Pro.

Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Configurer Adobe Acrobat Connect Pro Server 7.

Préparation de l'installation

Présentation technique d'Acrobat Connect Pro

Une installation Acrobat Connect Pro comprend plusieurs composants : Connect Pro Central Application Server, Adobe® Flash® Media Server, Connect Pro Presence Service et une base de données.

Connect Pro Central Application Server est une version J2EE qui utilise des composants de Macromedia® JRun™ d'Adobe. Egalement appelé *serveur d'application*, il gère les utilisateurs, les groupes, le contenu à la demande et les sessions des clients. Parmi les tâches du serveur d'applications, on retrouve le contrôle d'accès, la sécurité, les quotas, les licences et les fonctions d'audit et de gestion, telles que la mise en cluster, le basculement et la réplication. Il se charge également du transcodage des supports, notamment la conversion du contenu Microsoft® PowerPoint et audio au format Adobe® Flash®. Le serveur d'applications gère les requêtes de réunion et de transfert de contenu (diapositives, pages HTTP, fichiers SWF et contenu du module Partage de fichiers) sur une connexion HTTP ou HTTPS.

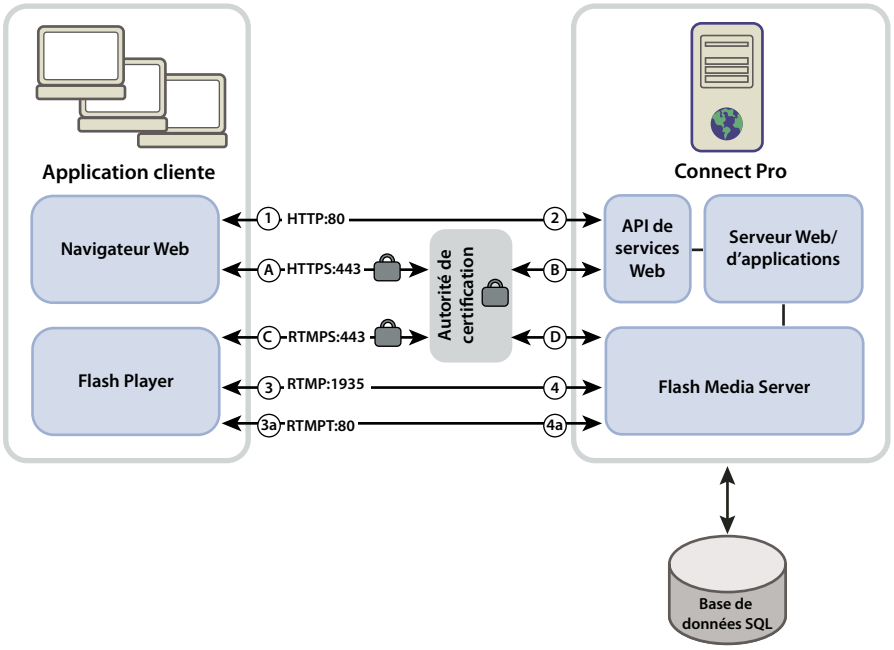
Flash Media Server, également appelé *serveur de réunions*, est installé avec Acrobat Connect Pro pour gérer la diffusion audio et vidéo en temps réel, la synchronisation des données et la diffusion des contenus multimédia, ainsi que les interactions avec Acrobat Connect Pro. Certaines tâches de Flash Media Server consistent à enregistrer et lire des réunions, à synchroniser le contenu audio et vidéo et à faire le transcodage (conversion et compression des données pour le partage d'écran en temps réel et les interactions). Flash Media Server réduit également la charge et les délais d'attente du serveur en mettant en cache les pages Web fréquemment visitées, les flux continus et les données partagées. Flash Media Server diffuse le son, la vidéo et les données de réunions associées via le protocole à haute performance RTMP ou RTMPS d'Adobe.

Connect Pro Presence Service intègre Acrobat Connect Pro à Microsoft® Live Communication Server 2005 et Microsoft® Office Communication Server pour afficher leur présence IM dans les salles de réunion Acrobat Connect Pro.

Acrobat Connect Pro requiert une base de données pour le stockage permanent des métadonnées transactionnelles et d'application, dont les informations sur les utilisateurs, les groupes, le contenu et les rapports. Vous pouvez utiliser le moteur de base de données intégré (MSDE) fourni dans le programme d'installation d'Acrobat Connect Pro Server 7 ou installer une version complète de Microsoft SQL Server. (Le moteur de base de données intégré est inclus dans l'installation d'Acrobat Connect Pro, mais pas Microsoft SQL Server.)

Flux de données

Le diagramme suivant illustre la circulation des données entre une application cliente et Acrobat Connect Pro.



Les données peuvent circuler sur une connexion chiffrée ou non chiffrée.

Connexion non chiffrée

Les connexions non chiffrées passent par HTTP et RTMP et empruntent les chemins décrits dans le tableau. Dans le tableau, les numéros correspondent à ceux du diagramme de flux des données.

Valeur numérique	Description
1	Le navigateur Web du client demande une réunion ou l'URL d'un contenu sur HTTP:80.
2	Le serveur Web répond et transfert le contenu ou fournit au client les informations nécessaires pour qu'il se connecte à la réunion.
3	Le Flash Player du client demande une connexion à la réunion sur RTMP:1935.
3a	Le Flash Player du client demande une connexion à la réunion, mais ne peut se connecter que sur RTMP:80.
4	Flash Media Server répond et ouvre une connexion permanente pour le trafic des flux continus d'Acrobat Connect.
4a	Flash Media Server répond et ouvre une connexion par tunnel pour le trafic des flux continus d'Acrobat Connect.

Connexion chiffrée

Les connexions chiffrées passent par HTTPS et RTMPS et empruntent les chemins décrits dans le tableau. Dans le tableau, les lettres correspondent à celles du diagramme de flux des données.

Lettre	Description
A	Le navigateur Web du client requiert une réunion ou l'URL d'un contenu via une connexion sécurisée sur HTTPS:443.
B.	Le serveur Web répond et transfert le contenu sur une connexion sécurisée ou fournit au client les informations nécessaires pour qu'il se connecte à la réunion de manière sécurisée.

Lettre	Description
C.	Le Flash Player du client demande une connexion sécurisée à Flash Media Server sur RTMPS:443.
D.	Flash Media Server répond et ouvre une connexion permanente et sécurisée pour le trafic des flux continus d'Acrobat Connect Pro.

Déroulement de l'installation

La procédure suivante vous aide à concevoir, installer et configurer un système Acrobat Connect Pro. Certaines étapes vous invitent à prendre des décisions, d'autres requièrent une tâche complète. Chaque étape vous renvoie vers des informations générales sur la décision ou la tâche.

1. Choisissez la base de données que vous souhaitez utiliser.

Pour plus d'informations, consultez la section « Choix d'une base de données » à la page 10.

2. Installez Acrobat Connect Pro sur un seul serveur.

Pour plus d'informations, consultez la section « Installation d'Acrobat Connect Pro Server 7 » à la page 13. Si vous choisissez d'utiliser le moteur de base de données intégré à l'étape 1, installez-le également. Le moteur de base de données intégré fait partie du programme d'installation d'Acrobat Connect Pro.

3. Si vous choisissez d'utiliser SQL Server 2005 Standard Edition à l'étape 1, installez-le.

Pour plus d'informations, consultez la documentation de SQL Server.

4. Déployez Acrobat Connect Pro.

Pour plus d'informations, consultez la section « Déploiement d'Acrobat Connect Pro Server 7 » à la page 22.

5. Assurez-vous qu'Acrobat Connect Pro est correctement installé.

Pour plus d'informations, consultez la section « Vérification de votre installation » à la page 16.

6. (Facultatif) Intégrez Acrobat Connect Pro à votre infrastructure.

De nombreuses possibilités permettent d'intégrer Acrobat Connect Pro à l'infrastructure existante de votre société. Il est généralement préférable de vérifier le bon fonctionnement d'Acrobat Connect Pro après la configuration de chacune de ces fonctionnalités.

Intégration à un annuaire LDAP Intégrez Acrobat Connect Pro au serveur d'annuaire LDAP de votre société pour éviter de devoir gérer plusieurs annuaires d'utilisateurs. Reportez-vous à la section « Intégration dans un service d'annuaire » à la page 28.

Configuration d'un protocole de communication sécurisé (SSL) Sécurisez l'ensemble des communications d'Acrobat Connect Pro. Voir SSL (Secure Sockets Layer).

Stockage du contenu sur des périphériques NAS/SAN Utilisez des périphériques réseau pour partager les tâches de stockage du contenu. Voir la section « Configuration du stockage partagé » à la page 35.

Intégration à Live Communication Server et Office Communication Server L'intégration à un serveur de communication permet aux hôtes de réunion de voir la présence IM des invités dans les salles de réunion. Les hôtes de réunion peuvent également envoyer des messages aux utilisateurs IM depuis la salle de réunion. Reportez-vous à la section « Intégration à Microsoft Live Communications Server 2005 et Microsoft Office Communications Server 2007 » à la page 39.

Configuration d'une infrastructure à clé publique (ICP) Si vous avez intégré Acrobat Connect Pro à un serveur d'annuaire LDAP, renforcez la sécurité en demandant des certificats clients. Reportez-vous à la section « Infrastructure à clé publique (ICP) » à la page 61.

Hébergement d'Acrobat Connect Add-in Les utilisateurs peuvent très facilement télécharger Acrobat Connect Add-in depuis les serveurs Adobe. Toutefois, si la stratégie de sécurité de votre société n'autorise pas les téléchargements externes, hébergez l'Add-in sur votre propre serveur pour améliorer le confort de vos utilisateurs. Voir la section « Hébergement d'Acrobat Connect Add-in » à la page 47.

7. (Facultatif) Choisissez d'installer ou non Acrobat Connect Pro Server 7 dans un cluster.

Pour plus d'informations, reportez-vous aux sections « Choix du déploiement d'Acrobat Connect Pro dans un cluster » à la page 9 et « Déploiement d'un cluster de serveurs Acrobat Connect Pro » à la page 22.

8. (Facultatif) Choisissez d'installer ou non des serveurs Edge.

Pour plus d'informations, consultez les sections « Choix du déploiement d'Acrobat Connect Pro Edge Server » à la page 11 et « Déploiement d'Acrobat Connect Pro Edge Server » à la page 26.

Choix du déploiement d'Acrobat Connect Pro dans un cluster

Il est possible d'installer tous les composants Acrobat Connect Pro Server 7, y compris la base de données, sur un seul serveur, mais cette configuration convient mieux à un environnement de test que de production.

Un groupe de serveurs connectés, chacun faisant le même travail, est généralement appelé *cluster*. Dans un cluster Acrobat Connect Pro Server 7, vous installez une copie identique d'Acrobat Connect Pro Server 7 sur chacun de ses serveurs.

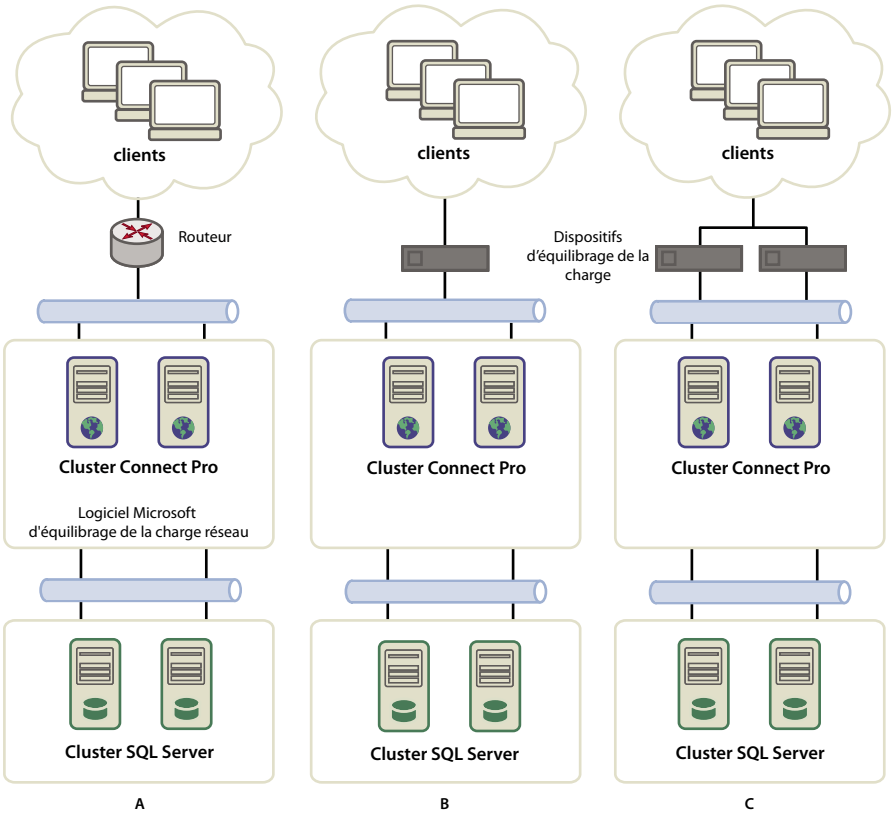
Remarque : *Lorsque vous installez Acrobat Connect Pro Server 7 dans un cluster, vous devez utiliser SQL Server 2005 Standard Edition et l'installer sur un ordinateur distinct.*

Tous les ordinateurs d'un cluster disposent de copies du même contenu. Lorsqu'un ordinateur du cluster échoue, un autre prend le relais et peut héberger la même réunion. Pour assurer l'équilibrage de charge du cluster, vous devez utiliser un logiciel ou un matériel tiers. Très souvent, le matériel d'équilibrage de charge peut également fonctionner comme un accélérateur SSL.

Remarque : *La Console de gestion des applications permet de configurer le stockage partagé de sorte que le contenu soit stocké sur des périphériques externes et mis en cache sur Acrobat Connect Pro Server 7.*

Les systèmes réseau fiables sont conçus avec des composants redondants : si l'un échoue, un autre composant identique (*redondant*) prend en charge le même travail. Lorsqu'un composant échoue et qu'un autre prend le relais, un *basculement* intervient.

Idéalement, chaque composant d'un système doit être redondant, pas seulement le serveur Acrobat Connect Pro 7. Par exemple, vous pouvez utiliser plusieurs périphériques matériels d'équilibrage de charge (tels que BIG-IP de F7 Networks), un cluster de serveurs hébergeant Acrobat Connect Pro Server 7 et des bases de données SQL Server sur plusieurs ordinateurs externes. Concevez votre système avec autant de redondances que possible et ajoutez-les progressivement à votre système.



Trois options de mise en cluster
***A.** Un cluster avec logiciel d'équilibrage NLB et deux bases de données externes **B.** Des périphériques d'équilibrage matériel BIG-IP, un cluster et deux bases de données externes **C.** Deux périphériques d'équilibrage BIG-IP, un cluster et deux bases de données externes*

Voir aussi

« Déploiement d'un cluster de serveurs Acrobat Connect Pro » à la page 22

« Configuration du stockage partagé » à la page 35

Choix d'une base de données

Acrobat Connect Pro Server 7 stocke les informations sur les utilisateurs, le contenu, les cours, les réunions et les rapports dans une base de données. Vous pouvez utiliser le moteur de base de données intégré (inclus avec le programme d'installation) ou installer Microsoft SQL Server 2005 Standard Edition (vendu séparément).

***Remarque :** Le moteur de base de données intégré est Microsoft SQL Server 2005 Express Edition.*

Base de données intégrée

Le moteur de base de données intégré est recommandé pour les phases de test et de développement. Il utilise les mêmes structures de données que SQL Server 2005 Standard Edition, mais n'est pas aussi puissant.

Le moteur de base de données intégré présente les limites suivantes :

- Du fait des restrictions de licence, vous devez l'installer sur le même ordinateur qu'Acrobat Connect Pro Server 7. Cet ordinateur doit être mono-processeur.
- La taille maximale de la base de données est de 2 Go.
- Le moteur de base de données intégré possède une interface de ligne de commande, et non une interface utilisateur graphique.

Microsoft SQL Server 2005 Standard Edition

Il est généralement préférable d'utiliser le moteur Microsoft SQL Server 2005 Standard Edition dans les environnements de production, car SQL Server est un système de gestion de bases de données évolutif (SGBDR) conçu pour prendre en charge un grand nombre d'utilisateurs simultanés. SQL Server 2005 Standard Edition fournit également des interfaces utilisateur graphiques pour la gestion et les interrogations de la base de données.

Vous pouvez installer SQL Server 2005 Standard Edition sur le même ordinateur qu'Acrobat Connect Pro Server 7 ou sur un autre ordinateur. Si vous les installez sur des ordinateurs différents, synchronisez ces machines sur la même source horaire. Pour plus d'informations, consultez la TechNote suivante : www.adobe.com/go/2e86ea67_fr.

Installez SQL Server en mode de connexion mixte afin de pouvoir utiliser l'authentification SQL. Définissez la base de données pour respecter la casse.

Utilisez SQL Server dans les scénarios de déploiement suivants :

- Vous souhaitez installer la base de données sur un ordinateur sur lequel Acrobat Connect Pro Server 7 n'est pas installé.
- Acrobat Connect Pro Server 7 est déployé dans un cluster.
- Acrobat Connect Pro Server 7 est installé sur des ordinateurs multi-processeurs avec Hyper-Threading.

Voir aussi

« Configurations de bases de données/serveur prises en charge » à la page 2

« Installation d'Acrobat Connect Pro Server 7 » à la page 13

Choix du déploiement d'Acrobat Connect Pro Edge Server

Lorsque vous déployez Acrobat Connect Edge Server sur votre réseau, les clients se connectent au serveur Edge qui, à son tour, se connecte à Acrobat Connect Pro (également appelé *serveur d'origine*). Cette connexion est transparente : les utilisateurs ont l'impression de se connecter directement au serveur d'origine qui héberge la réunion.

Les serveurs Edge présentent les avantages suivants :

Latence réseau réduite Les serveurs Edge mettent le contenu en cache à la demande (par exemple les réunions et les présentations enregistrées) et divisent les flux en direct, entraînant moins de trafic vers l'origine. Les serveurs Edge rapprochent les ressources des clients.

Stratégies Les serveurs Edge constituent une couche supplémentaire entre la connexion Internet cliente et l'origine.

Si votre licence l'autorise, vous pouvez installer et configurer un cluster de serveurs Edge. Le déploiement des serveurs Edge dans un cluster présente les avantages suivants :

Basculement Lorsqu'un serveur Edge échoue, les clients sont dirigés vers un autre serveur Edge.

Prise en charge pour des événements importants S'il vous faut plus de 500 connexions simultanées pour la même réunion, un seul serveur Edge n'aura plus assez de sockets. Un cluster autorise davantage de connexions à la même réunion.

Equilibrage de charge S'il vous faut plus de 100 réunions simultanées, un seul serveur Edge peut manquer de mémoire. Les serveurs Edge peuvent être placés en cluster derrière un équilibreur de charge.

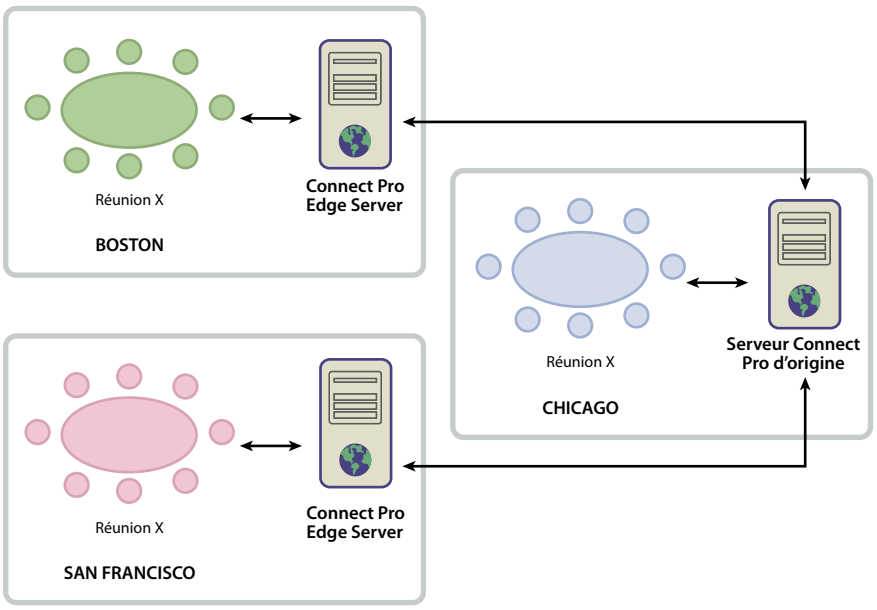
Fonctionnement des serveurs Edge

Les serveurs Edge authentifient les utilisateurs et autorisent leurs requêtes de services Web, telles qu'Acrobat Connect Pro Meeting, au lieu de transmettre chaque requête au serveur d'origine et de consommer les ressources de ce dernier pour ces tâches. Si les données demandées sont détectées dans le cache du serveur Edge, ce dernier les envoie au client sans appeler Acrobat Connect Pro.

Si les données demandées ne sont pas dans le cache du serveur Edge, ce dernier transmet la requête du client au serveur d'origine, où l'utilisateur est authentifié et la demande de services autorisée. Le serveur d'origine renvoie les résultats au serveur Edge, qui les transmet à son tour au client. Le serveur Edge stocke également ces informations dans sa mémoire cache, permettant ainsi à d'autres utilisateurs authentifiés d'y accéder.

Exemple de déploiement de serveur Edge

Considérez l'exemple de déploiement de serveur Edge suivant :



Les clients du site de Chicago utilisent le serveur d'origine situé dans un centre de données de Chicago. Les serveurs Edge de Boston et San Francisco réunissent les requêtes des clients locaux et les transmettent à l'origine. Les serveurs Edge reçoivent les réponses de l'origine à Chicago et les transmettent aux clients de leur régions.

Voir aussi

« Installation d'Acrobat Connect Pro Edge Server 7 » à la page 18

« Déploiement d'Acrobat Connect Pro Edge Server 7 » à la page 25

Chapitre 2 : Installation d'Acrobat Connect Pro Server 7 et d'Acrobat Connect Pro Edge Server 7

Pour installer Acrobat Connect Pro Server 7 et Acrobat Connect Pro Edge Server 7, exécutez le programme d'installation et suivez les étapes de l'Assistant de la Console de gestion des applications.

