

# ADOBE® CONNECT™ ENTERPRISE SERVER 6

GUIDE D'INSTALLATION ET DE CONFIGURATION



© 2006 Adobe Systems Incorporated. Tous droits réservés.

Guide d'installation et de configuration d'Adobe® Connect™ Enterprise Server 6 pour Windows® et Macintosh

Si le présent guide est fourni avec un logiciel régi par un contrat d'utilisateur final, ce guide, ainsi que le logiciel décrit, sont fournis sous licence et peuvent être utilisés ou copiés uniquement selon les clauses et conditions de la licence. A moins d'une autorisation expresse accordée par cette licence, aucune partie de ce guide ne peut être reproduite, stockée dans un système d'interrogation ou transmise, sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, par enregistrement ou autre) sans l'autorisation écrite préalable d'Adobe Systems Incorporated. Veuillez noter que le contenu du présent guide est protégé par la loi sur les droits d'auteur, même s'il n'est pas distribué avec un logiciel régi par un contrat de licence utilisateur.

Les informations contenues dans ce guide sont fournies à titre purement informatif ; elles sont susceptibles d'être modifiées sans préavis et ne doivent pas être interprétées comme étant un engagement de la part d'Adobe Systems Incorporated. Adobe Systems Incorporated n'accepte aucune responsabilité quant aux erreurs ou inexactitudes pouvant être contenues dans le présent guide.

Veuillez noter que les illustrations et images existantes que vous souhaitez éventuellement inclure dans votre projet sont susceptibles d'être protégées par les lois sur les droits d'auteur. L'inclusion non autorisée de tels éléments dans vos nouveaux travaux peut constituer une violation des droits du propriétaire. Veuillez vous assurer que vous obtenez toute autorisation nécessaire auprès du détenteur du copyright.

Toute référence à des noms de sociétés dans les modèles types n'est utilisée qu'à titre d'exemple et ne fait référence à aucune société réelle.

Adobe, le logo Adobe, Acrobat, Adobe Connect, Adobe Press, Breeze, Flash Media Server, Flash Player et JRun sont des marques commerciales ou des marques déposées d'Adobe Systems Incorporated aux Etats-Unis et/ou dans d'autres pays.

IBM est une marque commerciale d'International Business Machines Corporation aux Etats-Unis, dans d'autres pays, ou les deux. Linux est une marque déposée de Linus Torvalds aux Etats-Unis et dans d'autres pays. Macintosh est une marque commerciale d'Apple Computer, Inc., déposée aux Etats-Unis et dans d'autres pays. Microsoft, Windows et Windows Server sont des marques commerciales ou des marques déposées de Microsoft Corporation aux Etats-Unis et/ou dans d'autres pays. Solaris et Sun sont des marques commerciales ou déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. UNIX est une marque déposée de The Open Group aux Etats-Unis et dans d'autres pays. Toutes les autres marques citées appartiennent à leurs propriétaires respectifs.

A l'attention des utilisateurs du Gouvernement des Etats-Unis : Ce logiciel et sa documentation sont des « articles commerciaux », conformément à la définition de ce terme dans le document 48 C.F.R. §2.101, comprenant d'une part un « logiciel informatique commercial » et d'autre part une « documentation de logiciel informatique commercial », conformément à la définition de ces termes dans le document 48 C.F.R. §12.212 ou 48 C.F.R. §227.7202, si approprié. Conformément aux documents 48 C.F.R. §12.212 ou 48 C.F.R. §§227.7202-1 à 227.7202-4, si approprié, le logiciel informatique commercial et la documentation de logiciel informatique commercial sont accordés sous licence aux utilisateurs du Gouvernement des Etats-Unis (a) uniquement en tant que produits commerciaux et (b) uniquement avec les droits accordés à tous les autres utilisateurs selon les termes et conditions mentionnés dans le présent contrat. Droits non publiés réservés dans le cadre des lois sur les droits d'auteur en vigueur aux Etats-Unis. Adobe s'engage à respecter la législation relative à l'égalité des chances y compris, le cas échéant, les dispositions du décret 11246, tel qu'amendé, à la section 402 de la loi sur l'assistance aux vétérans du Vietnam (Vietnam Era Veterans Readjustment Assistance Act) de 1974 (38 USC 4212), et à la section 503 de la loi sur la réadaptation (Rehabilitation Act) de 1973, telle qu'amendée, et la réglementation des articles 41 CFR, alinéas 60-1 à 60-60, 60-250 et 60-741. La clause relative à l'égalité des chances et les règlements énoncés dans la phrase précédente doivent être compris comme tels lorsqu'il y est fait référence.