Installation d'Acrobat Connect Pro Server 7

Exécution du programme d'installation

1 Fermez toutes les applications.

2 Insérez le DVD d'installation dans votre lecteur. Dans l'écran de démarrage, cliquez sur le bouton Installation d'Adobe Acrobat Connect Pro Server 7.

Si le programme d'installation de ne démarre pas automatiquement, double-cliquez sur le fichier setup.exe dans le dossier racine d'installation du DVD.

3 Sélectionnez une langue dans la boîte de dialogue prévue à cet effet. Cliquez sur OK pour continuer.

4 Dans l'écran de configuration, cliquez sur Suivant pour continuer.

5 Dans l'écran d'accord de licence qui apparaît, lisez le contrat, sélectionnez J'accepte les termes de ce contrat, puis cliquez sur Suivant.

6 Pour sélectionner l'emplacement d'installation, effectuez l'une des opérations suivantes :

- Cliquez sur Suivant pour accepter le répertoire·d'installation par défaut (c:\breeze), ou cliquez sur Parcourir pour choisir un autre emplacement, puis cliquez sur Suivant.
- Si Acrobat Connect Pro est déjà installé sur cet ordinateur, la fenêtre de mise à jour de l'installation apparaît. Activez la case à cocher qui confirme que vous avez bien sauvegardé votre base de données et le répertoire racine de Connect Pro. Cliquez sur Suivant.

7 Dans la fenêtre Informations sur la société, entrez votre numéro de série et cliquez sur Suivant.

8 Effectuez l'une des opérations suivantes :

- Si la fenêtre du moteur de base de données intégré apparaît, choisissez de l'installer ou non. Si vous souhaitez l'installer à l'emplacement par défaut (c:\Program Files\Microsoft SQL Server), cliquez sur Suivant. Pour choisir un autre emplacement, cliquez sur Parcourir pour sélectionner un autre répertoire, puis cliquez sur Suivant. Si vous préférez ne pas installer le moteur de base de données intégré (car vous envisagez d'utiliser Microsoft SQL Server), sélectionnez Ne pas installer le moteur de base de données intégré, puis cliquez sur Suivant.
- Si le programme d'installation détecte que le moteur de base de données intégré ou Microsoft SQL Server est déjà installé sur l'ordinateur, le moteur de base de données intégré n'est pas installé. Si le moteur de base de données intégré est déjà installé, l'emplacement ne peut pas être modifié. Cliquez sur Suivant.

Remarque : *Il arrive parfois qu'une ancienne version de la base de données intégrée ne soit pas correctement supprimée et que le programme d'installation s'en aperçoive. Suivez les instructions de la TechNote 18927 (www.adobe.com/go/tn_18927_fr) et recommencez l'installation.*

9 Dans l'écran Sélectionnez un groupe de programmes, effectuez l'une des opérations suivantes :

- Cliquez sur Suivant pour accepter le nom et l'emplacement par défaut des raccourcis du menu Démarrer (Adobe Acrobat Connect Pro Server 7).
- Cliquez sur Parcourir pour sélectionner un autre emplacement, puis cliquez sur Suivant.

10 Dans la boîte de dialogue Prêt pour l'installation, vérifiez le répertoire d'installation, le nom et l'emplacement du menu Démarrer. Cliquez sur Précédent pour vérifier ou modifier ces paramètres, ou cliquez sur Installer.

La fenêtre d'installation s'affiche pendant l'installation de l'application.

11 Si vous avez choisi d'installer le moteur de base de données intégré, sa fenêtre d'installation apparaît. Entrez un mot de passe pour l'utilisateur « sa » de la base de données, puis cliquez sur Suivant pour commencer l'installation.

12 Dans l'écran Initialisation du service Connect Pro, effectuez l'une des opérations suivantes, puis cliquez sur Suivant :

- Sélectionnez Ne pas démarrer Connect Pro maintenant...
- Il est recommandé de sélectionner Démarrer Connect Pro et d'ouvrir un navigateur pour lancer l'Assistant de la Console de gestion des applications pour poursuivre la configuration.

13 Si vous avez démarré Acrobat Connect Pro, un message vous signale que le service démarre.

Acrobat Connect Pro Server 7 exécute quatre services Windows : Adobe Connect Enterprise Service, Flash Media Server (FMS), Flash Media Administration Server et Acrobat Connect Pro Presence Server. Voir « Démarrage et arrêt des serveurs » à la page 18.

14 Dans le programme d'installation, cliquez sur Terminer.

Si vous avez choisi Démarrer Connect Pro, l'Assistant de la Console de gestion des applications s'ouvre dans une fenêtre de navigateur pour vous guider tout au long des tâches de configuration.

Configuration d'Acrobat Connect Pro avec l'Assistant de la Console de gestion des applications

Après l'installation d'Acrobat Connect Pro, le programme d'installation démarre automatiquement l'Assistant de la Console de gestion des applications pour vous guider tout au long de la configuration des paramètres de la base de données et du serveur, du chargement de votre fichier de licence et de la création d'un administrateur.

Remarque : *Si une autre application s'exécute sur le port 80, la Console de gestion des applications ne s'ouvre pas. Arrêtez l'application qui occupe le port 80 et rouvrez la Console de gestion des applications.*

Pour accéder à la Console de gestion des applications, choisissez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Configurer Adobe Connect Pro Server 7, ou utilisez l'URL suivante : http://localhost:8510/console.

1. Lisez l'écran de bienvenue.

L'écran de bienvenue présente l'Assistant.

2. Entrez les paramètres de la base de données.

Définissez les valeurs des paramètres énumérés ci-dessous. Cliquez sur Suivant pour vous connecter à la base de données et vérifier vos paramètres.

Hôte de base de données Nom d'hôte de l'ordinateur sur lequel la base de données est installée. Si vous installez la base de données intégrée, la valeur est localhost.

Nom de la base de données Nom de la base de données. La valeur par défaut est breeze.

Port de base de données Port que la base de données utilise pour communiquer avec Acrobat Connect Pro. La valeur par défaut est 1433. (Si vous utilisez le moteur de base de données intégré, sélectionnez la valeur 1434.)

Utilisateur de base de données Nom de l'utilisateur de la base de données. Si vous avez installé la base de données intégrée, la valeur par défaut est « sa ».

Mot de passe de l'utilisateur de base de données Mot de passe de l'utilisateur de la base de données. Si vous avez installé la base de données intégrée, il s'agit de la valeur définie dans le programme d'installation.

3. Entrez les paramètres du serveur.

Nom du compte Nom qui identifie le compte Acrobat Connect Pro, par exemple « Compte Acrobat Connect Pro 7 ».

Hôte Connect Pro Nom de domaine pleinement qualifié (FQDN) que les clients utilisent pour se connecter à Acrobat Connect Pro. Par exemple, avec l'URL de compte http://connect.exemple.com, la valeur de l'hôte Connect Pro serait connect.exemple.com.

Port HTTP Port utilisé par Acrobat Connect Pro pour communiquer via le protocole HTTP. La valeur par défaut est 80. Si vous entrez une autre valeur que 80, les clients doivent ajouter ce numéro de port au nom d'hôte dans l'URL lorsqu'ils accèdent au compte Acrobat Connect Pro.

Mappages d'hôtes Nom correspond au nom d'hôte de l'ordinateur qui héberge Acrobat Connect Pro. Nom externe correspond au nom de domaine pleinement qualifié que les clients utilisent pour se connecter à Acrobat Connect Pro.

Remarque : *N'ajoutez pas de port au nom FQDN dans la zone Nom externe.*

Hôte SMTP Nom d'hôte de l'ordinateur hébergeant le serveur de messagerie SMTP.

Adresse de messagerie système Adresse de messagerie depuis laquelle les messages électroniques administratifs sont envoyés.

Adresse de messagerie de l'Assistance Adresse de messagerie de l'Assistance destinée aux utilisateurs d'Acrobat Connect Pro.

Adresse de messagerie Cci Adresse de messagerie en copie cachée à laquelle toutes les notifications destinées aux utilisateurs sont également envoyées. Cette variable autorise un suivi administratif des messages électroniques envoyés via Acrobat Connect Pro sans que l'adresse de messagerie interne ne soit exposée.

Stockage partagé Volume et répertoire d'un serveur externe où le contenu sera stocké, par exemple, \\volume\répertoire. Pour stocker du contenu sur plusieurs volumes, séparez-les par des points virgules (;). Avant de configurer cette fonction, consultez la section « Configuration du stockage partagé » à la page 35.

Taille du contenu mis en cache Nombre entier compris entre 1 et 100 définissant le pourcentage d'espace disque à utiliser pour stocker le contenu sur Acrobat Connect Pro. Le cache pouvant grossir au-delà du pourcentage spécifié, dès lors il est préférable de choisir une valeur comprise entre 15 et 50. Si vous ne renseignez pas ce champ ou si vous entrez 0, aucun cache n'est utilisé et le contenu est copié en miroir sur Acrobat Connect Pro et tous les volumes externes. Avant de configurer cette fonction, consultez la section « Configuration du stockage partagé » à la page 35.

4. Chargez le fichier de licence.

Pour activer Acrobat Connect Pro, vous devez télécharger un fichier de licence d'Adobe et l'installer sur l'ordinateur qui héberge Acrobat Connect Pro. Cette fenêtre de l'Assistant fournit un lien de téléchargement et un formulaire qui vous permet de sélectionner le fichier de licence téléchargé et de le copier dans votre installation d'Acrobat Connect Pro.

5. Créez un administrateur de compte.

Chaque compte Acrobat Connect Pro doit disposer d'au moins un administrateur chargé d'effectuer des tâches dans l'application Web Connect Pro Central. Les comptes mis à niveau possèdent déjà un administrateur, mais vous pouvez en ajouter un autre ici.

6. Continuez à utiliser Connect Pro.

Il s'agit du dernier écran de l'Assistant de la Console de gestion des applications. A partir de là, vous pouvez vous connecter au gestionnaire Enterprise Manager (l'application Web qui vous permet de gérer votre compte, de créer des réunions, des événements, etc., et de gérer le contenu sur l'ordinateur qui héberge Acrobat Connect Pro), revenir dans la Console de gestion des applications (pour modifier ou vérifier vos paramètres) ou consulter la documentation pour en savoir plus sur Connect Pro.

Vérification de votre installation

Vérification de la connectivité de la base de données

Si vous pouvez vous connecter à Connect Pro Central (application Web située dans Acrobat Connect Pro), la base de données et Acrobat Connect Pro peuvent fonctionner ensemble.

1 Accédez à l'adresse URL suivante : http://*[nomhôte]* .

Remarque : *Dans cette URL, [nomhôte] correspond à la valeur définie pour Hôte Connect Pro dans la Console de gestion des applications.*

2 Entrez l'identifiant de connexion et le mot de passe définis dans la Console de gestion des applications.

Si vous pouvez vous connecter, l'onglet d'accueil de Connect Pro Central apparaît.

Vérification du bon fonctionnement des notifications électroniques

Si vous avez choisi de ne pas renseigner le champ Hôte SMTP dans la fenêtre Paramètres de l'application > Paramètres du serveur de la Console de gestion des applications, Acrobat Connect Pro n'enverra pas de notifications électroniques et vous pouvez ignorer cette section.

1 Dans l'onglet d'accueil de Connect Pro, cliquez sur l'onglet Administration.

2 Ouvrez l'onglet Utilisateurs et groupes.

3 Cliquez sur Nouvel utilisateur.

4 Dans la page Informations sur le nouvel utilisateur, entrez les informations requises. Voici une liste partielle des options :

Adresse de messagerie Utilisez l'adresse électronique du nouvel utilisateur. Assurez-vous que l'option Envoyer par message électronique les informations sur le nouveau compte, nom d'utilisateur et mot de passe est activée.

Nouveau mot de passe Créez un mot de passe de 4 à 16 caractères.

5 Cliquez sur Suivant pour continuer.

6 Sous l'en-tête Modifier l'appartenance à un groupe, sélectionnez un groupe, affectez l'utilisateur au groupe et cliquez sur Terminer.

7 Laissez suffisamment de temps à l'utilisateur pour recevoir sa notification électronique.

Si l'utilisateur a reçu la notification, Acrobat Connect Pro fonctionne et vous pouvez envoyer des messages électroniques à l'aide du serveur de messagerie.

8 Si le message électronique n'arrive pas, procédez comme suit :

a Vérifiez la validité de l'adresse de messagerie.

b Assurez-vous que le message n'ait pas été filtré en tant que courrier indésirable.

c Assurez-vous d'avoir configuré Acrobat Connect Pro avec un hôte SMTP valide et que le service SMTP fonctionne en dehors d'Acrobat Connect Pro.

d Contactez l'Assistance technique d'Adobe à l'adresse www.adobe.com/go/connect_licensed_programs_fr.

Vérification du bon fonctionnement d'Adobe Presenter

Pour vérifier le bon fonctionnement d'Adobe Presenter, envoyez une présentation Microsoft PowerPoint à Acrobat Connect Pro pour sa compilation en présentation Flash, puis affichez-la.

Avant de pouvoir envoyer une présentation PowerPoint à Acrobat Connect Pro, vous devez installer Adobe Presenter sur un ordinateur sur lequel PowerPoint est déjà installé.

1 Insérez le CD d'Adobe Acrobat Connect Pro Server 7 dans votre lecteur.

2 Cliquez sur Installer Adobe Presenter 7 et suivez les instructions.

3 Si vous n'avez pas de présentation PowerPoint à envoyer à Acrobat Connect Pro pour sa compilation en présentation Flash, créez-en une avec une ou deux diapositives et enregistrez-la.

4 Ouvrez l'Assistant de publication de Connect Pro en choisissant Publier dans le menu Adobe Presenter de PowerPoint.

5 Sélectionnez Connect Pro et entrez les informations sur votre serveur.

6 Connectez-vous avec votre adresse de messagerie et votre mot de passe et suivez les instructions de l'Assistant de publication. Assurez-vous de faire partie du groupe Auteurs (Administration > Utilisateurs et Groupes dans Connect Pro Central).

Lorsque vous avez terminé les étapes de l'Assistant de publication, Adobe Presenter charge votre présentation PowerPoint sur Connect Pro qui la compile en présentation Flash.

7 A la fin de la compilation, ouvrez l'onglet Contenu dans Connect Pro Central et recherchez votre présentation.

8 Ouvrez votre présentation pour l'afficher.

Vérification du bon fonctionnement du module Formation

Remarque : *Adobe Acrobat Connect Pro Training est une fonctionnalité optionnelle qui doit être activée dans votre licence.*

❖ Cliquez sur l'onglet Formation de Connect Pro Central.

Si vous pouvez afficher et accéder à l'onglet Formation, Connect Training fonctionne correctement. Assurez-vous de faire partie du groupe Directeurs·de formation (Administration > Utilisateurs et Groupes).

Vérification du bon fonctionnement du module Réunion

Remarque : *Adobe Acrobat Connect Pro Meeting est une fonctionnalité optionnelle qui doit être activée dans votre licence.*

Pour vérifier le bon fonctionnement d'Acrobat Connect Pro Meeting, vous devez faire partie du groupe Hôtes de réunions ou du groupe Administrateurs.

1 Connectez-vous à Connect Pro Central en tant qu'utilisateur membre du groupe Hôtes de réunions ou Administrateurs.

2 Cliquez sur l'onglet Réunions et sélectionnez Nouvelle réunion.

3 Dans la page Entrer les informations sur la réunion, entrez les informations requises. Pour l'option Accès à la réunion, choisissez Seuls les utilisateurs inscrits et les visiteurs acceptés sont admis à la réunion. Cliquez sur Terminer pour créer la réunion.

4 Cliquez sur le bouton Entrer dans la salle de réunion.

5 Identifiez-vous pour participer à la réunion en tant qu'utilisateur inscrit.

6 Si la fenêtre Acrobat Connect Add-in apparaît, suivez les instructions pour l'installer.

Si la salle de réunion s'ouvre, Acrobat Connect Pro Meeting fonctionne correctement.

Vérification du bon fonctionnement du module Evénements

Remarque : *Adobe Acrobat Connect Pro Events est une fonctionnalité optionnelle qui doit être activée dans votre licence.*

1 Connectez-vous à Connect Pro Central en tant qu'utilisateur membre du groupe Gestionnaires d'événements ou Administrateurs.

2 Cliquez sur l'onglet Evénements de Connect Pro Central.

Si vous pouvez afficher et accéder à cet onglet, Connect Pro Events fonctionne correctement.

Installation d'Acrobat Connect Pro Edge Server 7

Exécution du programme d'installation

1 Fermez toutes les autres applications.

2 Insérez le DVD d'installation dans votre lecteur. Dans l'écran de démarrage, cliquez sur le bouton Installation d'Adobe Acrobat Connect Pro Edge Server 7.

Si le programme d'installation ne démarre pas automatiquement, double-cliquez sur le fichier edgesetup.exe dans le dossier racine d'installation du DVD.

3 Sélectionnez une langue dans la boîte de dialogue prévue à cet effet. Cliquez sur OK pour continuer.

4 Dans l'écran de configuration, cliquez sur Suivant pour continuer.

5 Dans l'écran d'accord de licence qui apparaît, lisez le contrat, sélectionnez J'accepte les termes de ce contrat, puis cliquez sur Suivant.

6 Effectuez l'une des opérations suivantes :

- Cliquez sur Suivant pour accepter le répertoire d'installation par défaut (c:\breeze), ou cliquez sur Parcourir pour choisir un autre emplacement, puis cliquez sur Suivant.
- Si Adobe Acrobat Connect Pro Edge Server est déjà installé sur cet ordinateur, la fenêtre de mise à jour de l'installation existante d'Adobe Acrobat Connect Pro Edge Server apparaît. Cliquez sur Suivant.

7 Dans la fenêtre Sélectionnez un groupe de programmes, cliquez sur Suivant pour accepter l'emplacement par défaut des raccourcis du menu Démarrer ou cliquez sur Parcourir pour choisir un autre emplacement et cliquez sur Suivant.

8 Dans la boîte de dialogue Prêt pour l'installation, vérifiez les emplacements d'installation d'Adobe Acrobat Connect Pro Edge Server et du dossier du menu de démarrage. Cliquez sur Précédent pour vérifier ou modifier ces paramètres, ou cliquez sur Installer.

9 Cliquez sur Terminer pour quitter l'installation d'Adobe Acrobat Connect Pro Edge Server 7.

Voir aussi

« Déploiement d'Acrobat Connect Pro Edge Server 7 » à la page 25

Démarrage et arrêt des serveurs

Démarrage et arrêt d'Acrobat Connect Pro Server 7

Vous pouvez démarrer ou arrêter Acrobat Connect Pro via le menu Démarrer, la fenêtre Services ou la ligne de commande.

Arrêt d'Acrobat Connect Pro via le menu Démarrer

1 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

2 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Meeting Server.

Démarrage d'Acrobat Connect Pro via le menu Démarrer

1 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Meeting Server.

2 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

Arrêt d'Acrobat Connect Pro via la fenêtre Services

1 Choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Arrêtez le service Adobe Connect Enterprise Service.

3 Arrêtez le service Flash Media Server (FMS).

4 Arrêtez le service Flash Media Administration Server.

Démarrage d'Acrobat Connect Pro via la fenêtre Services

1 Choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Démarrez le service Flash Media Server (FMS).

3 Démarrez le service Flash Media Server Administration Server.

4 Démarrez le service Adobe Connect Enterprise Service.

Arrêt d'Acrobat Connect Pro via la ligne de commande

1 Choisissez Démarrer > Exécuter pour ouvrir la fenêtre Exécuter. Entrez **cmd** pour ouvrir une invite de commande.

2 Entrez la commande suivante pour arrêter Acrobat Connect Pro :

```
net stop BreezeApp
```

3 Pour arrêter Flash Media Server, tapez :

```
net stop FMS
```

4 Pour arrêter Flash Media Server Administration Server, tapez :

```
net stop FMSAdmin
```

Démarrage d'Acrobat Connect Pro via la ligne de commande

1 Choisissez Démarrer > Exécuter pour ouvrir la fenêtre Exécuter. Entrez **cmd** pour ouvrir une invite de commande.

2 Pour démarrer Flash Media Server, tapez :

```
net start FMS
```

3 Pour démarrer Flash Media Server Administration Server, tapez :

```
net start FMSAdmin
```

4 Entrez la commande suivante pour démarrer Acrobat Connect Pro :

```
net start BreezeApp
```

Démarrage et arrêt de Connect Pro Presence Service

Vous pouvez arrêter et démarrer Connect Pro Presence Service dans le menu Démarrer ou dans la fenêtre Services. Ne démarrez Connect Pro Presence Service que si votre système Acrobat Connect Pro est intégré à Microsoft Live Communications Server ou à Office Communications Server.

Voir aussi

« Intégration à Microsoft Live Communications Server 2005 et Microsoft Office Communications Server 2007 » à la page 39

Arrêt du service de présence via le menu Démarrer

❖ Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Presence Service.

Lancement du service de présence via le menu Démarrer

❖ Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Presence Service.

Arrêt, démarrage ou redémarrage du service de présence via la fenêtre Services

1 Choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Sélectionnez Connect Pro Presence Service.

3 Sélectionnez Démarrer, Arrêter ou Redémarrer le service.

Démarrage et arrêt d'Acrobat Connect Pro Edge Server 7

Vous pouvez démarrer ou arrêter Acrobat Connect Pro Edge Server 7 via le menu Démarrer, la fenêtre Services ou la ligne de commande.

Arrêt d'Acrobat Connect Pro Edge Server 7 via le menu Démarrer

❖ Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Edge Server 7 > Arrêter Connect Pro Edge Server.

Démarrage d'Acrobat Connect Pro Edge Server 7 via le menu Démarrer

❖ Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Edge Server 7 > Démarrer Connect Pro Edge Server.

Arrêt d'Acrobat Connect Pro Edge Server 7 via la fenêtre Services

1 Choisissez Démarrer > Paramètres > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Arrêtez le service Flash Media Server (FMS).

3 Arrêtez le service Flash Media Server Administration Server.

Démarrage d'Acrobat Connect Pro Edge Server via la fenêtre Services

1 Choisissez Démarrer > Paramètres > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Démarrez le service Flash Media Server Administration Server.