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

# Sommaire

## Chapitre 1 : Avant de commencer

Présentation de la documentation .....	1
Ressources .....	2

## Chapitre 2 : Préparation de l'installation et de la configuration

Configuration requise pour l'installation .....	4
Configurations prises en charge .....	6
Préparation de la mise à niveau .....	7
Préparation de l'installation .....	10

## Chapitre 3 : Installation et mise à niveau Connect Enterprise

Installation de Connect Enterprise Server 6 .....	17
Installation de Connect Edge Server 6 .....	21

## Chapitre 4 : Déploiement et configuration de Connect Enterprise

Déploiement de Connect Enterprise Server 6 .....	24
Déploiement de Connect Edge Server 6 .....	25
Intégration de Connect Enterprise dans un service d'annuaire .....	27
Configuration du stockage partagé .....	35

## Chapitre 5 : Configuration des fonctions avancées

Authentification unique .....	38
Infrastructure de clé publique (PKI) .....	42
Hébergement d'Acrobat Connect Add-in .....	45
Tampons de tableau blanc personnalisés .....	46

## Chapitre 6 : Vérification de votre installation

Tâches de vérification de l'installation .....	47
--	----

## Chapitre 7 : Sécurisation de Connect Enterprise

Sécurisation de l'infrastructure .....	52
Sécurisation de Connect Enterprise Server .....	53
Ressources et conseils en matière de sécurité .....	55

Index .....	56
-------------	----

# Chapitre 1 : Avant de commencer

Ce chapitre fournit des informations sur la documentation, présente les nouveautés d'Adobe® Connect™ Enterprise Server 6 et vous explique où trouver des informations et une assistance supplémentaires.

## Présentation de la documentation

### Utilisateurs concernés

Ce manuel est destiné aux professionnels de l'informatique qui installent et configurent un système Adobe Connect Enterprise pour leur organisation.

### Nouveautés

Les fonctions suivantes sont des nouveautés d'Adobe Connect Enterprise 6 et d'Adobe Connect Edge Server 6.

**Stockage partagé** Configurez Connect Enterprise pour partager du contenu stocké à travers de nombreux périphériques NAS (Network Attached Storage) et SAN (Storage Area Network). Au fur et à mesure de la croissance du contenu et de la base d'utilisateurs de l'organisation, utilisez un stockage partagé pour ajuster et gérer votre système Connect Enterprise.

Vous pouvez choisir de faire entre une copie miroir du contenu dans Connect Enterprise Server ou stocker l'ensemble du contenu sur des périphériques externes et mettre le contenu actif en cache sur le serveur. Lorsqu'il n'est plus utilisé, le contenu est purgé du serveur. Pour plus d'informations, consultez la section « Configuration du stockage partagé » à la page 35.

**Infrastructure de clé publique (PKI)** Adobe® Acrobat® Connect™ Add-in prend en charge les certificats de client. Cette prise en charge vous permet d'implémenter une infrastructure de clé publique (PKI) pour renforcer la sécurité de votre réseau. Pour plus d'informations, consultez la section « Infrastructure de clé publique (PKI) » à la page 42.

**Pagination des requêtes LDAP** Spécifiez une taille de page pour recevoir les résultats des requêtes de protocole LDAP (Lightweight Directory Access Protocol) afin de pouvoir importer tous les utilisateurs dans votre annuaire. Pour plus d'informations, consultez la section « Intégration de Connect Enterprise dans un annuaire LDAP » à la page 29.

**Sécurisation de LDAP** Synchronisez Connect Enterprise 6 avec un serveur d'annuaire LDAP via le protocole LDAPS (Lightweight Directory Access Protocol) sécurisé. Pour plus d'informations, consultez la section « Configuration LDAPS » à la page 35.

**Mise en cluster d'Edge Server** Déployez Adobe Connect Edge Server dans un cluster afin d'assurer une plus grande évolutivité et une meilleure redondance du système. Les serveurs Edge consolident les flux, mettent le contenu en cache et offrent davantage de contrôle sur la circulation des informations. Pour plus d'informations, consultez la section « Choix du déploiement des serveurs Edge » à la page 15.

**Prise en charge des systèmes d'exploitation 64 bits** Connect Enterprise 6 assure la prise en charge de Windows Server® 2003 64 bits.

**Prise en charge SSL native** Dans les versions précédentes, les connexions sécurisées à Adobe® Breeze® passaient par un tunnelage. La prise en charge native de SSL (Secure Sockets Layer) améliore les performances réseau et réduit les délais de connexion. Pour plus d'informations, visitez la page [www.adobe.com/go/connect\\_ssl\\_fr](http://www.adobe.com/go/connect_ssl_fr).