3 Démarrez le service Flash Media Server (FMS).

Arrêt d'Acrobat Connect Pro Edge Server via la ligne de commande

1 Choisissez Démarrer > Exécuter pour ouvrir la fenêtre Exécuter. Entrez **cmd** pour ouvrir une invite de commande.

2 Pour arrêter Flash Media Server, tapez :

```
net stop FMS
```

3 Pour arrêter Flash Media Server Administrator Server, tapez :

```
net stop FMSAdmin
```

Démarrage d'Acrobat Connect Pro Edge Server via la ligne de commande

1 Choisissez Démarrer > Exécuter pour ouvrir la fenêtre Exécuter. Entrez **cmd** pour ouvrir une invite de commande.

2 Pour démarrer Flash Media Server Administrator Server, tapez :

```
net start FMSAdmin
```

3 Pour démarrer Flash Media Server, tapez :

```
net start FMS
```

Désinstallation des serveurs

Désinstallation d'Acrobat Connect Pro Server 7

1 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Désinstaller Connect Pro Server 7.

2 Supprimez le dossier Acrobat Connect Pro racine. Par défaut, l'emplacement est C:\breeze.

Lorsque vous désinstallez Acrobat Connect Pro, les fichiers custom.ini et config.ini et les fichiers de contenu ne sont pas supprimés. Ces fichiers sont supprimés en même temps que le répertoire racine.

3 (Facultatif) Si le moteur de base de données intégré a été installé, vous devez supprimer son entrée dans le registre. Choisissez Démarrer > Exécuter et entrez **regedit** dans le champ Ouvrir.

Dans l'Éditeur du Registre, supprimez la clé HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server. S'il y a également une clé HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLServer, supprimez-la aussi.

Désinstallation d'Acrobat Connect Pro Edge Server 7

1 Sélectionnez Démarrer > Paramètres > Panneau de configuration Paramètres > Ajout/Suppression de programmes > Adobe Acrobat Connect Pro Edge Server 7 > Supprimer.

2 Supprimez le dossier Acrobat Connect Pro racine. Par défaut, l'emplacement est C:\breeze.

Chapitre 3 : Déploiement et configuration d'Acrobat Connect Pro Server 7 et d'Acrobat Connect Pro Edge Server 7

Après avoir installé Adobe Acrobat Connect Pro Server 7 ou Adobe Acrobat Connect Pro Edge Server 7 et terminé la première phase de configuration avec la console de gestion des applications, configurez l'une de ces fonctions facultatives et déployez le serveur.

Déploiement d'Acrobat Connect Pro Server 7

Déploiement d'un seul serveur Acrobat Connect Pro

1 Sur votre serveur DNS, définissez un nom de domaine pleinement qualifié pour Acrobat Connect Pro (par exemple, connect.masociété.com). Mappez ce nom de domaine sur l'adresse IP statique de l'ordinateur qui héberge Acrobat Connect Pro.

2 Si vous souhaitez qu'Acrobat Connect Pro soit disponible hors de votre réseau, configurez les ports suivants dans un pare-feu :

80 Port associé par défaut au serveur d'applications Acrobat Connect Pro. Port tertiaire du serveur de réunions (Flash Media Server).

1935 Port par défaut du serveur de réunions (Flash Media Server).

443 Port par défaut pour SSL. Port secondaire du serveur de réunions (Flash Media Server).

Remarque : *Si le trafic d'Acrobat Connect Pro passe par une passerelle (avec une adresse IP différente), assurez-vous que les pare-feu soient configurés pour accepter les requêtes provenant de l'adresse IP de cette passerelle.*

Pour obtenir de l'aide pour le déploiement d'Acrobat Connect Pro, contactez l'assistance technique d'Adobe à l'adresse www.adobe.com/go/connect_licensed_programs_fr.

Déploiement d'un cluster de serveurs Acrobat Connect Pro

Avant de déployer un cluster, les éléments suivants sont nécessaires :

- Une licence prenant en charge le nombre de nœuds que compte votre cluster. Pour plus d'informations, contactez votre représentant Adobe.
- Chaque ordinateur du cluster doit posséder une adresse IP statique et une entrée DNS.
- Un serveur de messagerie.
- Une installation SQL Server sur un ordinateur dédié disposant d'une adresse IP statique. Si vous installez Acrobat Connect Pro dans un cluster, vous ne pouvez pas utiliser le moteur de base de données intégré. Chaque serveur hébergeant Acrobat Connect Pro se connecte à la base de données, mais les restrictions de licence n'autorisent la connexion que d'un seul serveur au moteur de base de données intégré.
- Une solution d'équilibrage de charge matérielle ou logicielle. Une solution d'équilibrage de charge matérielle nécessite un ordinateur distinct avec une adresse IP statique et une entrée DNS. Une solution logicielle peut être installée sur l'un des nœuds du cluster.
- Un ou plusieurs volumes de stockage partagé. Cette configuration n'est pas obligatoire, mais recommandée.

Avant de pouvoir déployer Acrobat Connect Pro dans un cluster, installez-le sur un seul ordinateur. Configurez également les fonctionnalités supplémentaires (par exemple, SSL, une intégration de service d'annuaire, une authentification unique, un stockage de contenu partagé, etc.) et vérifiez qu'elles fonctionnent correctement sur ce serveur.

1 Installez et configurez Acrobat Connect Pro sur un serveur dédié.

Utilisez les mêmes numéro de série et fichier de licence pour chaque installation d'Acrobat Connect Pro. N'installez pas le moteur de base de données intégré et, si votre solution de stockage partagé requiert la saisie d'un nom d'utilisateur et d'un mot de passe, ne démarrez pas Acrobat Connect Pro à partir du programme d'installation.

2 Si votre solution de stockage partagé requiert la saisie d'un nom d'utilisateur et d'un mot de passe, procédez comme suit pour les ajouter à Adobe Connect Enterprise Service :

a Ouvrez le panneau de configuration Services.

b Double-cliquez sur Adobe Connect Enterprise Service.

c Cliquez sur l'onglet Connexion.

d Cliquez sur la case d'option Ce compte et entrez le nom d'utilisateur du stockage partagé dans le champ. La syntaxe du nom d'utilisateur est [sous-domaine\]nom d'utilisateur.

e Entrez et confirmez le mot de passe du stockage partagé.

f Cliquez sur Appliquer, puis sur OK.

3 Procédez comme suit pour démarrer Acrobat Connect Pro :

a Dans le panneau de configuration Services, sélectionnez Flash Media Server (FMS) et cliquez ensuite sur Démarrer le service.

b Dans le panneau de configuration Services, sélectionnez Adobe Connect Enterprise Service et cliquez ensuite sur Démarrer le service.

4 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Configurer Connect Pro Server 7 pour ouvrir l'Assistant de la Console de gestion des applications, puis cliquez sur Suivant.

5 Dans l'écran Paramètres de la base de données, entrez les informations relatives à la base de données SQL Server, puis cliquez sur Suivant.

Si Acrobat Connect Pro est parvenu à se connecter à la base de données, un message de confirmation s'affiche et la fenêtre Paramètres de la base de données s'ouvre. Cliquez sur Suivant.

6 Dans l'écran Paramètres du serveur, procédez comme suit et cliquez sur Suivant :

a Entrez un nom de compte.

b Dans le champ Hôte Connect Pro, entrez le nom de l'ordinateur qui exécute l'équilibreur de charge.

c Entrez un numéro de port HTTP. Ce numéro peut être 80 ou 8080 selon l'équilibreur de charge utilisé.

d Entrez le nom externe du nœud de cluster.

e Entrez le nom de domaine de l'hôte SMTP et du système, ainsi que les adresses électroniques d'assistance.

f Si vous utilisez un stockage partagé, entrez le chemin d'accès au(x) volume(s) (séparez les volumes à l'aide d'un point-virgule).

g Entrez le pourcentage du serveur Acrobat Connect Pro que vous souhaitez utiliser comme cache local.

Remarque : *Le contenu est écrit dans le cache local et le volume de stockage partagé. Le contenu est conservé dans le cache local pendant 24 heures après sa dernière utilisation. Si le pourcentage de cache a été dépassé a l'issue de cette période, le contenu est vidé.*

7 Transférez le fichier de licence, puis cliquez sur Suivant.

8 Créez un administrateur et cliquez sur Terminer.

9 Répétez les étapes 1 à 8 pour chaque serveur du cluster.

10 Pour configurer l'équilibreur de charge, procédez comme suit :

a Configurez l'équilibreur de charge de sorte qu'il écoute sur le port 80.

b Ajoutez tous les noms des nœuds de cluster au fichier de configuration de l'équilibreur de charge.

Remarque : *Pour plus d'informations sur la configuration de l'équilibreur de charge, consultez la documentation du fabricant.*

11 Ouvrez un navigateur Web et entrez le nom de domaine de l'équilibreur de charge ; par exemple, http://connect.exemple.com.

Pour obtenir de l'aide sur le déploiement d'un cluster, contactez l'assistance technique d'Adobe à l'adresse www.adobe.com/go/connect_licensed_programs_fr.

Voir aussi

« Installation d'Acrobat Connect Pro Server 7 » à la page 13

« Configuration du stockage partagé » à la page 35

Vérification des opérations au sein d'un cluster

Si un ordinateur d'un cluster s'arrête, l'équilibreur de charge achemine toutes les requêtes HTTP vers un ordinateur opérationnel du cluster.

Lorsqu'une réunion commence, le serveur d'applications affecte un hôte principal et un hôte de secours à la salle de réunion en fonction de la charge rencontrée. Lorsque l'hôte principal s'arrête, les clients se reconnectent à l'hôte de secours.

Il est préférable de vérifier que le contenu chargé sur un serveur d'un cluster est bien répliqué sur les autres ordinateurs du cluster.

Dans les procédures suivantes, le cluster contient deux ordinateurs : Ordinateur1 et Ordinateur2.

Vérification de l'équilibrage de charge et du basculement de réunion

1 Démarrez Acrobat Connect Pro sur les deux ordinateurs.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Meeting Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

2 Connectez-vous à Connect Pro Central à partir de l'URL suivante :

http://*[nomhôte]*

Pour *nomhôte*, utilisez la valeur Hôte Connect Pro que vous avez saisie dans la Console de gestion des applications.

3 Sélectionnez l'onglet Réunions et cliquez sur le lien d'une réunion pour accéder à une salle de réunion.

Au besoin, créez une nouvelle réunion.

4 Arrêtez Acrobat Connect Pro sur Ordinateur2.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Meeting Server.

Si le basculement de réunion a bien fonctionné, le témoin de connexion de la réunion doit toujours être vert.

5 Dans Connect Pro Central, cliquez sur un onglet ou un lien quelconque.

Si l'équilibreur de charge fonctionne, vous devriez encore être en mesure d'envoyer des requêtes à Connect Pro Central et de recevoir des réponses.

Si le cluster contient plusieurs ordinateurs, testez cette procédure de démarrage-arrêt sur chacun d'eux.

Vérification de la réplication de contenu

1 Démarrez Acrobat Connect Pro sur Ordinateur1.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Meeting Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

2 Arrêtez Acrobat Connect Pro sur Ordinateur2.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter·Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter·Connect Pro Meeting Server.

3 Connectez-vous à Connect Pro Central à partir de l'URL suivante :

http://*[nomhôte]*

Pour *nomhôte*, entrez la valeur Hôte Connect Pro que vous avez saisie dans la Console de gestion des applications.

4 Transférez une image JPEG ou un autre contenu vers Acrobat Connect Pro sur Ordinateur1 :

- Pour ce faire, vous devez être membre du groupe Auteurs. (Si vous êtes Administrateur de compte, vous pouvez vous ajouter vous-même au groupe Auteurs dans Connect Pro Central.)
- Cliquez sur l'onglet Contenu.
- Cliquez sur Nouveau contenu et suivez les instructions qui s'affichent dans votre navigateur pour ajouter du contenu.

Lorsque le transfert de votre contenu test est terminé, la page Contenu utilisateurs s'ouvre et présente la liste des fichiers qui vous appartenaient.

5 Cliquez sur le lien pointant vers le contenu test que vous venez de transférer.

Une page d'informations sur les contenus contenant l'adresse URL qui permet d'afficher ce contenu apparaît.

6 Notez l'adresse URL pour l'utiliser à l'étape 10.

7 Cliquez sur l'URL.

8 Démarrez Ordinateur2, attendez que le démarrage d'Acrobat Connect Pro soit terminé, puis arrêtez Ordinateur1.

Si vous avez configuré un périphérique de stockage externe, il n'est pas nécessaire d'attendre que Ordinateur2 s'arrête ; le contenu requis est copié à partir du périphérique externe.

9 Fermez la fenêtre du navigateur dans laquelle le contenu test est affiché.

10 Ouvrez une nouvelle fenêtre de navigateur et entrez l'URL permettant d'afficher votre contenu test.

Si ce contenu apparaît, la réplication vers Ordinateur2 fonctionne. Une fenêtre vide ou un message d'erreur signifie que la réplication n'a pas fonctionné.

Déploiement d'Acrobat Connect Pro Edge Server 7

Procédure d'installation d'Acrobat Connect Pro Edge Server

1. Créez les régions des serveurs Edge.

Vous pouvez configurer des serveurs Edge ou des clusters de serveurs Edge dans différents sites, ou *régions*, afin d'affecter et d'équilibrer l'accès à Acrobat Connect Pro. Par exemple, vous pouvez configurer un serveur Edge à San Francisco pour les utilisateurs de la côte ouest des Etats-unis et un autre serveur Edge à Boston pour ceux de la côte est.

2. Installez Acrobat Connect Pro Edge Server.

Installez Acrobat Connect Pro Edge Server sur chaque ordinateur de chaque région. Par exemple, si vous avez un cluster de serveurs Edge dans une région, installez Acrobat Connect Pro Edge Server sur chaque ordinateur du cluster. Voir la section « Installation d'Acrobat Connect Pro Edge Server 7 » à la page 18.

3. Modifiez le serveur DNS de chaque région.

Mappez le nom de domaine pleinement qualifié (FQDN) du serveur Acrobat Connect Pro d'origine sur l'adresse IP statique du serveur Acrobat Connect Pro Edge de chaque région. Voir la section « Déploiement d'Acrobat Connect Pro Edge Server 7 » à la page 25.

4. Configurez le serveur Edge.

Vous devez ajouter les paramètres de configuration dans le fichier custom.ini de chaque serveur Acrobat Connect Pro Edge. Voir la section « Déploiement d'Acrobat Connect Pro Edge Server 7 » à la page 25.

5. Configurez le serveur d'origine.

Vous devez ajouter les paramètres de configuration dans le fichier custom.ini de chaque serveur Acrobat Connect Pro. Vous devez également définir le Nom externe du serveur Edge dans la Console de gestion des applications du serveur d'origine. Voir la section « Déploiement d'Acrobat Connect Pro Edge Server 7 » à la page 25.

6. Configurez l'équilibreur de charge.

Si vous configurez plusieurs serveurs Edge dans une région, vous devez utiliser un équilibreur pour équilibrer la charge entre les serveurs Edge et les configurer pour qu'ils écoutent le port 80. Les serveurs Edge écoutent le port 8080. Pour plus d'informations, consultez la documentation fournie par le fabricant de l'équilibreur de charge.

Déploiement d'Acrobat Connect Pro Edge Server

Avant de déployer des serveurs Edge, il est préférable de vérifier le bon fonctionnement d'Acrobat Connect Pro et de toute fonctionnalité supplémentaire (par exemple : SSL, une intégration de service d'annuaire, l'authentification unique, un stockage de contenu partagé, etc.).

1 Dans votre serveur DNS, mappez le nom de domaine pleinement qualifié (FQDN) du serveur d'origine avec l'adresse IP statique du serveur Edge. Si vous installez des serveurs Edge dans plusieurs régions, répétez cette étape pour chacune d'elles.

Remarque : *Vous pouvez également utiliser un fichier d'hôtes. Dans ce cas, chaque client doit disposer d'un fichier d'hôtes dont l'adresse IP statique du serveur Edge pointe sur le nom de domaine pleinement qualifié du serveur d'origine.*

2 Dans Acrobat Connect Pro Edge Server, ouvrez le fichier *[rép_install_racine]* \edgeserver\win32\conf\HttpCache.xml et remplacez le nom de l'ordinateur indiqué dans la balise HostName par le nom de domaine pleinement qualifié (FQDN) du serveur Edge ; edge1.exemple.com, par exemple.

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

3 Dans Acrobat Connect Pro Edge Server, ouvrez le fichier *[rép_install_racine]* \edgeserver\conf\config.ini dans un éditeur de texte et entrez les paramètres et valeurs suivants :

FCS_EDGE_HOST Nom de domaine pleinement qualifié (FQDN) du serveur Edge, par exemple `FCS_EDGE_HOST=edge1.votresociété.com`.

FCS_EDGE_REGISTER_HOST Nom de domaine pleinement qualifié (FQDN) du serveur d'origine Acrobat Connect Pro ; par exemple, `FCS_EDGE_REGISTER_HOST=connect.votresociété.com`.

FCS_EDGE_CLUSTER_ID Nom du cluster. Chaque cluster de serveurs Edge doit disposer d'un ID unique. Chaque ordinateur du cluster doit avoir le même identifiant. Le format recommandé est *`nomsociété-nomcluster`* ; par exemple, `FCS_EDGE_CLUSTER_ID=votresociété-us`.

Remarque : *Vous devez configurer ce paramètre même si vous ne déployez qu'un seul serveur Acrobat Connect Pro Edge.*

FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT Adresse IP ou nom de domaine et numéro de port de l'ordinateur sur lequel est installé Acrobat Connect Pro ; par exemple, `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.votresociete.com:80`. Acrobat Connect Pro Edge Server se connecte au serveur d'origine d'Acrobat Connect Pro à cet emplacement.

FCS_EDGE_PASSWORD (Facultatif) Mot de passe du serveur Edge. Si vous définissez une valeur pour ce paramètre, vous devez définir la même valeur pour chaque serveur Edge et pour le serveur d'origine.

FCS_EDGE_EXPIRY_TIME (Facultatif) Nombre de millisecondes accordées au serveur Edge pour s'enregistrer sur le serveur d'origine avant son expiration dans le cluster et le basculement du système sur un autre serveur Edge. Commencez par la valeur par défaut `FCS_EDGE_EXPIRY_TIME=60000`.

FCS_EDGE_REG_INTERVAL (Facultatif) Intervalle, en millisecondes, durant lequel le serveur Edge tente de s'enregistrer auprès du serveur d'origine. Ce paramètre détermine la fréquence à laquelle le serveur Edge se met à la disposition du serveur d'origine. Commencez par la valeur par défaut `FCS_EDGE_REG_INTERVAL=30000`.

DEFAULT_FCS_HOSTPORT (Facultatif) Pour configurer les ports du serveur Edge, ajoutez la ligne suivante :
`DEFAULT_FCS_HOSTPORT=:1935,80,-443`

Le signe moins (-) placé devant 443 désigne le port 443 comme port sécurisé recevant uniquement des connexions RTMPS. Si vous tentez une demande de connexion RTMPS au port 1935 ou 80, la connexion échouera. De même, une demande de connexion RTMP non sécurisée envoyée au port 443 échoue également.

Remarque : *Si votre serveur Edge utilise un accélérateur matériel externe, il n'est pas nécessaire de configurer le port 443 comme port sécurisé.*

Vous trouverez, ci-dessous, des exemples de valeurs pour le fichier 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 Redémarrez le serveur Edge.

5 Sur le serveur d'origine Acrobat Connect Pro, ouvrez le fichier *[rép_install_racine]* \custom.ini dans un éditeur de texte et mappez la valeur du paramètre `FCS_EDGE_CLUSTER_ID` sur un ID de région ; la syntaxe est `Edge.`*`FCS_EDGE_CLUSTER_ID = zone-id`*. Même si vous ne déployez qu'un seul serveur Edge, vous devez mapper l'identifiant du cluster sur un identifiant de région.

Chaque cluster de serveurs Edge doit disposer d'un identifiant de région. L'identifiant de région peut être tout entier positif supérieur à 0. Par exemple, vous pouvez avoir trois clusters mappés sur les régions 1 à 3 :

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

Ce qui suit est un exemple de fichier custom.ini pour le serveur d'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
```

Remarque : *Si vous définissez un paramètre* `FCS_EDGE_PASSWORD` *dans le fichier config.ini du serveur Edge, définissez le même mot de passe dans le fichier custom.ini du serveur d'origine.*

6 Redémarrez le serveur d'origine.

7 Sur le serveur d'origine, ouvrez la console de gestion des applications (Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Configurer Connect Pro Server 7). Ouvrez l'onglet Paramètres de l'application, puis choisissez Paramètres du serveur et, dans la section Mappages de l'hôte, entrez le Nom externe du serveur Edge. Le nom externe doit être identique à la valeur définie pour le paramètre `FCS_EDGE_HOST` sur le serveur Edge.

8 Sur le serveur d'origine, configurez le pare-feu Windows de sorte que les serveurs Edge puissent accéder au port 8506.

9 Répétez les étapes 2 à 4 pour chaque serveur Edge de chaque région.

10 Répétez les étapes 5 à 7 pour chaque serveur d'origine de chaque région.

Pour obtenir de l'aide sur le déploiement des serveurs Edge, contactez l'assistance technique d'Adobe à l'adresse www.adobe.com/go/connect_licensed_programs_fr..

Voir aussi

« Choix du déploiement d'Acrobat Connect Pro Edge Server » à la page 11

Intégration dans un service d'annuaire

Présentation de l'intégration du service d'annuaire

Vous pouvez intégrer Acrobat Connect Pro à un service d'annuaire afin d'authentifier les utilisateurs par rapport à l'annuaire LDAP et d'éviter d'ajouter manuellement des groupes et des utilisateurs individuels. Les comptes d'utilisateur sont créés automatiquement dans Acrobat Connect Pro par le biais de synchronisations manuelles ou planifiées avec l'annuaire de la société.

Pour être intégré à Acrobat Connect Pro, votre serveur d'annuaire doit utiliser le protocole LDAP (Lightweight Directory Access Protocol) ou LDAPS (secure Lightweight Directory Access Protocol). Le protocole LDAP est un protocole Internet client-serveur qui permet de rechercher les coordonnées des utilisateurs dans un serveur d'annuaire compatible LDAP.

Acrobat Connect Pro se connecte à un annuaire LDAP en tant que client LDAP. Il importe les utilisateurs et les groupes et synchronise les informations de ceux-ci avec un annuaire LDAP. Vous pouvez également configurer Acrobat Connect Pro pour authentifier les utilisateurs par rapport à l'annuaire LDAP.

Tout service d'annuaire compatible LDAP peut s'intégrer à Acrobat Connect Pro. Vous trouverez la liste des annuaires LDAP certifiés à l'adresse www.adobe.com/go/connect_sysreqs_fr.

Présentation de la structure d'annuaire LDAP

Les annuaires LDAP organisent les informations selon la norme X.500.

Dans un annuaire LDAP, un utilisateur ou un groupe est appelé une *entrée*. Une entrée est un ensemble d'attributs. Un attribut se compose d'un type et d'une ou plusieurs valeurs. Les types utilisent des chaînes mnémoniques comme `ou` pour une entité organisationnelle ou `cn` pour un nom commun. Les valeurs des attributs sont des informations, telles qu'un numéro de téléphone, une adresse de messagerie et une photo. Pour connaître la structure d'annuaire LDAP de votre société, contactez votre administrateur LDAP.

Chaque entrée présente un *nom unique* qui décrit le chemin de l'entrée par l'intermédiaire d'une structure en arborescence allant de l'entrée jusqu'à la racine. Le nom unique d'une entrée dans l'annuaire LDAP est une concaténation du nom de l'entrée (appelé *nom unique relatif*, RDN) et des noms de ses entrées parentes dans la structure d'arborescence.

L'arborescence peut refléter des emplacements géographiques ou les limites des services d'une société. Par exemple, si Alicia Solis est un utilisateur du service QA d'Acme, Inc. en France, le nom unique de cet utilisateur peut être :

cn=Alicia Solis, ou=QA, c=France, dc=Acme, dc=com

Importation des branches d'annuaire

Lors de l'importation d'utilisateurs et de groupes depuis un annuaire LDAP vers Acrobat Connect Pro, vous indiquez le chemin vers une section de l'arborescence LDAP à l'aide du nom unique de cette section. L'opération spécifie l'étendue de la recherche. Par exemple, vous pouvez n'importer que les utilisateurs d'un groupe particulier de votre société. Pour ce faire, vous devez savoir où sont situées les entrées de ce groupe dans l'arborescence de l'annuaire.

Une technique courante consiste à utiliser le domaine Internet de la société en tant que racine de l'arborescence. Par exemple, Acme, Inc. pourrait utiliser `dc=com` pour spécifier l'élément racine de l'arborescence. Un nom unique qui spécifie le bureau d'Acme, Inc. à Singapour pourrait être `ou=Singapour` , `ou=Marketing` , `ou=Employés` , `dc=Acme` , `dc=com`. (Dans cet exemple, `ou` est l'abréviation de « entité organisationnelle » et `dc` l'abréviation de « composant de domaine ».)

Remarque : *Tous les annuaires LDAP n'ont pas de racine unique. Dans ce cas, vous pouvez importer des branches distinctes.*

Importation d'utilisateurs et de groupes

Il existe deux moyens de structurer les entrées d'utilisateurs et de groupes dans un annuaire LDAP : sous le même nœud d'une branche ou sous des branches différentes.

Si les utilisateurs et les groupes sont sous le même nœud d'une branche LDAP, les paramètres d'utilisateurs et de groupes liés à l'importation des entrées contiennent le même nom unique de branche. Cela signifie que vous devez utiliser un filtre pour ne sélectionner que les utilisateurs lorsque vous importez des utilisateurs, et un filtre pour ne sélectionner que les groupes lorsque vous importez des groupes.

Si les utilisateurs et les groupes sont placés sous des branches différentes de l'arborescence, utilisez un nom unique de branche qui sélectionne la branche d'utilisateurs lorsque vous importez les utilisateurs et la branche de groupes lorsque vous importez les groupes.

Vous pouvez également importer des sous-branches pour importer les utilisateurs de toutes les branches au-dessous d'un certain niveau. Par exemple, pour importer tous les employés du service commercial, vous pouvez utiliser le nom unique de la branche suivante :

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

Le personnel commercial peut, cependant, être stocké dans des sous-branches. Dans ce cas, dans l'écran Mappage du profil utilisateur, définissez le paramètre Recherche de sous-arborescence sur `true` pour vous assurer que les utilisateurs sont importés depuis les sous-branches situées sous ce niveau dans l'arborescence.

Filtrage des entrées sélectionnées

Un filtre précise la condition que doit remplir une entrée pour être sélectionnée. Les sélections d'entrée au sein d'une partie de l'arborescence sont ainsi limitées. Par exemple, si le filtre spécifie `(objectClass=organizationalPerson)` , seules les entrées dont l'attribut est `organizationalPerson` sont sélectionnées pour l'importation.

Remarque : *L'attribut* `objectClass` *doit être présent dans toutes les entrées d'un annuaire LDAP.*

Utilisateurs et groupes internes et externes

Les utilisateurs et les groupes créés directement dans Acrobat Connect Pro et non importés depuis un annuaire LDAP sont appelés utilisateurs et groupes *internes*. Les utilisateurs et les groupes importés dans la base de données Acrobat Connect Pro depuis un annuaire LDAP sont appelés utilisateurs et groupes *externes*.

Pour que les groupes importés restent synchronisés avec l'annuaire LDAP externe, vous ne pouvez pas ajouter d'utilisateurs et de groupes internes dans les groupes externes. Vous pouvez, en revanche, ajouter des utilisateurs et des groupes externes dans les groupes internes.

Si la valeur de l'identifiant ou du nom d'une entrée de groupe ou d'utilisateur importée correspond à celle d'un groupe ou d'un utilisateur interne existant, la synchronisation des annuaires transforme le groupe ou l'utilisateur importé d'interne en externe et place un avertissement dans le journal de synchronisation.

Intégration d'Acrobat Connect Pro à un annuaire LDAP

L'intégration du service d'annuaire a lieu dans l'onglet Paramètres du service d'annuaire de la Console de gestion des applications. Utilisez un compte d'administrateur.

Vous pouvez configurer un serveur d'annuaire pour l'authentification des utilisateurs et la synchronisation LDAP. La configuration peut pointer vers une ou plusieurs branches du service d'annuaire.

1. Ouvrez la Console de gestion des applications.

Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Configurer Connect Pro Server 7.

2. Entrez les paramètres de connexion du serveur LDAP.

Ouvrez l'onglet Paramètres du service d'annuaire. Entrez des valeurs dans l'écran Paramètres LDAP > Paramètres de connexion, puis cliquez sur Enregistrer.

Lorsque vous cliquez sur Enregistrer, Acrobat Connect Pro teste la connexion LDAP. Si le test échoue, le message suivant s'affiche : « Vos paramètres ont bien été enregistrés, mais la connectivité LDAP n'a pu être vérifiée. » Vérifiez l'URL et le port LDAP.

Champ	Valeur par défaut	Description
Adresse URL du serveur LDAP	Aucune valeur par défaut.	La forme habituelle est `ldap://` *`[nomduserveur:numérodeport]`* . Si votre société utilise un serveur LDAP sécurisé, utilisez `ldaps://`. Si vous ne spécifiez pas de port, Acrobat Connect Pro utilise le port LDAP standard (389) ou le port LDAPS (636). Le protocole LDAPS requiert des certificats SSL. Si vous configurez Acrobat Connect Pro pour travailler dans une forêt Microsoft Active Directory où le catalogue global est activé, utilisez ce dernier (port standard : 3268).
Méthode d'authentification de connexion LDAP	Aucune valeur par défaut.	Mécanisme d'authentification des informations d'identification de connexion (nom d'utilisateur LDAP, mot de passe LDAP) du compte de service LDAP pour Acrobat Connect Pro (droits d'administrateur). **Simple** (authentification standard - recommandée). **Anonyme** (sans mot de passe - votre serveur LDAP doit être configuré pour autoriser la connexion anonyme). **Résumé MD5** (configurez votre serveur LDAP pour autoriser l'authentification résumée).
Nom d'utilisateur de connexion LDAP	Aucune valeur par défaut.	Identifiant de connexion d'administrateur sur le serveur LDAP.
Mot de passe de connexion LDAP	Aucune valeur par défaut.	Mot de passe d'administrateur sur le serveur LDAP.
Expiration de la requête LDAP	Aucune valeur par défaut.	Délai pouvant s'écouler avant que la requête ne soit annulée, en secondes. Si vous ne renseignez pas ce champ, il n'y a pas de délai. Définissez cette valeur sur 120.
Limite de taille de la page de requête d'entrée LDAP	Aucune valeur par défaut.	Taille de la page de résultats renvoyée par le serveur LDAP. Si ce champ est vide ou égal à 0, aucune taille de page n'est utilisée. Utilisez ce champ lorsqu'une taille de résultats maximale a été configurée pour les serveurs LDAP. Définissez une taille de page inférieure à la taille de résultats maximale de sorte que l'ensemble des résultats soit récupéré sur le serveur en plusieurs pages. Ainsi, si vous tentez d'intégrer un important annuaire LDAP qui ne peut afficher que 1 000 utilisateurs alors qu'il y en a 2 000 à importer, l'intégration échoue. Si vous définissez la taille de la page de requête sur 100, les résultats sont renvoyés sur 20 pages et tous les utilisateurs sont importés.

Voici un exemple de syntaxe LDAP pour les paramètres de connexion :

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

3. Mappez les profils utilisateurs de l'annuaire LDAP avec Acrobat Connect Pro.

Ouvrez l'onglet Mappage du profil utilisateur, entrez les valeurs, puis cliquez sur Enregistrer.

Champ	Valeur par défaut	Description
Connexion	Aucune valeur par défaut.	Attribut de connexion dans le service d'annuaire.
Prénom	Aucune valeur par défaut.	Attribut du prénom dans le service d'annuaire.
Nom	Aucune valeur par défaut.	Attribut du nom dans le service d'annuaire.
Adresse de messagerie	Aucune valeur par défaut.	Attribut d'adresse de messagerie dans le service d'annuaire.

Si vous avez défini des champs personnalisés, ils apparaissent dans la fenêtre Mappage du profil utilisateur. Cet exemple mappe un profil d'utilisateur Acrobat Connect Pro sur un profil d'utilisateur LDAP Active Directory. Connexion réseau est un champ personnalisé.

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

4. (Facultatif) Ajoutez une branche d'utilisateur.

Cliquez sur Ajouter pour ajouter des informations sur un utilisateur d'une branche donnée de votre société. Entrez les valeurs dans les champs Branche et Filtre, puis cliquez sur Enregistrer.

Pour importer des utilisateurs à partir de sous-branches, sélectionnez True dans le menu Recherche de sous-arborescence, sinon sélectionnez False.

Pour plus d'informations, consultez la section « Présentation de la structure d'annuaire LDAP » à la page 28.

Champ	Valeur par défaut	Attribut/notes LDAP
Nom unique de la branche	Aucune valeur par défaut.	Nom unique du nœud racine de la branche. Un lien vers la branche sélectionnée s'affiche.
Filtre	Aucune valeur par défaut.	Chaîne du filtre de requête.
Recherche de sous-arborescence	True	True ou False. La valeur True déclenche une recherche récursive dans toutes les sous-arborescences de la branche.

5. Mappez les profils de groupes de l'annuaire LDAP avec Acrobat Connect Pro.

Ouvrez l'onglet Mappage du profil de groupe, entrez des valeurs, puis cliquez sur Enregistrer.

Remarque : *Les profils de groupes d'Acrobat Connect Pro ne prennent pas en charge les champs personnalisés.*

Champ	Valeur par défaut	Attribut/notes LDAP
Nom du groupe	Aucune valeur par défaut.	Attribut du nom du groupe dans le service d'annuaire.
Membre du groupe	Aucune valeur par défaut.	Attribut du membre du groupe dans le service d'annuaire.

Voici un mappage entre les attributs d'entrée de groupes LDAP et un profil de groupe Acrobat Connect Pro :

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

6. (Facultatif) Ajoutez une branche de groupe.

Cliquez sur Ajouter pour ajouter des informations sur un groupe d'une branche donnée de votre société. Entrez les valeurs dans les champs Branche et Filtre, puis cliquez sur Enregistrer.

Pour importer des groupes à partir de sous-branches, sélectionnez True dans le menu Recherche de sous-arborescence, sinon sélectionnez False.

Pour plus d'informations, consultez la section « Présentation de la structure d'annuaire LDAP » à la page 28.

Champ	Valeur par défaut	Attribut/notes LDAP
Nom unique de la branche	Aucune valeur par défaut.	Nom unique du nœud racine de la branche. Chaque branche de la société possède son propre attribut de nom unique LDAP. Un lien vers la branche sélectionnée s'affiche.
Filtre	Aucune valeur par défaut.	Chaîne du filtre de requête.
Recherche de sous-arborescence	True	Valeur booléenne `true` ou `false`. La valeur `true` lance une recherche récursive dans toutes les sous-arborescences de la branche.

L'exemple suivant indique une syntaxe LDAP illustrant comment ajouter une branche de la société et définir ses groupes :

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

7. Entrez les paramètres d'authentification.

Sélectionnez l'onglet Paramètres d'authentification. Pour authentifier les utilisateurs Acrobat Connect Pro à l'aide du service d'annuaire de votre société, sélectionnez « Activer l'authentification de l'annuaire LDAP ». Si vous ne sélectionnez pas cette option, Acrobat Connect Pro utilise l'authentification native (informations de connexion de l'utilisateur stockées dans la base de données Acrobat Connect Pro).

Si vous activez la case à cocher « Activer la reprise de Connect Pro en cas d'échec d'authentification de l'annuaire LDAP », Acrobat Connect Pro utilise l'authentification native.

Remarque : *Cette option peut être utile en cas de panne de connexion LDAP momentanée sur le réseau. Il se peut, toutefois, que les informations de connexion LDAP soient différentes des celles de la base de données Acrobat Connect Pro.*

Activez la case à cocher « Créer un compte d'utilisateur Connect Pro en cas d'authentification réussie à l'annuaire LDAP » pour permettre aux nouveaux utilisateurs d'accéder au serveur Acrobat Connect Pro si l'authentification LDAP a réussi. Si un utilisateur de votre service d'annuaire est autorisé à utiliser Acrobat Connect Pro, laissez cette option cochée et sélectionnez « Interne » comme type de compte d'utilisateur. Pour plus d'informations, consultez la section « Utilisateurs et groupes internes et externes » à la page 29.

Activez la case à cocher « Activer l'inscription de groupe lors de la connexion initiale uniquement » pour créer un identifiant dans Acrobat Connect Pro et placer les utilisateurs dans des groupes spécifiques lorsqu'ils se connectent à Acrobat Connect Pro pour la première fois. Entrez les groupes dans la zone Noms des groupes.

8. Planifiez la synchronisation.

Ouvrez l'onglet Paramètres de synchronisation. Dans l'écran Paramètres de planification, cochez la case Activer la synchronisation planifiée pour programmer des synchronisations régulières, quotidiennes, hebdomadaires ou mensuelles, à une heure donnée. Pour plus d'informations, consultez la section « Recommandations relatives à la synchronisation » à la page 33.

Vous pouvez également effectuer une synchronisation manuelle dans la fenêtre Actions de synchronisation.

9. Définissez une stratégie de mot de passe et une stratégie de suppression.

Ouvrez l'onglet Paramètres de la stratégie, choisissez une stratégie de configuration des mots de passe et une stratégie de suppression, puis cliquez sur Enregistrer. Pour plus d'informations sur la stratégie de mot de passe, consultez la section « Gestion des mots de passe » à la page 33.

Remarque : *Si vous sélectionnez l'option Supprimer des utilisateurs et des groupes, durant la synchronisation, tous les utilisateurs externes qui ont été supprimés du serveur LDAP sont également supprimés du serveur Acrobat Connect Pro.*

10. Consultez un aperçu de la synchronisation.

Ouvrez l'onglet Synchroniser les actions. Dans la section Aperçu de la synchronisation des annuaires, cliquez sur Aperçu. Pour plus d'informations, consultez la section « Recommandations relatives à la synchronisation » à la page 33.

Gestion des mots de passe

Si vous n'activez pas l'authentification LDAP, vous devez choisir comment Acrobat Connect Pro authentifie les utilisateurs.

Lorsqu'Acrobat Connect Pro importe les informations d'utilisateurs à partir d'un annuaire externe, il n'importe pas les mots de passe réseau. Vous devez donc implémenter une autre méthode de gestion des mots de passe pour les utilisateurs importés dans l'annuaire Acrobat Connect Pro.

Notification des utilisateurs pour définir leur mot de passe

Dans l'écran Paramètres de la stratégie de l'onglet Paramètres de synchronisation, vous pouvez opter pour l'envoi d'un message électronique aux utilisateurs importés avec un lien qui leur permettra de définir leur mot de passe.

Définition du mot de passe sur un attribut LDAP

Vous pouvez choisir de définir le premier mot de passe d'un utilisateur importé sur la valeur d'un attribut d'entrée d'annuaire de cet utilisateur. Par exemple, si l'annuaire LDAP contient un champ de numéro ID d'employé, vous pouvez faire de cette valeur le mot de passe initial des utilisateurs. Lorsque les utilisateurs se connectent à l'aide de ce mot de passe, ils peuvent alors le modifier.

Recommandations relatives à la synchronisation

En tant qu'administrateur, deux méthodes vous permettent de synchroniser Acrobat Connect Pro avec un annuaire LDAP externe :

- Vous pouvez planifier la synchronisation pour qu'elle ait lieu à intervalles réguliers.
- Vous pouvez effectuer une synchronisation manuelle qui synchronise immédiatement l'annuaire d'Acrobat Connect Pro et l'annuaire LDAP de la société.

Avant d'importer les utilisateurs et les groupes dans une première synchronisation, il est préférable de vérifier les paramètres de connexion à l'aide d'un navigateur LDAP. Les navigateurs suivants sont disponibles en ligne : Navigateur/Editeur LDAP et Administrateur LDAP.

Important : *Pendant la synchronisation, ne relancez pas votre serveur LDAP et n'exécutez aucune tâche parallèle. En effet, cela entraînerait la suppression d'utilisateurs ou de groupes dans Acrobat Connect Pro.*

Synchronisations planifiées

Les synchronisations planifiées sont conseillées car elles permettent de s'assurer qu'Acrobat Connect Pro dispose d'une image à jour des utilisateurs et des groupes importés depuis l'annuaire LDAP de la société.

Si vous importez un grand nombre d'utilisateurs et de groupes, il se peut que la synchronisation initiale exploite une grande quantité de ressources. Dans ce cas, il est préférable de planifier cette première synchronisation en dehors des heures de pointe, tard dans la nuit, par exemple. (Vous pouvez également effectuer la première synchronisation manuellement.)

Pour configurer une synchronisation planifiée, utilisez la fenêtre Paramètres de synchronisation > Paramètres de planification de la Console de gestion des applications.

Lorsqu'une synchronisation a lieu, Acrobat Connect Pro compare les entrées de l'annuaire LDAP à celles de son annuaire et importe uniquement celles comportant au moins un champ modifié.

Aperçu de la synchronisation

Avant l'importation d'utilisateurs et de groupes dans la première synchronisation, Adobe vous recommande de tester vos mappages en affichant un aperçu de la synchronisation. Dans un aperçu, les utilisateurs et groupes ne sont pas à proprement parler importés, mais les erreurs sont enregistrées dans un journal. Vous pouvez alors examiner ces erreurs afin de diagnostiquer les problèmes éventuels.

Pour accéder aux journaux de synchronisation, utilisez la fenêtre Journaux de synchronisation. Chaque ligne du journal présente un événement de synchronisation et la synchronisation produit au moins un événement par utilisateur ou groupe traité. Si des avertissements ou des erreurs sont générés pendant l'aperçu, ils sont inscrits dans une liste dans un second journal d'avertissements.

Valeurs des fichiers journaux

Les journaux de synchronisation stockent les valeurs dans un format séparé par des virgules. Dans les tableaux suivants, le terme *principal* (mandant) fait référence aux entrées d'utilisateur et de groupe. Les valeurs suivantes sont incluses dans les entrées des journaux :

Champ	Description
Date	Valeur de date et d'heure, cette dernière allant jusqu'aux millisecondes. Le format est *aaaaMMjj'T'HHmmss.SSS*.
ID mandant	Nom de connexion ou nom du groupe.
Type de mandant	Caractère unique : U pour utilisateur, G pour groupe.
Evénement	L'action entreprise ou la condition rencontrée.
Détail	Informations détaillées sur l'événement.

Le tableau suivant présente les différents types d'événements pouvant apparaître dans les fichiers journaux de synchronisation.

Evénement	Description	Détail
add	Le mandant a été ajouté dans Acrobat Connect Pro.	Paquet XML abrégé décrivant les champs mis à jour à l'aide d'une série de paires de balises au format `<fieldname>valeur</fieldname>` (par exemple, `<first-name>Joe</first-name>`). Le nœud parent et les champs non mis à jour sont omis.
update	Le mandant est un utilisateur externe et certains champs ont été mis à jour.	

update-members	Le mandant est un groupe externe et des mandants ont été ajoutés ou supprimés dans le groupe.	Paquet XML abrégé décrivant les membres supprimés et ajoutés. Le nœud parent est omis :
		`<add>ID list</add>`
		`<remove>ID list</remove>`
		La liste d'ID est une série de paquets `<id>principal ID</id>` où `principal ID` est un ID répertorié dans la colonne ID mandant, tel qu'un nom d'utilisateur ou un nom de groupe. S'il n'existe aucun membre d'une liste d'ID, le nœud parent est généré comme `<add/>` ou `<remove/>`.

delete	Le mandant a été supprimé d'Acrobat Connect Pro.	
up-to-date	Le mandant est un mandant externe dans Acrobat Connect Pro et est déjà synchronisé avec l'annuaire externe. Aucun changement n'a été effectué.	Un utilisateur ou un groupe créé dans Acrobat Connect Pro est considéré comme un mandant interne. Un utilisateur ou un groupe créé par le processus de synchronisation est considéré comme un mandant externe.
make-external	Le mandant est un mandant interne d'Acrobat Connect Pro et a été converti en mandant externe.	Cet événement permet à la synchronisation de modifier ou de supprimer le mandant et est généralement suivi d'un autre événement qui fait l'un ou l'autre. Cet événement est consigné dans le journal d'avertissement.
warning	Un événement de niveau avertissement est survenu.	Message d'avertissement.
error	Une erreur s'est produite.	Message d'exception Java.

A propos du protocole LDAPS

Acrobat Connect Pro prend nativement en charge le protocole *LDAPS* (protocole LDAP sécurisé). Le serveur d'annuaire LDAP doit fournir une connexion SSL. Pour établir une connexion sécurisée à un serveur d'annuaire LDAP, utilisez le protocole LDAPS dans l'URL de connexion, comme dans l'exemple suivant : `ldaps://` *`ServeurAnnuaireExemple`* `:` *`NumeroPort`*.

Configuration du stockage partagé

A propos du stockage partagé

Vous pouvez utiliser la Console de gestion des applications pour configurer Acrobat Connect Pro afin qu'il gère le stockage de contenu avec des périphériques NAS et SAN. Le terme « contenu » désigne tout fichier publié dans Acrobat Connect Pro, tel que des cours, des fichiers SWF, PPT ou PDF et des enregistrements archivés.

Configurations de stockage partagé possibles :

- Le contenu est copié sur les principaux périphériques de stockage externes et extrait vers le dossier de contenu de chaque serveur Acrobat Connect Pro lorsque cela s'avère nécessaire. L'ancien contenu est purgé du dossier de contenu de chaque serveur afin de libérer de la place pour le nouveau contenu lorsque cela s'avère nécessaire. Cette

configuration libère des ressources sur le serveur d'applications, ce qui se révèle particulièrement utile dans le cas d'un cluster volumineux. (Entrez une valeur dans les champs Stockage partagé et Taille du contenu mis en cache.)

- Le contenu est copié sur tous les serveurs et sur le principal périphérique de stockage externe. Cette configuration est recommandée pour les petits clusters, sauf si vous disposez d'une grande quantité de contenu dont l'accès est aléatoire. (Entrez une valeur dans le champ Stockage partagé ; ne renseignez pas le champ Taille du contenu mis en cache.)

Remarque : *Si vous utilisez un cluster Acrobat Connect Pro et que vous ne configurez pas les périphériques de stockage partagé, le cluster fonctionne en mode miroir complet (le contenu publié dans Acrobat Connect Pro est copié sur tous les serveurs) et le contenu n'est jamais supprimé automatiquement d'aucun serveur.*

Configuration du stockage partagé

Si vous configurez un stockage partagé pour un seul serveur Acrobat Connect Pro, suivez les instructions de la première tâche. Si vous configurez un stockage partagé pour un cluster, suivez les instructions de la première tâche pour un ordinateur du cluster, puis les instructions de la seconde tâche pour tous ses autres ordinateurs.

Voir aussi

« Périphériques de stockage de contenu pris en charge » à la page 3

« Déploiement d'un cluster de serveurs Acrobat Connect Pro » à la page 22

Configuration du stockage partagé

Avant de commencer, Acrobat Connect Pro doit être configuré sans stockage partagé et s'exécuter sur un serveur.

1 Configurez un volume partagé sur un périphérique de stockage externe.

Si le volume partagé présente un nom d'utilisateur et un mot de passe, tous les volumes partagés doivent utiliser le même nom d'utilisateur et le même mot de passe.

2 (Facultatif) Si vous actualisez un serveur Acrobat Connect Pro existant afin d'utiliser des volumes de stockage partagés, vous devez copier le contenu de l'un de ces serveurs sur le volume partagé.

a Arrêtez le serveur (Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server et Arrêter Connect Pro Meeting Server).

b Copiez le dossier *[rép_install_racine]*\content\7 dans le volume partagé créé à l'étape 1.

Il se peut que certains ordinateurs d'un cluster présentent du contenu supplémentaire. Acrobat Connect Pro ne peut pas utiliser ces fichiers, mais si vous souhaitez les copier sur le volume partagé pour les archiver, vous pouvez rédiger et exécuter un script qui compare le contenu de chaque ordinateur avec celui du volume partagé.

c Démarrez Acrobat Connect Pro (Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Meeting Server et Démarrer Connect Pro Central Application Server).

3 Dans Acrobat Connect Pro, choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services, sélectionnez Adobe Connect Enterprise Service, puis procédez comme suit :

a Cliquez avec le bouton droit et sélectionnez Propriétés.

b Sélectionnez l'onglet Connexion.

c Sélectionnez Ce compte et, si le volume partagé possède un nom d'utilisateur et un mot de passe, entrez-les, puis cliquez sur Appliquer.

4 Redémarrez Acrobat Connect Pro (serveur d'applications uniquement).

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

5 Ouvrez la Console de gestion des applications (Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Configurer Connect Pro Server 7).

6 Dans l'onglet Paramètres de l'application, ouvrez l'onglet Paramètres du serveur, localisez la section Paramètres du stockage partagé et entrez un chemin de dossier dans le champ Stockage partagé (par exemple, **\\stockage**).

Si le périphérique de stockage principal est plein, vous pouvez ajouter un autre périphérique à l'emplacement principal. Séparez les chemins par des points-virgules (;) : **\\nouveau-stockage;\\stockage**.

Remarque : *L'écriture (copie dans le dossier de stockage) s'effectue uniquement dans le premier dossier. La lecture (copie depuis le dossier de stockage) s'effectue en séquence, en commençant par le premier dossier jusqu'à ce que le fichier soit localisé.*

7 (Facultatif) Pour configurer le dossier de contenu sur Acrobat Connect Pro pour faire office de cache (des ressources sont supprimées automatiquement lorsque de l'espace est nécessaire et rétablies sur demande), entrez une valeur dans la zone Taille du contenu mis en cache.

La taille du cache du contenu correspond à un pourcentage de l'espace disque devant être utilisé comme cache. Adobe recommande de définir une valeur comprise entre 15 et 50, car le cache peut grossir bien au-delà de la taille définie. Le cache n'est purgé que lorsque le contenu affiché a expiré (24 heures après sa dernière consultation).

8 Cliquez sur Enregistrer et fermez la Console de gestion des applications.

9 Redémarrez Acrobat Connect Pro (serveur d'applications uniquement).

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

Configuration du stockage partagé pour d'autres serveurs d'un cluster

1 Installez Acrobat Connect Pro sans le démarrer. Si Acrobat Connect Pro est installé et déjà en cours d'exécution, arrêtez-le.

2 Dans Acrobat Connect Pro, choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services, sélectionnez Adobe Connect Enterprise Service, puis procédez comme suit :

a Cliquez avec le bouton droit et sélectionnez Propriétés.

b Sélectionnez l'onglet Connexion.

c Sélectionnez Ce compte et, si le volume partagé possède un nom d'utilisateur et un mot de passe, entrez-les, puis cliquez sur Appliquer.

3 Démarrez Acrobat Connect Pro.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Server 7 > Démarrer Adobe Connect Meeting Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

4 (Facultatif) Si vous installez Acrobat Connect Pro pour la première fois, suivez les étapes indiquées à la section « Déploiement d'un cluster de serveurs Acrobat Connect Pro » à la page 22.

5 Cliquez sur Enregistrer et fermez la Console de gestion des applications.

Configuration des paramètres de notification de compte

Définition de l'heure d'envoi des rapports mensuels

Acrobat Connect Pro vous envoie chaque mois un courrier électronique concernant la capacité de votre compte. Par défaut, les rapports mensuels de capacité de compte sont envoyés à 15h00 UTC. Pour qu'Acrobat Connect Pro envoie le courrier électronique à une autre heure, vous pouvez ajouter des paramètres au fichier custom.ini et définir les valeurs souhaitées.

Pour plus d'informations sur la configuration des notifications de compte dans Connect Pro Central, reportez-vous au chapitre « Administration d'Acrobat Connect Pro » du document *Utilisation d'Adobe Acrobat Connect Pro 7* disponible en ligne à l'adresse www.adobe.com/go/connect_documentation_fr.

1 Ouvrez le fichier *Rép_Install_Racine*\custom.ini et ajoutez les paramètres suivants au fichier avec les valeurs souhaitées :

THRESHOLD_MAIL_TIME_OF_DAY_HOURS Heure UTC à laquelle sont envoyés les rapports mensuels de notification de capacité. Cette valeur doit être un entier compris entre 0 et 23. Ce paramètre doit être défini dans le fichier custom.ini ; il ne peut pas être défini dans Connect Pro Central.

THRESHOLD_MAIL_TIME_OF_DAY_MINUTES Minute à laquelle sont envoyés les rapports mensuels de notification de capacité. Cette valeur doit être un entier compris entre 0 et 59. Ce paramètre doit être défini dans le fichier custom.ini ; il ne peut pas être défini dans Connect Pro Central.

Remarque : *Si l'un des paramètres précédents n'est pas spécifié ou est erroné, le courrier électronique est envoyé à 15h00 (UTC).*

Exemples de valeurs ajoutées au fichier custom.ini :

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

2 Procédez comme suit pour redémarrer Acrobat Connect Pro :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

Définition de seuils de capacité

Les administrateurs de compte Acrobat Connect Pro peuvent définir des seuils de capacité dans Connect Pro Central. Le dépassement de ces seuils par un compte déclenche l'envoi d'une notification. Vous pouvez ajouter au fichier custom.ini des paramètres qui définissent les seuils de capacité par défaut dans Connect Pro Central.

Pour plus d'informations sur la configuration des notifications de compte dans Connect Pro Central, reportez-vous au chapitre « Administration d'Acrobat Connect Pro » du document *Utilisation d'Adobe Acrobat Connect Pro 7* disponible en ligne à l'adresse www.adobe.com/go/connect_documentation_fr.

1 Ouvrez le fichier *Rép_Install_Racine* \custom.ini et ajoutez l'un des paramètres suivants au fichier avec les valeurs souhaitées :

THRESHOLD_NUM_OF_MEMBERS Pourcentage de seuil par défaut du quota d'auteurs et d'hôtes de réunion. Cette valeur doit être un entier compris entre 10 et 100 et divisible par 10. Si aucune valeur n'est spécifiée ou qu'elle est erronée, c'est la valeur 80 qui est utilisée.

THRESHOLD_CONC_USERS_PER_MEETING Pourcentage de seuil par défaut du quota d'utilisateurs simultanés par réunion. Cette valeur doit être un entier compris entre 10 et 100 et divisible par 10. Si aucune valeur n'est spécifiée ou qu'elle est erronée, c'est la valeur 80 qui est utilisée.

THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT Pourcentage de seuil par défaut du quota de participants à la réunion à l'échelle du compte. Cette valeur doit être un entier compris entre 10 et 100 et divisible par 10. Si aucune valeur n'est spécifiée ou qu'elle est erronée, c'est la valeur 80 qui est utilisée.

THRESHOLD_CONC_TRAINING_USERS Pourcentage de seuil par défaut du quota de stagiaires simultanés. Cette valeur doit être un entier compris entre 10 et 100 et divisible par 10. Si aucune valeur n'est spécifiée ou qu'elle est erronée, c'est la valeur 80 qui est utilisée.

Exemples de valeurs ajoutées au fichier 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 Procédez comme suit pour redémarrer Acrobat Connect Pro :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

Intégration à Microsoft Live Communications Server 2005 et Microsoft Office Communications Server 2007

Procédure de configuration de l'intégration de présence

Intégrez Acrobat Connect Pro à un serveur de communications en temps réel Microsoft de manière à ce que les hôtes de réunion puissent voir la présence LCS ou OCS des participants à la réunion enregistrés dans la liste des invités et initier des conversations texte avec des utilisateurs en ligne.

Pour plus d'informations sur la liste des invités, reportez-vous au document *Utilisation d'Adobe Acrobat Connect Pro* disponible en ligne à l'adresse www.adobe.com/go/connect_documentation_fr.

1. Acrobat Connect Pro Server 7 et un serveur de communications doivent être installés.

Installez et vérifiez l'installation d'Acrobat Connect Pro Server 7 et d'un serveur de communications. Acrobat Connect Pro Server 7 prend en charge l'intégration à Microsoft Live Communications Server 2005 et Microsoft Office Communications Server 2007. Reportez-vous à la section « Installation d'Acrobat Connect Pro Server 7 » à la page 13 et à la documentation du serveur de communications.

2. Configurez le serveur de communication.

Configurez le serveur de communications pour échanger des données avec Acrobat Connect Pro Server 7. Reportez-vous à la section « Configuration de Live Communications Server 2005 ou d'Office Communications Server 2007 » à la page 40.

3. Arrêtez Connect Pro Presence Service.

Acrobat Connect Pro Presence Service fait partie de Connect Pro Server 7. Arrêtez le service avant de configurer Acrobat Connect Pro. Reportez-vous à la section « Démarrage et arrêt de Connect Pro Presence Service » à la page 44.

4. Configurez Connect Pro Presence Service.

Configurez Acrobat Connect Pro pour échanger des données avec le serveur de communications. Le serveur de présence est installé par défaut sous C:\breeze\presserv. Reportez-vous à la section « Configuration de Connect Pro Presence Service » à la page 41.

5. Démarrez Connect Pro Presence Service.

Reportez-vous à la section « Démarrage et arrêt de Connect Pro Presence Service » à la page 44.

6. Activez la liste des invités et le module Conversation dans Connect Pro Central.

Connectez-vous à Connect Pro Central en tant qu'administrateur. Sélectionnez Administration > Conformité et contrôle > Gestion de modules. Décochez l'option pour désactiver la liste des invités et le module Conversation.

Configuration de Live Communications Server 2005 ou d'Office Communications Server 2007

1 Sélectionnez Démarrer > Programmes > Outils d'administration > Live Communications Server 2005 ou Office Communications Server 2007 pour ouvrir la Console de configuration.

2 Cliquez avec le bouton droit sur la forêt, sélectionnez Propriétés, et procédez comme suit :

a Sélectionnez l'onglet Fédération.

b Activez la case à cocher Activer la connectivité IM publique et de fédération.

c Entrez l'adresse réseau d'Acrobat Connect Pro.

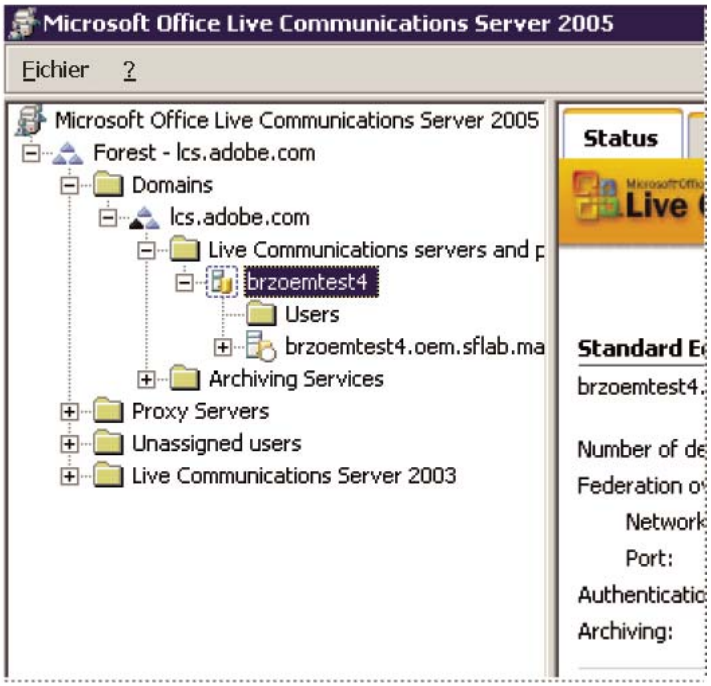
d Entrez le port 5072.

5072 est le numéro de port par défaut de Connect Pro Presence Service dans le fichier \presserv\conf\lcsgw.xml.

e Cliquez sur OK.

3 Dans le volet gauche de la Console de configuration, développez Domaines, développez votre domaine, puis développez les serveurs et les pools Live Communications.

4 Cliquez avec le bouton droit sur le nom d'hôte de votre pool et sélectionnez Propriétés.



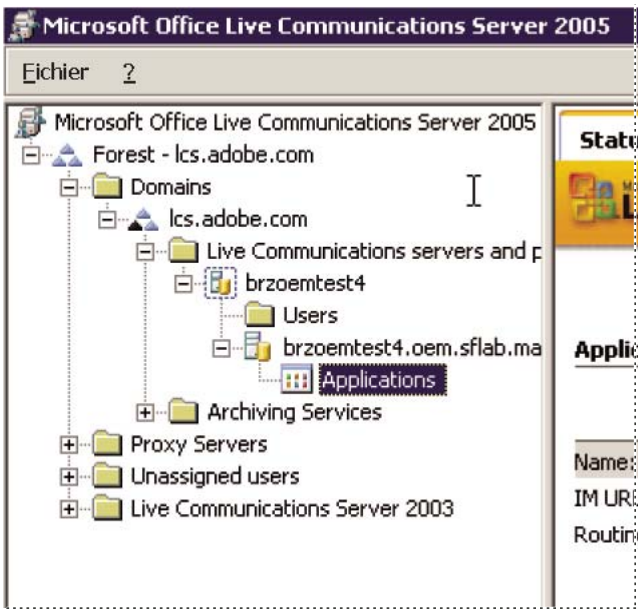
5 Dans la boîte de dialogue Propriétés du serveur, procédez comme suit :

a Sélectionnez l'onglet Autorisation d'hôte. Ajoutez l'adresse IP d'Acrobat Connect Pro. Vérifiez que Sortant uniquement a la valeur Non, que Accélérer comme serveur a la valeur Oui, et que Traiter comme authentification a la valeur Oui.

b Si un équilibreur de charge est installé devant votre serveur Acrobat Connect Pro, ajoutez son adresse IP.

c Cliquez sur OK.

6 Dans le volet gauche de la Console de configuration, développez le nom de domaine pleinement qualifié (FQDN) de votre serveur et sélectionnez Applications.



7 Effectuez les opérations suivantes :

a Cliquez sur Paramétrage de l'application de filtre URL IM. Dans la boîte de dialogue Propriétés, désactivez l'option Activer. Si cette option est activée, les hôtes de réunion ne peuvent pas envoyer d'URL dans des messages instantanés.

8 Fermez la Console de configuration.

Configuration des clients du serveur de communication

L'intégration d'Acrobat Connect Pro à des serveurs de communications Microsoft fonctionne avec des clients Microsoft Office Communicator 2005 (MOC 2005) standard. Les clients ne nécessitent aucune configuration particulière. Toutefois, pour pouvoir cliquer sur les URL Connect Meeting dans MOC 2005, modifiez la propriété « Autoriser les liens hypertexte dans les messages instantanés » du modèle Administration du communicateur. Pour plus d'informations, visitez http://technet.microsoft.com/en-us/library/bb963959.aspx.

1 Sélectionnez Démarrer > Exécuter.

2 Entrez gpedit.msc dans la zone Ouvrir pour ouvrir la fenêtre Stratégie de groupe.

3 Cliquez pour développer Configuration de l'ordinateur.

4 Cliquez pour développer Modèles d'administration.

5 Cliquez avec le bouton droit sur Paramètres de la stratégie de Microsoft Office Communicator et choisissez Propriétés.

Remarque : *Si le modèle Paramètres de la stratégie de Microsoft Office Communicator n'apparaît pas dans le dossier Modèles d'administration, ajoutez-le. Localisez Communicator.adm dans le package client Microsoft Office Communicator 2005 et copiez-le sous C:\WINDOWS\inf\. Dans la fenêtre Stratégie de groupe, cliquez avec le bouton droit sur Modèles d'administration, cliquez sur Ajouter/Supprimer des modèles, puis sur Ajouter, accédez au fichier, puis cliquez sur Ouvrir.*

Configuration de Connect Pro Presence Service

Effectuez les quatre procédures suivantes pour configurer Connect Pro Presence Service pour échanger des données avec un serveur de communication. Une fois la configuration terminée, redémarrez Connect Pro Central Application Server.

Définition de la connexion de passerelle entre Connect Pro Presence Service et le serveur de communication

1 Ouvrez le fichier \breeze\presserv\conf\lcsgw.xml dans un éditeur XML.

2 Modifiez le fichier comme suit en remplaçant vos valeurs par celles en gras :