**Tampons de tableau blanc personnalisés** Vous pouvez créer vos propres tampons personnalisés et les inclure dans les outils de dessin du Tableau blanc d'Adobe Acrobat Connect Professional. Pour plus d'informations, consultez la section « Tampons de tableau blanc personnalisés » à la page 46.

**Hébergement de l'extension Adobe Acrobat Connect Add-in** Acrobat Connect Add-in est téléchargé de manière transparente à partir des serveurs d'Adobe lorsqu'un client en a besoin dans une réunion. Toutefois, si la stratégie de

sécurité de votre organisation interdit les téléchargements externes, vous pouvez héberger Acrobat Connect Add-in sur vos propres serveurs. Pour plus d'informations, consultez la section « Hébergement d'Acrobat Connect Add-in » à la page 45.

## Utilisation de ce manuel

Ce manuel comprend les six chapitres suivants :

« **Avant de commencer** » Liste des nouveautés, des ressources disponibles sur le Web et des coordonnées du support technique d'Adobe.

« **Préparation de l'installation et de la configuration** » Configurations système, présentation technique de Connect Enterprise et informations qui vous aideront à intégrer Connect Enterprise aux ressources existantes de votre organisation. Si vous connaissez déjà les composants et les fonctionnalités facultatives de Connect Enterprise, vous pouvez vous contenter de lire le chapitre consacré à la configuration système, puis passer directement aux instructions d'installation.

« **Installation et mise à niveau de Connect Enterprise** » Instructions d'installation de Connect Enterprise Server et Connect Edge Server.

« **Déploiement et configuration de Connect Enterprise** » Procédures de déploiement de Connect Enterprise Server et Connect Edge Server, pour la configuration de fonctions facultatives, telles que le stockage de contenu externe, et l'intégration de Connect Enterprise à un service d'annuaire.

« **Configuration des fonctions avancées** » Procédure d'hébergement d'Acrobat Connect Add-in sur votre propre serveur, implémentation d'une infrastructure de clé publique (PKI), configuration d'une authentification unique et création de tampons de tableau blanc personnalisés.

« **Vérification de votre installation** » Procédure permettant de vérifier le bon fonctionnement de tous les composants de votre système.

« **Sécurisation de Connect Enterprise** » Informations relatives à la sécurisation de votre réseau, de la base de données et de Connect Enterprise Server.

## Ressources

### Adobe.fr

Ces ressources sont disponibles sur le site Web d'Adobe ([www.adobe.fr](http://www.adobe.fr)):

**Pôle de création Adobe** Propose des articles, des astuces et des didacticiels dans divers formats (vidéo, Adobe PDF et HTML, entre autres). Créé par des experts du domaine, des concepteurs et les partenaires de publication Adobe, le contenu est mis à jour chaque mois. Vous pourrez également accéder au Adobe® Studio® Exchange, où les utilisateurs téléchargent et partagent gratuitement des milliers d'actions, des modules externes et d'autres éléments de contenu. Le Pôle de création Adobe est disponible en anglais, français, allemand et japonais.

**Centre des développeurs Adobe** Fournit des informations destinées aux utilisateurs avancés, notamment aux développeurs de logiciels et de modules externes. Vous y trouverez des didacticiels, des kits de développement de logiciels et des échantillons de code, mais aussi des forums, des fils RSS, des séminaires en ligne et d'autres ressources techniques.

**Support - Accueil** Contient des informations sur les options de support technique gratuites et payantes. Les principaux problèmes sont énumérés par produit dans les sites Web américain et japonais d'Adobe. Suivez le lien Formation pour accéder aux livres Adobe Press, aux ressources de formation vidéo et en ligne dirigées par un instructeur, aux programmes de certification logicielle d'Adobe, etc.

**Téléchargements** Propose des mises à jour gratuites, des versions d'évaluation et d'autres logiciels utiles. La section Plugins du magasin d'Adobe permet d'accéder à des milliers de modules issus de développeurs tiers, qui vous aideront à automatiser vos tâches, à personnaliser vos flux de travail, à créer des effets professionnels spéciaux, etc.

**Communautés** Propose des forums, des blogs et d'autres lieux de rencontre dans lesquels les utilisateurs peuvent partager technologies, outils et informations, poser des questions et découvrir d'autres moyens d'exploiter leurs logiciels au maximum. Les forums utilisateur sont disponibles en anglais, français, allemand et japonais ; les blogs sont rédigés dans un large éventail de langues.

### **Contactez l'assistance technique**

En cas de résultats inattendus après l'installation de Connect Enterprise Server ou Connect Edge Server sur un serveur unique ou dans un cluster de serveurs, ou pour obtenir de l'aide sur la configuration du serveur, contactez l'assistance technique à l'adresse [www.adobe.com/go/connect\\_licensed\\_programs\\_fr](http://www.adobe.com/go/connect_licensed_programs_fr).