```
<?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>
```

Paramètre	Description
<host>	Domaine SIP des utilisateurs LCS ou OCS
<bind>	Adresse IP du serveur LCS ou OCS (ou de l'équilibreur de charge)
<area>	Domaine SIP des utilisateurs LCS ou OCS

Configuration du fichier custom.ini.

1 Ouvrez le fichier \breeze\custom.ini dans un éditeur de texte.

2 Entrez les paramètres et valeurs ci-dessous :

Paramètre	Valeur
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Cette valeur respecte la casse.
OPN_HOST	Adresse réseau de Connect Pro Presence Service (par exemple, localhost).
OPN_PORT	Port interne utilisé entre Acrobat Connect Pro et Connect Pro Presence Service. La valeur par défaut (10020) doit correspondre à la valeur du fichier \breeze\presserv\conf.router.xml. Ne modifiez pas cette valeur.
OPN_PASSWORD	Jeton interne utilisé entre Acrobat Connect Pro et Connect Pro Presence Service. La valeur par défaut (secret) doit correspondre à la valeur du fichier \breeze\presserv\conf.router.xml. Ne modifiez pas cette valeur.
OPN_DOMAIN	Nom de domaine du serveur Acrobat Connect Pro (serveur d'applications). Connect Pro Presence Service utilise ce nom pour identifier le serveur d'applications. Dans un cluster, chaque serveur d'applications doit avoir son propre nom de domaine.
MEETING_PRESENCE_POLL_INTERVAL	Les clients hôtes interrogent régulièrement le serveur de présence pour récupérer l'état des invités. Ce paramètre définit le nombre de secondes entre des requêtes d'interrogation. La valeur par défaut est 30. Ne modifiez pas cette valeur.

Exemples de paramètres :

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

Définition de la passerelle SIP vers Connect Pro Presence Service

1 Ouvrez le fichier \breeze\presserv\conf\router.xml dans un éditeur XML.

2 Modifiez le fichier comme suit en remplaçant vos valeurs par celles en gras :

```
<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>
```

Dans la balise `<liaison>`, entrez l'adresse IP de l'ordinateur qui héberge Acrobat Connect Pro. Si plusieurs adresses IP sont renvoyées, sélectionnez l'adresse IP interne ou externe que le serveur LCS ou OCS distant peut résoudre pour se connecter à Acrobat Connect Pro.

3 Redémarrez Connect Pro Central Application Server.

Configuration de Connect Pro Presence Service dans un cluster

Si vous exécutez Connect Pro dans un cluster, exécutez Connect Pro Presence Service sur un seul ordinateur du cluster. Veillez cependant à configurer Connect Pro Presence Service sur tous les ordinateurs du cluster de manière à permettre l'échange du trafic de présence.

1 Ouvrez *rép_install_racine*\custom.ini dans un éditeur de texte.

2 Entrez les paramètres et valeurs ci-dessous :

Paramètre	Valeur
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Cette valeur respecte la casse.
OPN_HOST	Nom de domaine pleinement qualifié de l'ordinateur qui exécute Connect Pro Presence Service. La valeur du paramètre OPN_HOST est la même sur chaque ordinateur d'un cluster.
OPN_PORT	Port interne utilisé entre Acrobat Connect Pro et Connect Pro Presence Service. La valeur par défaut (10020) doit correspondre à la valeur du fichier \breeze\presserv\conf.router.xml. Ne modifiez pas cette valeur.
OPN_PASSWORD	Jeton interne utilisé entre Acrobat Connect Pro et Connect Pro Presence Service. La valeur par défaut (secret) doit correspondre à la valeur du fichier \breeze\presserv\conf.router.xml. Ne modifiez pas cette valeur.
OPN_DOMAIN	Domaine qu'utilise Connect Pro Presence Service pour identifier un serveur Connect Pro dans un cluster. Chaque ordinateur d'un cluster doit avoir une valeur unique. Le paramètre OPN_DOMAIN peut avoir une valeur quelconque (par exemple, presence.connect1, presence.connect2, connect3) pour autant qu'elle soit unique dans le cluster.
MEETING_PRESENCE_POLL_INTERVAL	Les clients hôtes interrogent régulièrement le serveur de présence pour récupérer l'état des invités. Ce paramètre définit le nombre de secondes entre des requêtes d'interrogation. La valeur par défaut est 30. Ne modifiez pas cette valeur.

Exemples de paramètres :

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

3 Redémarrez Connect Pro Central Application Server.

Démarrage et arrêt de Connect Pro Presence Service

Vous pouvez arrêter et démarrer Connect Pro Presence Service dans le menu Démarrer ou dans la fenêtre Services.

Démarrage et arrêt de Connect Pro Presence Service via le menu Démarrer

❖ Effectuez l'une des opérations suivantes :

- Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Presence Service.
- Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Presence Service.

Démarrage et arrêt de Connect Pro Presence Service via la fenêtre Services

1 Choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services.

2 Sélectionnez Acrobat Connect Pro Presence Service et cliquez sur Démarrer le service, Arrêter le service ou Redémarrer le service.

Configuration de l'authentification unique

A propos de l'authentification unique

L'authentification unique est un mécanisme qui authentifie les utilisateurs pour toutes les applications pour lesquelles ils disposent de droits d'accès sur un réseau. L'authentification unique utilise un serveur proxy pour authentifier les utilisateurs afin qu'ils ne doivent pas ouvrir de session dans Acrobat Connect Pro.

Acrobat Connect Pro prend en charge le mécanisme d'authentification unique suivant :

Authentification des en-têtes HTTP Configurez un proxy d'authentification pour intercepter la requête HTTP, analysez les informations de connexion de l'utilisateur dans l'en-tête et transmettez-les à Acrobat Connect Pro.

Vous pouvez également écrire votre propre filtre d'authentification. Pour plus d'informations, contactez l'assistance technique d'Adobe.

Configuration de l'authentification des en-têtes HTTP

Lorsque l'authentification des en-têtes HTTP est configurée, les requêtes de connexion à Acrobat Connect Pro sont acheminées vers un agent placé entre le client et Acrobat Connect Pro. Cet agent peut être un proxy d'authentification ou une application logicielle qui authentifie l'utilisateur, ajoute un autre en-tête dans la requête HTTP et envoie celle-ci à Acrobat Connect Pro. Sur Acrobat Connect Pro, vous devez retirer le commentaire d'un filtre Java et configurer un paramètre du fichier custom.ini qui indique le nom de l'en-tête HTTP supplémentaire.

Voir aussi

« Démarrage et arrêt d'Acrobat Connect Pro Server 7 » à la page 18

Configuration d'une authentification des en-têtes HTTP sur Acrobat Connect Pro

Pour activer l'authentification des en-têtes HTTP, configurez le mappage d'un filtre Java et un paramètre d'en-tête sur l'ordinateur qui héberge Acrobat Connect Pro.

1 Ouvrez le fichier *[rép_install_racine]*\appserv\conf\WEB-INF\web.xml et procédez comme suit :

a Retirez les commentaires du mappage du filtre Java HeaderAuthenticationFilter.

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

b Appliquez un commentaire au mappage du filtre Java NtlmAuthenticationFilter.

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

2 Arrêtez Acrobat Connect Pro :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Server 7 > Arrêter Adobe Connect Meeting Server.

3 Ajoutez la ligne suivante dans le fichier custom.ini :

`HTTP_AUTH_HEADER=`*`header_field_name`*

Votre agent d'authentification doit ajouter un en-tête à la requête HTTP envoyée à Acrobat Connect Pro. Le nom de l'en-tête doit être *`header_field_name`*.

4 Enregistrez le fichier custom.ini et redémarrez Acrobat Connect Pro.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Server 7 > Démarrer Adobe Connect Meeting Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

Rédaction du code d'authentification

Le code d'authentification doit authentifier l'utilisateur, ajouter un champ dans l'en-tête HTTP contenant le nom d'utilisateur et envoyer une requête à Acrobat Connect Pro.

1 Sélectionnez la valeur du champ d'en-tête *`nom_champ_en-tête`* pour une connexion utilisateur à Acrobat Connect Pro.

2 Envoyez une requête HTTP à Acrobat Connect Pro à l'adresse URL suivante :

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

Le filtre Java sur Acrobat Connect Pro intercepte la requête, recherche l'en-tête *`nom_champ_en-tête`*, puis recherche un utilisateur avec l'ID transmis dans l'en-tête. Si l'utilisateur est localisé, il est authentifié et une réponse est envoyée.

3 Dans le contenu HTTP de la réponse d'Acrobat Connect Pro, recherchez la chaîne « `OK` » qui indique une authentification réussie.

4 Dans la réponse d'Acrobat Connect Pro, recherchez le cookie `BREEZESESSION`.

5 Redirigez l'utilisateur vers l'URL requise sur Acrobat Connect Pro et transmettez le cookie `BREEZESESSION` représentant la valeur du paramètre `session`, comme suit :

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

Remarque : *Vous devez transmettre le cookie* `BREEZESESSION` *dans toute requête ultérieure à Acrobat Connect Pro au cours de la session client.*

Configuration de l'authentification des en-têtes HTTP avec Apache

La procédure suivante décrit un exemple d'implémentation de l'authentification des en-têtes HTTP qui utilise Apache comme agent d'authentification.

1 Installez Apache en tant que proxy inverse sur un autre ordinateur que celui qui héberge Acrobat Connect Pro.

2 Choisissez Démarrer > Programmes > Apache HTTP Server > Configurer Apache Server et modifiez le fichier de configuration httpd.conf d'Apache de la manière suivante :

a Retirez les commentaires de la ligne suivante :

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

b Retirez les commentaires des trois lignes suivantes :

```
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 Ajoutez les lignes suivantes à la fin du fichier :

```
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 Arrêtez Acrobat Connect Pro :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Server 7 > Arrêter Adobe Connect Meeting Server.

4 Sur l'ordinateur qui héberge Acrobat Connect Pro, ajoutez les lignes de code suivantes dans le fichier custom.ini (situé dans le répertoire racine d'installation, c:\breeze par défaut) :

```
HTTP_AUTH_HEADER=custom-auth
```

Le paramètre `HTTP_AUTH_HEADER` doit correspondre au nom configuré sur le serveur proxy. (Dans cet exemple, il a été configuré à la ligne 1 de l'étape 2c.) Le paramètre correspond à l'en-tête HTTP supplémentaire.

5 Enregistrez le fichier custom.ini et redémarrez Acrobat Connect Pro.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Server 7 > Démarrer Adobe Connect Meeting Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

6 Ouvrez le fichier *[rép_install_racine]*\appserv\conf\WEB-INF\web.xml et procédez comme suit :

a Retirez les commentaires du mappage du filtre Java HeaderAuthenticationFilter.

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

b Appliquez un commentaire au mappage du filtre Java NtlmAuthenticationFilter.

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

Hébergement d'Acrobat Connect Add-in

Présentation d'Acrobat Connect Add-in

Adobe Acrobat Connect Add-in est une version de Flash Player qui comprend des fonctionnalités avancées pour les réunions Acrobat Connect Pro.

Lorsqu'Acrobat Connect Add-in est nécessaire, il est téléchargé depuis un serveur Adobe par un processus transparent que l'utilisateur ne voit pas. Toutefois, si votre société n'autorise pas ses employés à télécharger des logiciels à partir de serveurs externes, vous pouvez héberger Acrobat Connect Add-in sur votre propre serveur.

Les invités aux réunions, les utilisateurs inscrits et les présentateurs sont invités à télécharger Acrobat Connect Add-in lorsqu'une ancienne version est installée sur leur ordinateur et qu'ils sont promus hôte ou présentateur ou que des droits étendus leur sont accordés pour le module Partage.

Les hôtes de réunion doivent obligatoirement télécharger Acrobat Connect Add-in lorsqu'il n'est pas installé ou pour remplacer une ancienne version.

Personnalisation de l'emplacement de téléchargement d'Acrobat Connect Add-in

Vous pouvez héberger Acrobat Connect Add-in sur votre serveur et envoyer directement les utilisateurs vers les fichiers exécutables. Vous pouvez également diriger les utilisateurs vers une page d'instructions de téléchargement contenant des liens vers les fichiers exécutables. Vous pouvez créer votre propre page d'instructions de téléchargement ou utiliser celle fournie par Adobe. La page d'Adobe est traduite dans toutes les langues prises en charge.

Envoyez directement les utilisateurs vers les fichiers exécutables.

1 Recherchez les fichiers de langue XML Acrobat Connect Pro sur le serveur hébergeant Acrobat Connect Pro. Les fichiers XML se trouvent dans les deux répertoires suivants :*[rép_install_racine]*\appserv\web\common\intro\lang et *[rép_install_racine]*\appserv\web\common\meeting\lang\.

2 Entrez un chemin aux fichiers exécutable pour chaque plate-forme dans la section `addInLocation` de chaque plate-forme dans chaque fichier de langue :

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

Remarque : *Il s'agit là des emplacements par défaut des fichiers exécutables de l'Add-in. Vous pouvez modifier ces emplacements sur votre serveur et modifier les chemins d'accès en conséquence dans la section addInLocation.*

Envoyez les utilisateurs vers les pages d'instructions de téléchargement fournies par Adobe.

1 Recherchez les fichiers de langue XML Acrobat Connect Pro sur le serveur hébergeant Acrobat Connect Pro. Les fichiers XML se trouvent dans les deux répertoires suivants :*[rép_install_racine]*\appserv\web\common\intro\lang et *[rép_install_racine]*\appserv\web\common\meeting\lang\.

2 Entrez le chemin à la page d'instructions de téléchargement dans la section `addInLocation` de chaque plate-forme dans chaque fichier de langue :

```
<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>
```

Remarque : *Le chemin comprend une chaîne* `#lang#` *qu'Acrobat Connect Pro traduit dans la langue de la réunion au moment de l'exécution.*

3 Le fichier addindownload.htm comprend des liens vers les emplacements par défaut des fichiers exécutables de l'Add-in sur Acrobat Connect Pro (/common/addin/setup.exe et /common/addin/AcrobatConnectAddin.z). Si vous modifiez l'emplacement des fichiers exécutables, actualisez les liens de la page addindownload.htm pour chaque langue.

Envoyez les utilisateurs vers vos propres pages d'instructions de téléchargement.

1 Recherchez les fichiers de langue XML Acrobat Connect Pro sur le serveur hébergeant Acrobat Connect Pro. Les fichiers XML se trouvent dans les deux répertoires suivants :*[rép_install_racine]*\appserv\web\common\intro\lang et *[rép_install_racine]*\appserv\web\common\meeting\lang\.

2 Dans la section `addInLocation` de chaque plate-forme dans chaque fichier de langue, entrez le chemin à la page d'instructions que vous avez créée :

```
<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>
```

Remarque : *Vous pouvez créer des pages d'instructions distinctes pour chaque plate-forme.*

3 Créez une page d'instruction pour chaque langue que vous désirez prendre en charge. Dans la page d'instructions, ajoutez des liens vers les fichiers exécutables de l'Add-in pour chaque plate-forme.

Chapitre 4 : Sécurité

La sécurisation d'Adobe Acrobat Connect Pro Server 7 protège votre société contre les pertes de biens et les actes de malveillance. Il est important de sécuriser l'infrastructure de votre société, Acrobat Connect Pro, ainsi que le serveur de base de données qu'utilise Acrobat Connect Pro.

Protocole SSL (Secure Sockets Layer)

A propos de la prise en charge SSL

Acrobat Connect Pro est composé de deux serveurs : Adobe® Flash® Media Server et le serveur d'applications Acrobat Connect Pro. Flash Media Server est appelé « *serveur de réunions* » car il permet au client d'accéder aux réunions via une connexion RTMP en temps réel. Le serveur d'applications Acrobat Connect Pro gère la connexion HTTP entre le client et la logique applicative d'Acrobat Connect Pro.

Remarque : *Dans le menu Démarrer, le serveur de réunions est appelé « Connect Pro Meeting Server » et le serveur d'applications « Connect Pro Central Application Server ». Dans la fenêtre Services, le serveur de réunions est appelé « Flash Media Server (FMS) » et le serveur d'applications « Adobe Connect Enterprise Service »..*

Vous pouvez configurer SSL pour le serveur d'applications, pour le serveur de réunions, ou pour les deux :

Solution matérielle Pour obtenir une configuration SSL la plus fiable possible, utilisez un accélérateur SSL.

Achetez un accélérateur SSL séparément. Adobe a vérifié le fonctionnement d'Acrobat Connect Pro avec les accélérateurs matériels SSL suivants : F5 Big-IP 1000, Cisco Catalyst 6590 Switch et Radware T100.

Solution logicielle Utilisez la prise en charge native de SSL dans Acrobat Connect Pro.

Remarque : *SSL n'est pas pris en charge sous Microsoft® Windows® 98.*

Acrobat Connect Pro utilise la méthode HTTP `CONNECT` pour demander une connexion SSL. Les serveurs proxy doivent autoriser les clients à utiliser la méthode `CONNECT` . Si les clients ne peuvent pas utiliser la méthode `CONNECT` , les connexions RTMP passent par HTTP/HTTPS.

Pour obtenir de l'aide sur la configuration de SSL, contactez l'assistance technique d'Adobe à l'adresse www.adobe.com/go/connect_licensed_programs_fr.

Utilisation de certificats

Un certificat SSL vérifie l'identité du serveur sur le client.

Pour sécuriser les connexions des serveurs de réunions (RTMP) et d'applications (HTTP), vous devez disposer de deux certificats SSL, un pour chaque connexion. Pour configurer SSL pour un cluster d'ordinateurs qui hébergent Acrobat Connect Pro, vous devez avoir un certificat SSL pour chaque serveur de réunions. Vous pouvez utiliser un certificat pour tous les serveurs d'applications d'un cluster.

Par exemple, pour sécuriser les connexions des serveurs de réunions et d'applications sur un seul serveur, il vous faudra deux certificats SSL. Pour sécuriser les connexions des serveurs de réunions et d'applications sur un cluster de trois serveurs, il vous faudra quatre certificats SSL : un pour les serveurs d'applications et les trois autres pour les serveurs de réunions.

Obtention de certificats

❖ Contactez une autorité de certification, organisme tiers approuvé qui vérifie l'identité du demandeur. (Les certificats auto-signés ne fonctionnent pas avec Acrobat Connect Pro.)

L'autorité de certification vous invite à générer un fichier CSR (Certificate Signing Request) SSL. Envoyez-le à l'autorité de certification qui le convertira en certificat SSL. Il contient des informations sur votre société et le nom de domaine pleinement qualifié associé au certificat SSL. Pour des instructions précises sur la création d'un fichier CSR, contactez votre autorité de certification.

Important : *Conservez les mots de passe de vos certificats SSL dans un endroit sécurisé et accessible.*

Installation des certificats

❖ Installez les certificats SSL au format PEM dans le dossier racine d'Acrobat Connect Pro (C:\breeze, par défaut).

Si vous recevez un fichier CRT d'une autorité de certification, vous pouvez le renommer en lui donnant l'extension .pem.

Remarque : *Vous devez disposer d'un seul fichier de clé publique/privée.*

Configuration d'un protocole SSL logiciel

Lorsque vous configurez un protocole SSL logiciel, vous pouvez sécuriser le serveur d'applications (HTTP), le serveur de réunions (RTMP) ou les deux. Configurez le serveur DNS. Il est conseillé de tester votre configuration avant de l'utiliser en production.

Configuration du serveur DNS

❖ Créez des entrées DNS qui définissent un nom de domaine pleinement qualifié pour chaque connexion sécurisée.

Le nom de domaine pleinement qualifié du serveur d'applications est l'URL avec laquelle les utilisateurs finaux se connectent à Acrobat Connect Pro. Entez ce nom de domaine pleinement qualifié pour la valeur Hôte Connect Pro dans la page Paramètres du serveur de la Console de gestion des applications. « connect » est un exemple de valeur valide. *votresociété* .com

Les utilisateurs finaux ne voient pas le nom de domaine pleinement qualifié du serveur de réunions. Il est cependant indispensable d'en définir un pour le serveur de réunions si vous souhaitez tenir des réunions via une connexion sécurisée. Entrez le nom de domaine pleinement qualifié dans la zone Nom externe de la page Paramètres du serveur de la Console de gestion des applications. Valeur possible : fms.votresociété.com.

Remarque : *Vous pouvez utiliser un certificat SSL pour tous les serveurs d'applications d'un cluster, mais il vous faut un certificat SSL unique pour chaque serveur de réunions. Pour sécuriser à la fois les connexions HTTP et RTMP sur un serveur, il vous faut deux noms de domaine pleinement qualifiés et deux certificats.*

Sécurisation des serveurs de réunions et d'applications

1 Ouvrez le fichier Adaptor.xml situé dans le dossier *[rép_install_racine]*\comserv\win32\conf_defaultRoot_ et enregistrez une copie de sauvegarde à un autre emplacement.

2 Ajoutez le code suivant dans le fichier Adaptor.xml d'origine, à l'intérieur des balises `<Adaptor></Adaptor>` (remplacez le code en italique par vos propres valeurs) :

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

3 Localisez la ligne suivante dans le fichier Adaptor.xml :

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

4 Remplacez le code de l'étape 3 par :

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

5 Enregistrez le fichier Adaptor.xml.

6 (Facultatif) Ouvrez le fichier Adaptor.xml dans un navigateur Web pour valider sa syntaxe.

Si le navigateur signale une erreur, corrigez-la, puis rouvrez le fichier dans un navigateur Web. Répétez ce processus jusqu'à ce que le fichier soit valide.

7 Ouvrez le fichier custom.ini situé dans le répertoire d'installation racine (c:\breeze, par défaut) et enregistrez une copie de sauvegarde dans un autre emplacement.

8 Insérez le code suivant dans le fichier custom.ini, sans remplacer ni supprimer le texte existant :

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

Remarque : *Le fichier custom.ini respecte la casse ; utilisez des majuscules pour les noms de paramètre et des minuscules pour les valeurs.*

9 Enregistrez le fichier custom.ini.

10 Ouvrez le fichier VHost.xml situé dans le dossier *[rép_install_racine]*\comserv\win32\conf_defaultRoot__defaultVHost_ et enregistrez une copie de sauvegarde à un autre emplacement.

11 Localisez la ligne suivante dans le fichier VHost.xml :

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

12 Remplacez la ligne de l'étape 11 par le code suivant :

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

13 Enregistrez le fichier VHost.xml.

14 (Facultatif) Ouvrez le fichier VHost.xml dans un navigateur Web pour valider sa syntaxe.

15 Redémarrez Adobe Connect Pro Server 7 :

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Meeting Server.

c Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Meeting Server.

d Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

16 Ouvrez la Console de gestion des applications ((http://localhost:8510/console ou Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Configurer Connect Pro Server 7).

17 Dans l'écran Paramètres de l'application, sélectionnez Paramètres du serveur et procédez comme suit :

a Entrez le nom de domaine pleinement qualifié de votre compte Connect Acrobat Pro dans la zone Hôte Connect Pro. Ce nom de domaine pleinement qualifié est l'URL avec laquelle les utilisateurs finaux se connectent à Acrobat Connect Pro.

b Entrez le nom de domaine pleinement qualifié du serveur de réunions Acrobat Connect Pro dans la zone Nom externe sous Mappages de l'hôte. Le serveur utilise cette valeur en interne.

Sécurisation du serveur d'applications uniquement

1 Ouvrez le fichier Adaptor.xml situé dans le dossier *[rép_install_racine]*\comserv\win32\conf_defaultRoot_ et enregistrez une copie de sauvegarde à un autre emplacement.

2 Ajoutez le code suivant dans le fichier Adaptor.xml d'origine, à l'intérieur des balises `<Adaptor></Adaptor>` (remplacez le code en italique par vos propres valeurs) :

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

3 Localisez la ligne suivante dans le fichier Adaptor.xml :

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

4 Insérez le code suivant sous la ligne ajoutée à l'étape 3 :

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

5 Enregistrez le fichier Adaptor.xml.

6 (Facultatif) Ouvrez le fichier Adaptor.xml dans un navigateur Web pour valider sa syntaxe.

Si le navigateur signale une erreur, corrigez-la, puis rouvrez le fichier dans un navigateur Web. Répétez ce processus jusqu'à ce que le fichier soit valide.

7 Ouvrez le fichier custom.ini situé dans le répertoire d'installation racine (c:\breeze, par défaut) et enregistrez une copie de sauvegarde dans un autre emplacement.

8 Insérez le code suivant dans le fichier custom.ini, sans remplacer ni supprimer le texte existant :

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

***Remarque :** Le fichier custom.ini respecte la casse ; utilisez des majuscules pour les noms de paramètre et des minuscules pour les valeurs.*

9 Enregistrez le fichier custom.ini.

10 Redémarrez Acrobat Connect Pro Server 7.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Meeting Server.

c Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Meeting Server.

d Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

Sécurisation du serveur de réunions uniquement

1 Ouvrez le fichier Adaptor.xml situé dans le dossier *[rép_install_racine]*\comserv\win32\conf_defaultRoot_ et enregistrez une copie de sauvegarde à un autre emplacement.

2 Ajoutez le code suivant dans le fichier Adaptor.xml d'origine, à l'intérieur des balises `<Adaptor></Adaptor>` (remplacez le code en italique par vos propres valeurs) :

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

3 Localisez la ligne suivante dans le fichier Adaptor.xml :

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

4 Remplacez le code de l'étape 3 par :

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

5 Enregistrez le fichier Adaptor.xml.

6 (Facultatif) Ouvrez le fichier Adaptor.xml dans un navigateur Web pour valider sa syntaxe.

Si le navigateur signale une erreur, corrigez-la, puis rouvrez le fichier dans un navigateur Web. Répétez ce processus jusqu'à ce que le fichier soit valide.

7 Ouvrez le fichier VHost.xml situé dans le dossier *[rép_install_racine]*\comserv\win32\conf_defaultRoot__defaultVHost_ et enregistrez une copie de sauvegarde à un autre emplacement.

8 Localisez la ligne suivante dans le fichier VHost.xml :

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

9 Remplacez la ligne de l'étape 8 par le code suivant :

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

10 Enregistrez le fichier VHost.xml.

11 (Facultatif) Ouvrez le fichier VHost.xml dans un navigateur Web pour valider sa syntaxe.

12 Ouvrez le fichier custom.ini situé dans le répertoire d'installation racine (c:\breeze, par défaut) et enregistrez une copie de sauvegarde dans un autre emplacement.

13 Insérez le code suivant dans le fichier custom.ini, sans remplacer ni supprimer le texte existant :

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

14 Enregistrez le fichier custom.ini.

15 Redémarrez Acrobat Connect Pro Server 7.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Meeting Server.

c Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Meeting Server.

d Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

Test de la configuration

1 Si vous avez sécurisé le serveur d'applications, connectez-vous à Connect Pro Central. Un cadenas apparaît dans votre navigateur.

2 Si vous sécurisez le serveur de réunions, accédez à une salle de réunion Acrobat Connect Pro. Un cadenas apparaît dans le témoin de connexion.

Configuration d'un protocole SSL matériel

Lorsque vous configurez un protocole SSL matériel, vous pouvez sécuriser le serveur d'applications (HTTP), le serveur de réunions (RTMP) ou les deux. Configurez le serveur DNS. Il est conseillé de tester votre configuration avant de l'utiliser en production.

Pour plus d'informations sur la configuration de l'accélérateur matériel, consultez la documentation du fournisseur.

Configuration du serveur DNS

❖ Créez des entrées DNS pour tous les serveurs à sécuriser.

Définissez un nom de domaine pleinement qualifié pour chaque serveur sécurisé (par exemple, application.exemple.com et reunion1.exemple.com). En effet, les certificats SSL sont associés à des noms, et non à des adresses IP.

Remarque : *Vous pouvez utiliser un certificat SSL pour tous les serveurs d'applications d'un cluster, mais il vous faut un certificat SSL unique pour chaque serveur de réunions.*

Configuration de SSL pour les serveurs de réunions et d'application

1 Configurez le périphérique matériel dans les objectifs suivants :

a Ecoutez le port 443 en externe pour application.exemple.com.

b Transmettez les données non chiffrées au serveur d'applications sur le port 8443.

c Ecoutez le port 443 en externe pour reunion1.exemple.com.

d Transmettez les données non chiffrées au serveur de réunions sur le port 1935.

e (Facultatif) Ecoutez le port 80 en externe pour application.exemple.com et transmettez les données non chiffrées au serveur d'applications sur le port 80. Le serveur d'applications redirige les utilisateurs vers le port 443.

2 Configurez le pare-feu dans les objectifs suivants :

a Autorisez le trafic vers le serveur d'applications sur le port 443 (et sur le port 80 si vous avez terminé l'étape 1e).

b Autorisez le trafic vers le serveur de réunions sur le port 443.

3 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Configurer Connect Pro Server 7 pour ouvrir la Console de gestion des applications. Dans l'écran Paramètres de l'application, sélectionnez Paramètres du serveur et procédez comme suit :

a Entrez le nom de domaine pleinement qualifié du serveur d'applications (par exemple, connect.exemple.com) dans la zone Hôte Connect Pro. Ce nom de domaine pleinement qualifié est l'URL avec laquelle les utilisateurs finaux se connectent à Acrobat Connect Pro.

b Entrez le nom de domaine pleinement qualifié du serveur de réunions (par exemple, fms.exemple.com) dans la zone Nom externe sous Mappages de l'hôte. Le serveur utilise cette valeur en interne.

4 Ouvrez le fichier custom.ini situé dans le répertoire d'installation racine (c:\breeze, par défaut) et enregistrez une copie de sauvegarde dans un autre emplacement.

5 Insérez le code suivant dans le fichier custom.ini, sans remplacer ni supprimer le texte existant :

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

Remarque : *Le fichier custom.ini respecte la casse ; utilisez des majuscules pour les noms de paramètre et des minuscules pour les valeurs.*

6 Enregistrez le fichier custom.ini.

7 Redémarrez Acrobat Connect Pro Server 7.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

Configuration de SSL pour le serveur de réunions uniquement

1 Configurez le périphérique matériel dans les objectifs suivants :

a Ecoutez le port 443 en externe pour reunion1.exemple.com.

b Transmettez les données non chiffrées au serveur de réunions sur le port 1935.

2 Configurez le pare-feu pour autoriser le trafic vers le serveur de réunions sur le port 443.

3 Ouvrez le fichier custom.ini situé dans le répertoire d'installation racine (c:\breeze, par défaut) et enregistrez une copie de sauvegarde dans un autre emplacement.

4 Insérez le code suivant dans le fichier custom.ini, sans remplacer ni supprimer le texte existant :

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

5 Enregistrez le fichier custom.ini.

Configuration de SSL pour le serveur d'applications uniquement

1 Configurez le périphérique matériel dans les objectifs suivants :

a Ecoutez le port 443 en externe pour application.exemple.com.

b Transmettez les données non chiffrées au serveur d'applications sur le port 8443.

c (Facultatif) Ecoutez le port 80 en externe pour application.exemple.com et transmettez les données non chiffrées au serveur d'applications sur le port 80. Le serveur d'applications redirige les utilisateurs vers le port 443.

2 Configurez le pare-feu de manière à autoriser le trafic vers le serveur d'applications sur le port 443 (et sur le port 80 si vous avez terminé l'étape 1c).

3 Dans Acrobat Connect Pro, ajoutez le fichier custom.ini suivant dans le répertoire racine d'installation (C:\breeze, par défaut) :

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

Remarque : *Le fichier custom.ini respecte la casse ; utilisez des majuscules pour les noms de paramètre et des minuscules pour les valeurs.*

4 Redémarrez Acrobat Connect Pro Server 7.

a Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Arrêter Connect Pro Central Application Server.

b Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Démarrer Connect Pro Central Application Server.

Test de la configuration

1 Si vous avez sécurisé le serveur d'applications, connectez-vous à Connect Pro Central. Un cadenas apparaît dans votre navigateur.

2 Si vous sécurisez le serveur de réunions, accédez à une salle de réunion Acrobat Connect Pro. Un cadenas apparaît dans le témoin de connexion.

Configuration du protocole SSL logiciel pour un serveur Edge

Si le protocole SSL logiciel est configuré sur le serveur d'origine, configurez l'authentification SSL logicielle pour chaque serveur Edge à sécuriser.

A l'instar d'un serveur d'origine, un serveur Edge comprend deux services : un service de réunion et un service d'application. Pour configurer SSL pour le service de réunion et le service d'application, il vous faut deux noms de domaine pleinement qualifiés et deux adresses IP. Vous pouvez partager le nom de domaine pleinement qualifié du service d'application avec le serveur d'origine, mais le service de réunion, en revanche, doit avoir son propre nom de domaine pleinement qualifié. Le nom de domaine pleinement qualifié du service d'application est l'URL avec laquelle les utilisateurs se connectent à leurs comptes Acrobat Connect Pro.

Par exemple, si vous avez un serveur Edge et un serveur d'origine, il vous faut trois noms de domaine pleinement qualifiés et trois certificats SSL : un pour chaque service de réunion et un pour les services d'application à partager. Il vous faut également quatre adresses IP : une pour chaque service de réunion et une pour chaque service d'application.

Dans cet exemple de configuration, le serveur d'origine a les adresses IP et les noms de domaine pleinement qualifiés suivants :

```
10.192.37.11 = connect.yourcompany.com
10.192.37.10 = meeting1.yourcompany.com
```

Le serveur Edge a les adresses IP et les noms de domaine pleinement qualifiés suivants :

```
10.192.37.100 = connect.yourcompany.com
10.192.37.101 = edge1.yourcompany.com
```

Remarque : *Si vous installez le serveur Edge et le serveur d'origine pour la première fois, configurez les deux serveurs sans SSL et vérifiez qu'ils parviennent à communiquer ensemble. Une fois que la communication est établie, vous pouvez configurer SSL pour les deux serveurs.*

Voir aussi

« Déploiement d'Acrobat Connect Pro Edge Server 7 » à la page 25

« A propos de la prise en charge SSL » à la page 49

Configuration du serveur Edge

1 Sur le serveur d'origine, ouvrez le fichier c:\breeze\comserv\win32\conf_defaultRoot_\Adaptor.xml et copiez toute la section `<SSL></SSL>` , comme suit :

```
<SSL>
    <Edge name="applicationserver">
        <SSLServerCtx>
        <SSLCertificateFile>C:\breeze\connect.yourcompany.com.pem</SSLCertificateFile>
            <SSLCertificateKeyFile type="PEM">C:\breeze\connect.yourcompany.com.pem
            </SSLCertificateKeyFile>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
    <Edge name="meetingserver">
        <SSLServerCtx>
            <SSLCertificateFile>C:\breeze\meeting1.yourcompany.com.pem
            </SSLCertificateFile>
            <SSLCertificateKeyFile type="PEM">C:\breeze\meeting1.yourcompany.com.pem
            </SSLCertificateKeyFile>
            <SSLPassPhrase></SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

Remarque : *Votre code peut contenir différentes valeurs, mais il doit contenir les mêmes éléments XML.*

2 Sur le serveur Edge, ouvrez le fichier c:\breeze\edgeserver\win32\conf_defaultRoot_\Adaptor.xml et collez le bloc de code `<SSL></SSL>` du serveur d'origine après la balise `<Adaptor>` .

3 Procédez comme suit pour configurer le service d'application et le service de réunion sur le serveur Edge :

a Le service d'application est la balise `<Edge name="applicationserver">` dans le bloc `<SSL>` . Le service d'application utilise le même nom de domaine pleinement qualifié que le service d'application sur le serveur d'origine. Copiez les fichiers .pem du certificat et de la clé du serveur d'origine vers le même emplacement sur le serveur Edge. Dans cet exemple, le nom de domaine pleinement qualifié est connect.votresociété.com.

```
<Edge name="applicationserver">
    <SSLServerCtx>
        <SSLCertificateFile>C:\breeze\connect.yourcompany.com.pem</SSLCertificateFile>
        <SSLCertificateKeyFile type="PEM">C:\breeze\connect.yourcompany.com.pem
            </SSLCertificateKeyFile>
        <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
        <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
</Edge>
```

b Le service de réunion est la balise `<Edge name="meetingserver">` dans le bloc `<SSL>` . Modifiez le code XML de telle sorte que le service de réunion pointe vers un certificat et une clé uniques pour son nom de domaine pleinement qualifié unique. Dans cet exemple, le nom de domaine pleinement qualifié est edge1.votresociété.com.

```
<Edge name="meetingserver">
    <SSLServerCtx>
        <SSLCertificateFile>C:\breeze\edge1.yourcompany.com.pem
        </SSLCertificateFile>
        <SSLCertificateKeyFile type="PEM">C:\breeze\edge1.yourcompany.com.pem
        </SSLCertificateKeyFile>
        <SSLPassPhrase></SSLPassPhrase>
        <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
        <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
</Edge>
```

4 Dans le fichier Adaptor.xml sur le serveur Edge, localisez la ligne `<HostPort name="edge1">${FCS.HOST_PORT}</HostPort>` . Ajoutez les deux lignes ci-dessous à la suite :

```
<HostPort name="meetingserver" ctl_channel=":19354">206.192.37.100:-443</HostPort>
<HostPort name="applicationserver" ctl_channel=":19355">206.192.37.101:-443</HostPort>
```

Ce code relie les adresses IP internes du serveur Edge pour sécuriser le port 443. Cet exemple utilise les adresses IP internes 206.192.37.100 et 206.192.37.101. Dans votre code, remplacez les adresses IP internes de votre serveur Edge.

5 Enregistrez le fichier Adaptor.xml.

6 Ouvrez le fichier Adaptor.xml dans un navigateur Web pour vérifier que le code XML est valide.

S'il contient des erreurs de syntaxe, le navigateur Web affiche un message d'erreur. Corrigez les erreurs de code XML et revérifiez le fichier.

7 Sur le serveur Edge, ouvrez le fichier c:\breeze\edgeserver\win32\conf_defaultRoot__defaultVHost_\Vhost.xml. Localisez la balise `<RouteEntry></RouteEntry>` et remplacez-la par ce qui suit :

```
<RouteEntry protocol="rtmp">*:*;10.192.37.11:8506</RouteEntry>
```

Ce code a pour effet que le serveur Edge dirige les connexions RTMP des adresses IP et des ports vers le serveur d'origine via le port 8506. Cet exemple utilise l'adresse IP 10.192.37.11. Dans votre code, remplacez l'adresse IP du service d'application sur le serveur d'origine.

8 Enregistrez le fichier VHost.xml.

9 Ouvrez le fichier Vhost.xml dans un navigateur Web pour vérifier que le code XML est valide.

S'il contient des erreurs de syntaxe, le navigateur Web affiche un message d'erreur. Corrigez les erreurs de code XML et revérifiez le fichier.

10 Sur le serveur Edge, ouvrez le fichier c:\breeze\edgeserver\custom.ini.

11 Entrez le paramètre `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` et définissez-le sur l'adresse IP ou le nom de domaine pleinement qualifié du serveur d'origine, comme dans l'exemple suivant :

```
FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT=connect.yourcompany.com:443
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
FCS_EDGE_HOST=edge1.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=sanfran
FCS_EDGE_EXPIRY_TIME=60000
FCS_EDGE_REG_INTERVAL=30000
```

Si vous souhaitez configurer votre système pour se connecter via SSL uniquement, commentez le paramètre `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT` comme suit :

```
# FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

Remarque : *Si le serveur Edge a des difficultés à résoudre le nom de domaine pleinement qualifié du serveur d'origine, utilisez l'adresse IP.*

12 Sur le serveur Edge, ouvrez le fichier C:\breeze\edgeserver\win32\conf\HttpCache.xml et mettez à jour la balise `<HostName>` comme suit :

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

13 Enregistrez le fichier HttpCache.xml.

14 Ouvrez le fichier HttpCache.xml dans un navigateur Web pour vérifier que le code XML est valide.

S'il contient des erreurs de syntaxe, le navigateur Web affiche un message d'erreur. Corrigez les erreurs de code XML et revérifiez.

Configuration du serveur d'origine

1 Configurez le serveur d'origine pour SSL. Pour plus d'informations, reportez-vous à la section « Protocole SSL (Secure Sockets Layer) » à la page 49.

2 Sur le serveur d'origine, ouvrez le fichier c\breeze\custom.ini et entrez ce qui suit pour lier le serveur Edge au serveur d'origine :

`edge.FCS_EDGE_CLUSTER_ID=1`

Utilisez la valeur du paramètre `FCS_EDGE_CLUSTER_ID` défini dans le fichier custom.ini sur le serveur Edge. Dans cet exemple, la valeur est `sanfran`, le code est donc `edge.sanfran=1`.

Remarque : *La valeur 0 est réservée et ne peut pas être utilisée.*

3 Redémarrez Connect Pro Central Application Server et Connect Pro Meeting Server.

4 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Configurer Connect Pro Server 7 pour ouvrir la Console de gestion des applications. Effectuez les opérations suivantes :

a Cliquez sur Paramètres du serveur.

b La zone Nom externe contient le nom de domaine pleinement qualifié du serveur Edge et une zone vide à droite. Si le nom de domaine pleinement qualifié n'apparaît pas, patientez quelques minutes et actualisez le navigateur.

c Entrez le nom de domaine pleinement qualifié du serveur Edge dans la zone vide, puis cliquez sur Enregistrer. Le serveur Edge est alors enregistré sur le serveur d'origine.

5 Configurez le serveur DNS local pour diriger les utilisateurs vers le serveur Edge lorsqu'ils demandent une URL Acrobat Connect Pro.

Configuration du protocole SSL matériel pour un serveur Edge

Si le protocole SSL matériel est configuré sur le serveur d'origine, configurez l'authentification SSL matérielle pour chaque serveur Edge à sécuriser.

A l'instar d'un serveur d'origine, un serveur Edge comprend deux services : un service de réunion et un service d'application. Pour configurer SSL pour le service de réunion et le service d'application, il vous faut deux noms de domaine pleinement qualifiés et deux adresses IP. Vous pouvez partager le nom de domaine pleinement qualifié du service d'application avec le serveur d'origine, mais le service de réunion, en revanche, doit avoir son propre nom de domaine pleinement qualifié. Le nom de domaine pleinement qualifié du service d'application est l'URL avec laquelle les utilisateurs se connectent à leurs comptes Acrobat Connect Pro.

Par exemple, si vous avez un serveur Edge et un serveur d'origine, il vous faut trois noms de domaine pleinement qualifiés et trois certificats SSL : un pour chaque service de réunion et un pour les services d'application à partager. Il vous faut également quatre adresses IP : une pour chaque service de réunion et une pour chaque service d'application.

Dans cet exemple de configuration, le serveur d'origine a les adresses IP et les noms de domaine pleinement qualifiés suivants :

```
10.192.37.11 = connect.yourcompany.com
10.192.37.10 = meeting1.yourcompany.com
```

Le serveur Edge a les adresses IP et les noms de domaine pleinement qualifiés suivants :

```
10.192.37.100 = connect.yourcompany.com
10.192.37.101 = edge1.yourcompany.com
```

Remarque : *Si vous installez le serveur Edge et le serveur d'origine pour la première fois, configurez les deux serveurs sans SSL et vérifiez qu'ils parviennent à communiquer ensemble. Une fois que la communication est établie, vous pouvez configurer SSL pour les deux serveurs.*

Voir aussi

« Déploiement d'Acrobat Connect Pro Edge Server 7 » à la page 25

« A propos de la prise en charge SSL » à la page 49

Configuration du serveur Edge

1 Sur le serveur Edge, ouvrez le fichier c:\breeze\edgeserver\custom.ini.

2 Entrez le paramètre `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` et définissez-le sur l'adresse IP ou le nom de domaine pleinement qualifié du serveur d'origine, comme dans l'exemple suivant :

```
FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT=connect.yourcompany.com:443
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
FCS_EDGE_HOST=edge1.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=sanfran
FCS_EDGE_EXPIRY_TIME=60000
FCS_EDGE_REG_INTERVAL=30000
```

Si vous souhaitez configurer votre système pour se connecter via SSL uniquement, commentez le paramètre `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT` comme suit :

```
# FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

Remarque : *Si le serveur Edge a des difficultés à résoudre le nom de domaine pleinement qualifié du serveur d'origine, utilisez l'adresse IP.*

3 Sur le serveur Edge, ouvrez le fichier C:\breeze\edgeserver\win32\conf\HttpCache.xml et mettez à jour la balise `<HostName>` comme suit :

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

4 Enregistrez le fichier HttpCache.xml.

5 Ouvrez le fichier HttpCache.xml dans un navigateur Web pour vérifier que le code XML est valide.

S'il contient des erreurs de syntaxe, le navigateur Web affiche un message d'erreur. Corrigez les erreurs de code XML et revérifiez.

Configuration du serveur d'origine

1 Configurez le serveur d'origine pour SSL. Pour plus d'informations, reportez-vous à la section « Protocole SSL (Secure Sockets Layer) » à la page 49.

2 Sur le serveur d'origine, ouvrez le fichier c\breeze\custom.ini et entrez ce qui suit pour lier le serveur Edge au serveur d'origine :

```
edge.FCS_EDGE_CLUSTER_ID=1
```

Utilisez la valeur du paramètre *`FCS_EDGE_CLUSTER_ID`* défini dans le fichier custom.ini sur le serveur Edge. Dans cet exemple, la valeur est `sanfran`, le code est donc `edge.sanfran=1`.

Remarque : *La valeur 0 est réservée et ne peut pas être utilisée.*

3 Redémarrez Connect Pro Central Application Server et Connect Pro Meeting Server.

4 Sélectionnez Démarrer > Programmes > Adobe Acrobat Connect Pro Server 7 > Configurer Connect Pro Server 7 pour ouvrir la Console de gestion des applications. Effectuez les opérations suivantes :

a Cliquez sur Paramètres du serveur.

b La zone Nom externe contient le nom de domaine pleinement qualifié du serveur Edge et une zone vide à droite. Si le nom de domaine pleinement qualifié n'apparaît pas, patientez quelques minutes et actualisez le navigateur.

c Entrez le nom de domaine pleinement qualifié du serveur Edge dans la zone vide, puis cliquez sur Enregistrer. Le serveur Edge est alors enregistré sur le serveur d'origine.

5 Configurez le serveur DNS local pour diriger les utilisateurs vers le serveur Edge lorsqu'ils demandent une URL Acrobat Connect Pro.

Balises XML SSL

Balise	Valeur par défaut	Description
SSLCertificateFile	Aucune valeur par défaut.	Emplacement du fichier de certificat à envoyer au client. Lorsque aucun chemin absolu n'est spécifié, le certificat est supposé être situé dans le répertoire Adaptor.
SSLCertificateKeyFile	Aucune valeur par défaut.	Emplacement du fichier de la clé privée du certificat. Lorsque aucun chemin absolu n'est spécifié, le fichier de la clé est supposé être situé dans le répertoire Adaptor. Si le fichier de la clé est chiffré, la phrase secrète doit être spécifiée dans la balise SSLPassPhrase. L'attribut type indique le type de codage utilisé pour le fichier de clé du certificat. Il peut s'agir de PEM ou de ASN1 .
SSLCipherSuite	Voir la description.	Algorithme de chiffrement. L'algorithme est composé d'éléments séparés par des signes deux-points (:). Il peut s'agir d'algorithmes d'échange, de méthodes d'authentification, de méthodes de chiffrement, de types de résumés ou d'un nombre d'alias sélectionnés pour des regroupements courants. Pour obtenir la liste des composants, consultez la documentation de Flash Media Server. Cette balise présente le paramètre par défaut suivant : ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH Contactez l'assistance technique d'Adobe avant de modifier les paramètres par défaut.
SSLPassPhrase	Aucune valeur par défaut.	Phrase secrète à utiliser pour déchiffrer le fichier de la clé privée. Si le fichier de la clé privée n'est pas chiffré, laissez cette balise vide.
SSLSessionTimeout	5	Délai, en minutes, pendant lequel la session SSL demeure valide.

Paramètres de configuration SSL

Paramètre	Valeur par défaut	Description
ADMIN_PROTOCOL	http://	Protocole utilisé par le serveur d'applications. Défini sur https:// pour configurer SSL.
DEFAULT_FCS_HOSTPORT	:1935	Port utilisé par Flash Media Server pour communiquer via le protocole RTMP. Défini sur :-443,1935 pour configurer SSL.
HTTPS_PORT	Aucune valeur par défaut.	Port sur lequel le serveur d'applications écoute les requêtes HTTPS. Ce paramètre est généralement défini sur 443 ou sur 8443 pour configurer SSL.
SSL_ONLY	no	Défini sur yes si le serveur ne prend en charge que les connexions sécurisées. Ce paramètre implique que toutes les URL Acrobat Connect Pro utilisent le protocole HTTPS.
RTMP_SEQUENCE	Aucune valeur par défaut.	Ports et points d'origine et d'extrémité utilisés pour se connecter au Flash Media Server (serveur de réunions).

Infrastructure à clé publique (ICP)

A propos de l'infrastructure à clé publique (ICP)

Vous pouvez configurer une infrastructure à clé publique (ICP) pour gérer les informations d'identification dans le cadre de l'architecture de sécurité Acrobat Connect Pro de vos clients. Dans le protocole SSL plus répandu, l'identité du serveur est vérifiée auprès du client ; dans une infrastructure à clé publique, l'identité du client est vérifiée auprès du serveur.

Une tierce partie approuvée, appelée autorité de certification, vérifie l'identité d'un client et lui associe un certificat. Le certificat (également appelé *clé publique*) est au format X.509. Lorsque le client se connecte à Acrobat Connect Pro, un proxy négocie sa connexion pour l'infrastructure à clé publique. Si le client dispose d'un cookie issu d'une session précédente ou d'un certificat valide, il est connecté à Acrobat Connect Pro.

Pour plus d'informations sur l'infrastructure à clé publique, consultez le Centre de technologie ICP de Microsoft.

Configuration requise ICP

Les utilisateurs doivent exécuter Windows XP ou Windows 2003 et avoir installé sur leur ordinateur local un certificat de client valide avant d'accéder à une réunion requérant une authentification ICP. Lorsque l'utilisateur accède à une réunion, une boîte de dialogue lui demande de choisir un certificat de client valide parmi ceux qui sont installés sur son ordinateur.

Adobe recommande que les clients utilisent Adobe Acrobat Connect Add-in pour participer aux réunions requérant des authentifications avec clé publique. Les clients doivent installer l'Add-in à l'aide de son programme d'installation autonome avant d'accéder à la réunion.

Les clients peuvent également utiliser la dernière version de Flash Player dans le navigateur pour accéder aux réunions, mais la prise en charge des clés publiques par Flash Player n'est pas aussi étendue que celle de l'Add-in. Cependant, pour afficher les archives de réunions, les clients doivent avoir installé la dernière version de Flash Player.

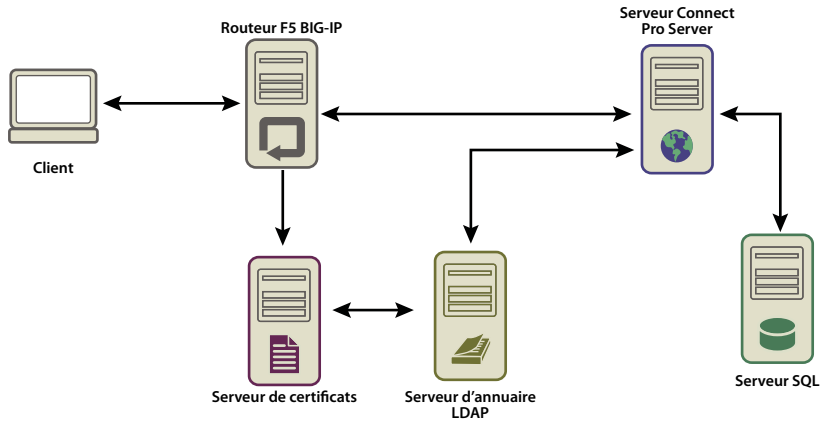
Vous pouvez concevoir un système ICP qui ne requiert que l'authentification des connexions HTTP ou des connexions HTTP et RTMP. Si vous exigez des certificats côté client pour les connexions HTTP et RTMP, le système interroge les utilisateurs à chaque nouvelle connexion au serveur. Par exemple, ils devront répondre à deux invites pour se connecter à une réunion, l'une pour HTTP et l'autre pour RTMP. La connexion RTMP ne pouvant pas être établie sans authentification HTTP, vous pouvez choisir d'exiger une authentification côté client uniquement pour la connexion HTTP.

Mise en œuvre de l'infrastructure à clé publique (ICP)

La procédure suivante vous guide tout au long de l'implémentation de l'infrastructure à clé publique (ICP) configurée avec un routeur F5 BIG-IP LTM 9.1.2 (version 40.2) comme proxy. Servez-vous des sections sensibles pour concevoir votre propre solution, avec un routeur F5 ou un autre périphérique.

Cette implémentation de référence respectent des normes de sécurité rigoureuses, par exemple, elle exige un certificat côté client pour les connexions HTTP (serveur d'applications) et RTMP (serveur de réunions).

Remarque : *Adobe vous recommande vivement d'adopter une stratégie de sécurité avant d'implémenter l'infrastructure à clé publique. Celle-ci exploite, en effet, un grand nombre de technologies différentes et le maintien de la sécurité est essentiel lors des interactions entre ces systèmes.*



Flux des données dans une infrastructure de clé publique

Cet exemple suppose la présence des éléments suivants :

- Acrobat Connect Pro est installé.

- Acrobat Connect Pro est intégré dans un service d'annuaire LDAP.
- Un utilisateur importé depuis le service d'annuaire LDAP peut accéder à une réunion de Acrobat Connect Pro.
- Un routeur F5 est installé.

1. Configurez le serveur d'annuaire LDAP.

Un attribut LDAP `email` doit être spécifié pour chaque utilisateur. Cet attribut est ajouté dans le champ objet du certificat du client.

F5 iRule recherche l'adresse électronique dans X.509::objet et ajoute la valeur dans l'en-tête HTTP. Acrobat Connect Pro utilise l'en-tête HTTP pour authentifier l'utilisateur.

Remarque : *Cet exemple utilise l'attribut* `email` *. Vous pouvez utiliser un identifiant unique quelconque au format X.509, d'une longueur maximale de 254 caractères et partagé par le service d'annuaire LDAP et Acrobat Connect Pro.*

2. Définissez la stratégie de connexion d'Acrobat Connect Pro.

Acrobat Connect Pro doit utiliser une adresse électronique comme identifiant de connexion de l'utilisateur. Dans Connect Pro Central, ouvrez l'onglet Administration, cliquez sur Utilisateurs et Groupes, puis sur Modifier les stratégies de nom d'utilisateur et de mot de passe.

3. Configurez un serveur d'autorité de certification.

Le serveur CA (Autorité de certification) traite les demandes de certificats, vérifie l'identité des clients, publie les certificats et gère la liste CRL (certificats révoqués).

Dans cette implémentation, le serveur CA s'adresse au serveur d'annuaire LDAP pour obtenir un certificat de client. Le serveur CA demande les informations du client au serveur LDAP et, si le client existe et n'a pas été révoqué, les met en forme dans un certificat.

Assurez-vous que le certificat du client soit installé et opérationnel en examinant le champ d'objet. Il doit se présenter comme suit :

```
E = adavis@asp.sflab.macromedia.com
CN = Andrew Davis
CN = Users
DC = asp
DC = sflab
DC = macromedia
DC = com
```

4. Configuration d'Acrobat Connect Pro pour qu'il utilise l'authentification des en-têtes HTTP

Dans le fichier *[rép_install_racine]*\appserv\conf\WEB-INF\web.xml, retirez les commentaires du code suivant :

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

Arrêtez le serveur de réunions et le serveur d'applications. Dans le fichier custom.ini du répertoire racine de l'installation, ajoutez la ligne suivante :

```
HTTP_AUTH_HEADER=hah_login
```

Enregistrez le fichier custom.ini et redémarrez Acrobat Connect Pro.

5. Configurez la logique applicative du routeur F5.

La logique applicative de F5 recherche l'adresse électronique dans le champ Objet du certificat du client. Elle transfère ensuite l'adresse électronique vers Acrobat Connect Pro dans un en-tête HTTP supplémentaire.

Les clients qui ne possèdent pas de certificat sont rejetés. Lorsqu'un client possède un certificat, celui-ci doit être authentifié. OCSP (Online Certification Status Protocol) et la recherche LDAP sont des exemples de mécanismes d'authentification.

Une fois le certificat authentifié, recherchez-y un identifiant unique connu d'Acrobat Connect Pro. Dans cet exemple, une adresse électronique est recherchée dans un certificat valide.

Une requête qui inclut la chaîne `session` ou qui contient un cookie `BREEZESESSION` peut être transmise sans authentification car le client a déjà été authentifié. (Acrobat Connect Pro vérifie ces arguments par une requête à la base de données.)

Si la requête n'inclut pas la chaîne `session` ou le cookie `BREEZESESSION`, l'utilisateur doit se connecter à Acrobat Connect Pro. Pour connecter un utilisateur, placez l'identifiant unique (en l'occurrence, l'adresse électronique) dans le champ `HTTP_AUTH_HEADER` et redirigez la requête vers la page de connexion d'Acrobat Connect Pro.

Le code suivant est un routeur F5 iRule placé dans le profil HTTPS qui gère les requêtes :

```
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]]
}
```

Voir aussi

« Démarrage et arrêt d'Acrobat Connect Pro Server 7 » à la page 18

Sécurisation de l'infrastructure

Sécurité du réseau

Pour ses communications, Acrobat Connect Pro s'appuie sur plusieurs services TCP/IP privés. Ces services ouvrent plusieurs ports et canaux qui doivent être protégés des utilisateurs extérieurs. Acrobat Connect Pro exige que vous placiez les ports sensibles derrière un pare-feu. Le pare-feu doit prendre en charge l'inspection de paquets avec état (pas seulement le filtrage des paquets). Une option du pare-feu doit permettre de « refuser tous les services par défaut à l'exception des services autorisés explicitement ». Le pare-feu doit être au moins un pare-feu à double interface (au moins deux interfaces réseau). Cette architecture permet d'éviter que des utilisateurs non autorisés ne contournent la sécurité du pare-feu.

La solution la plus simple pour sécuriser Acrobat Connect Pro consiste à bloquer tous les ports du serveur à l'exception des ports 80, 1935 et 443. Un pare-feu matériel externe offre un niveau de protection pour pallier les défectuosités du système d'exploitation. Vous pouvez configurer plusieurs couches de pare-feu matériel pour former des zones démilitarisées (DMZ). Si votre service informatique applique scrupuleusement tous les patchs de sécurité de Microsoft au serveur, il est possible de configurer un pare-feu logiciel pour assurer une sécurité supplémentaire.

Accès Intranet

Si certains de vos utilisateurs doivent accéder à Acrobat Connect Pro sur votre réseau Intranet, il est préférable de placer les serveurs Acrobat Connect Pro et leur base de données sur un sous-réseau distinct, isolé par un pare-feu. Le segment de réseau interne sur lequel est installé Acrobat Connect Pro doit utiliser des adresses IP privées (10.0.0.0/8, 172.16.0.0/12 ou 192.168.0.0/16) afin qu'il soit encore plus difficile pour un attaquant éventuel d'acheminer le trafic vers une adresse IP publique et depuis l'adresse IP réseau traduite en adresse IP interne. Pour plus d'informations, voir la rubrique RFC 1918. La configuration de ce pare-feu doit tenir compte de tous les ports d'Acrobat Connect Pro et de leur paramétrage pour un trafic entrant ou sortant.

Sécurité du serveur de base de données

Que vous hébergiez ou non votre base de données sur le même serveur qu'Acrobat Connect Pro, vous devez la protéger. Les ordinateurs hébergeant une base de données doivent être physiquement placés en un lieu protégé. Vous devez prendre les précautions supplémentaires suivantes :

- Installez la base de données dans la zone sécurisée de l'Intranet de votre société.
- Ne connectez jamais directement la base de données à Internet.
- Sauvegardez régulièrement toutes les données et stockez les copies dans un emplacement protégé hors site.
- Installez les derniers patchs publiés pour votre serveur de base de données.

Pour plus d'informations sur la sécurisation de SQL Server, rendez-vous sur le site Web consacré à la sécurité de Microsoft SQL.

Création de comptes de service

La création d'un compte de service pour Acrobat Connect Pro vous permet d'exécuter Acrobat Connect Pro de façon plus sécurisée. Adobe recommande de créer un compte de service et un compte de service MSDE pour Acrobat Connect Pro. Pour plus d'informations, consultez les articles de Microsoft « Comment faire pour modifier le compte de service de SQL Server ou de l'Agent SQL Server sans utiliser SQL Enterprise Manager dans SQL Server 2000 ou le Gestionnaire de configuration SQL Server dans SQL Server 2005 » et « Le guide de la planification de la sécurité des services et des comptes de service ».

Création d'un compte de service

1 Créez un compte local appelé ConnectService et ne comprenant aucun groupe par défaut.

2 Définissez les services Adobe Connect Enterprise Server, Flash Media Administration Server et Flash Media Server (FMS) sur ce nouveau compte.

3 Définissez un « Contrôle total » pour la clé de registre suivante :

`HKLM\SYSTEM\ControlSet001\Control\MediaProperties\PrivateProperties\Joystick\Winmm`

4 Définissez un « Contrôle total » sur les dossiers NTFS du chemin du dossier racine d'Acrobat Connect Pro (C:\breeze, par défaut).

Les sous-dossiers et les fichiers doivent disposer des mêmes autorisations. Dans le cas de clusters, modifiez les chemins correspondants sur chaque nœud d'ordinateur.

5 Définissez les droits de connexion suivants pour le compte ConnectService :

Ouvrir une session en tant que service—SeServiceLogonRight

Création d'un compte de service MSDE

1 Créez un compte local appelé ConnectSqlService et ne comprenant aucun groupe par défaut.

2 Remplacez le compte de service MSDE LocalSystem par ConnectSqlService.

3 Définissez un « Contrôle total » de ConnectSqlService pour les clés de registre suivantes :

```
HKEY_LOCAL_MACHINE\Software\Clients\Mail
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\80
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\[databaseInstanceName]
```

Pour les clusters, suivez cette procédure pour chaque nœud du cluster. L'autorisation Contrôle total s'applique à toutes les clés enfants d'une instance de base de données nommée.

4 Définissez un « Contrôle total » de ConnectSqlService pour les dossiers de la base de données. Les sous-dossiers et les fichiers doivent également disposer des mêmes autorisations. Dans le cas de clusters, modifiez les chemins correspondants sur chaque nœud d'ordinateur.

5 Définissez les droits d'utilisateur suivants pour le service ConnectSqlService :

Agir comme faisant partie du système d'exploitation—SeTcbPrivilege Outrepasser le contrôle de parcours—SeChangeNotify Verrouiller les pages en mémoire—SeLockMemory Ouvrir une session en tant que tâche—SeBatchLogonRight Ouvrir une session en tant que service—SeServiceLogonRight Remplacer un jeton au niveau du processus—SeAssignPrimaryTokenPrivilege

Sécurisation des installations à serveur unique

La procédure suivante résume le processus de configuration et de sécurisation d'Acrobat Connect Pro sur un ordinateur unique. Elle part du principe que la base de données est installée sur le même ordinateur et que les utilisateurs accèdent à Acrobat Connect Pro via Internet.

1. Installez un pare-feu.

Si vous autorisez les utilisateurs à se connecter à Acrobat Connect Pro via Internet, le serveur est à la merci des pirates informatiques. Un pare-feu vous permettra de bloquer l'accès au serveur et de contrôler les communications entre celui-ci et Internet.

2. Configurez le pare-feu.

Après avoir installé votre pare-feu, configurez-le comme suit :

- Ports d'entrée (depuis Internet) : 80, 443, 1935.
- Ports de sortie (vers le serveur de messagerie) : 25.
- Utilisez le protocole TCP/IP uniquement.

La base de données étant située sur le même serveur qu'Acrobat Connect Pro, il n'est pas nécessaire d'ouvrir le port 1434 sur le pare-feu.

3. Installez Acrobat Connect Pro.

4. Vérifiez le bon fonctionnement des applications Acrobat Connect Pro.

Après avoir installé Acrobat Connect Pro, vérifiez qu'il fonctionne correctement depuis Internet et depuis votre réseau local.

5. Testez le pare-feu.

Une fois que vous avez installé et configuré le pare-feu, vérifiez qu'il fonctionne correctement. Testez le pare-feu en tentant d'utiliser les ports bloqués.

Sécurisation des clusters

Les systèmes de clusters (multi-serveurs) sont par nature plus complexes que les configurations à serveur unique. Un cluster Acrobat Connect Pro peut être situé dans un centre de données ou réparti géographiquement dans plusieurs centres d'exploitation du réseau. Vous pouvez installer et configurer les serveurs qui hébergent Connect Pro dans plusieurs sites et les synchroniser par l'intermédiaire d'une réplication de la base de données.

Remarque : *Les clusters doivent utiliser Microsoft SQL Server, et non·le moteur de base de données intégré.*

Conseils importants pour la sécurisation des clusters :

Réseaux privés La solution la plus simple pour les clusters situés sur le même site consiste à créer un sous-réseau supplémentaire pour le système Acrobat Connect Pro. Cette méthode offre un haut niveau de sécurité.

Pare-feux logiciels locaux Pour les serveurs Acrobat Connect Pro situés dans un cluster, mais partageant un réseau public avec d'autres serveurs, un pare-feu logiciel installé sur chaque serveur peut être approprié.

Systèmes VPN Dans les installations multi-serveurs hébergeant Acrobat Connect Pro dans des sites différents, vous pouvez envisager d'utiliser un canal chiffré pour communiquer avec les serveurs distants. De nombreux fournisseurs proposent des technologies VPN permettant de sécuriser les communications avec les serveurs distants. Si le trafic des données doit être chiffré, Acrobat Connect Pro s'appuie sur cette sécurité externe.

Ressources et conseils en matière de sécurité

Recommandations en matière de sécurité

La liste de contrôle suivante propose des recommandations pour la sécurisation de votre système Acrobat Connect Pro.

Protéger le trafic réseau par SSL Vous pouvez sécuriser la connexion avec le serveur de réunions, le serveur d'applications ou les deux.

Exécuter les services nécessaires uniquement N'exécutez pas d'applications, telles qu'un contrôleur de domaine, un serveur Web ou un serveur FTP, sur le même ordinateur qu'Acrobat Connect Pro. Pour minimiser les risques qu'une autre application soit utilisée pour compromettre le serveur, réduisez le nombre d'applications et de services exécutés sur l'ordinateur qui héberge Acrobat Connect Pro.

Mettre à jour la sécurité du système d'exploitation Vérifiez régulièrement la publication de mises à jour critiques corrigeant des failles de sécurité et appliquez les correctifs requis. Un pare-feu élimine certains de ces problèmes de sécurité. De façon générale, il est préférable d'appliquer à vos serveurs tous les correctifs de sécurité publiés et approuvés par Microsoft et les fournisseurs des autres plates-formes concernées.

Sécuriser les systèmes hôtes Si vous stockez des informations « sensibles » sur vos serveurs, veillez à la protection physique de vos systèmes. Acrobat Connect Pro dépend de la sécurisation de l'ordinateur hôte. Les serveurs doivent donc être protégés contre les intrusions s'ils contiennent des données personnelles et confidentielles. Acrobat Connect Pro est conçu pour tirer parti des fonctionnalités natives de l'environnement, telles que le chiffrement du système de fichiers.

Utiliser des mots de passe difficiles à déchiffrer Des mots de passe difficiles à déchiffrer protègent les données. Les administrateurs d'Acrobat Connect Pro peuvent définir des stratégies de mot de passe et de connexion dans Connect Pro Central. Les installations Acrobat Connect Pro utilisent souvent Microsoft SQL Server, qui requiert également une protection par des mots de passe difficiles à déchiffrer.

Effectuer des audits de la sécurité réguliers Il est recommandé d'effectuer régulièrement des audits des systèmes informatiques pour vérifier que toutes les mesures de sécurité prises fonctionnent comme prévu. Vous pouvez par exemple tester un pare-feu à l'aide d'un scanner de ports.

Références et ressources sur la sécurité

Les ressources suivantes peuvent vous aider à sécuriser vos serveurs.

Sécurisation du réseau L'Institut SANS (System Administration, Networking, and Security) est une organisation de coopération à vocation de recherche et de formation, constituée d'administrateurs système, de professionnels de la sécurité et d'administrateurs réseau. Cet institut propose des cours sur la sécurité des réseaux, ainsi qu'une certification en sécurité réseau.

Sécurisation de SQL Server La page relative aux ressources de sécurité Microsoft SQL du site Web de Microsoft fournit des informations sur la sécurisation de SQL Server. Ces informations s'appliquent également au moteur de base de données intégré installé avec Connect Enterprise.

Outils NMap est une puissante application de scanner qui signale tous les ports ouverts sur un ordinateur. Il est disponible gratuitement au titre de la licence publique GNU (GPL).

Remarque : *L'efficacité de toute mesure de sécurité dépend de nombreux facteurs, tels que les fonctions de sécurité assurées par le serveur et les logiciels de sécurité que vous avez installés. Le logiciel Acrobat Connect Pro n'est pas conçu pour assurer la sécurité de votre serveur et des informations qu'il renferme. Pour plus d'informations, consultez l'avis d'exonération de responsabilité de garantie, dans le contrat de licence applicable fourni avec Acrobat Connect Pro.*

Index