# Chapitre 2 : Préparation de l'installation et de la configuration

Lorsque vous vous préparez à concevoir et à installer un système Connect Enterprise, vérifiez les conditions d'installations requises, les configurations prises en charge et la présentation technique. Si vous effectuez une mise à niveau vers Adobe Connect Enterprise Server 6, suivez les instructions pour sauvegarder les fichiers et migrer vers un système plus avancé.

## Configuration requise pour l'installation

### Configuration matérielle requise pour Connect Enterprise Server

Composant	Configuration requise
Processeur du serveur	Dual Xeon, 3 Ghz ou supérieur (recommandé) Pentium 4, 2 Ghz (minimum)
Mémoire	4 Go de RAM (recommandé)
Disque dur	+ de 100 Go recommandé Répartition : 1 Go pour l'installation 10 Go par lot de 100 présentations 80 Go minimum d'espace disque pour le stockage du contenu (l'espace nécessaire augmente au fur et à mesure de la croissance du contenu)
Connexion réseau	100 Mbits minimum
Lecteur	CD-ROM ou DVD-ROM
Autres	Pour activer SSL, vous devez utiliser un accélérateur matériel SSL ou le logiciel SSL natif. Pour plus d'informations, visitez la page <a href="http://www.adobe.com/go/connect_ssl_fr">www.adobe.com/go/connect_ssl_fr</a> .  Pour équilibrer la charge d'un cluster, vous devez disposer d'un matériel d'équilibrage de charge, tel que BIG-IP de F5 ou Network Load Balancing (NLB) de Microsoft.  Connect Enterprise Server requiert un serveur dédié.  L'ordinateur qui héberge Connect Enterprise Server et celui qui héberge SQL Server doivent être synchronisés sur la même source horaire. Consultez les articles Microsoft « How to configure an authoritative time server in Windows 2000 » et « How to configure an authoritative time server in Windows Server 2003 ».

Pour connaître les recommandations et les configurations système requises pour Connect Enterprise Server, consultez la page Web [www.adobe.com/go/connect\\_sysreqs\\_fr](http://www.adobe.com/go/connect_sysreqs_fr).

## Configuration logicielle requise pour Connect Enterprise Server

Composant	Configuration requise
Système d'exploitation	Microsoft Windows Server 2000 ou Microsoft Windows Server 2003
Bases de données	SQL Server 2000 SP4 (version anglaise) ou SQL Server 2005 SP1 (version anglaise) ou le moteur de base de données intégré MSDE (fourni avec Connect Enterprise Server)
Serveur de messagerie SMTP	Le serveur SMTP peut être sur le même ordinateur ou peut être relayé sur un autre ordinateur, tel qu'un serveur sendmail UNIX® ou un serveur Microsoft Exchange. Il est utilisé pour envoyer des notifications par messagerie. Un serveur SMTP n'est pas obligatoire, mais une adresse électronique système et une adresse électronique d'assistance technique sont nécessaires.
Système de fichiers	Système de fichiers NTFS
Serveur Web	Connect Enterprise Server possède son propre serveur Web ; aucun autre serveur Web (tel qu'Apache) ne peut être utilisé avec Connect. Adobe recommande de désactiver le service de serveur Web IIS, car Connect utilise le port IIS.
Autres	Un antivirus fonctionnant en temps réel ne peut pas être installé sur le serveur.

### Voir aussi

« Choix d'une base de données » à la page 14

## Configuration utilisateur requise pour Connect Enterprise Server

Pour connaître la configuration utilisateur requise pour Adobe Connect Enterprise Server 6, visitez la page [www.adobe.com/go/connect\\_sysreqs\\_fr](http://www.adobe.com/go/connect_sysreqs_fr).

## Configuration de ports requise pour Connect Enterprise Server

Ce tableau 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

Ce tableau décrit les ports ouverts à l'intérieur d'un cluster. Chaque serveur Connect Enterprise 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 Connect Enterprise 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

Ce tableau présente les ports du serveur utilisés par Connect Enterprise pour communiquer en interne. Ces ports ne doivent pas être utilisés sur un serveur qui héberge Connect Enterprise sinon ce dernier peut 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

## Configuration matérielle requise pour Connect Edge Server

Pour connaître la configuration système requise pour Adobe Connect Edge Server 6, visitez la page [www.adobe.com/go/connect\\_sysreqs\\_fr](http://www.adobe.com/go/connect_sysreqs_fr).

# Configurations prises en charge

## Configurations de bases de données/serveur prises en charge

Connect Enterprise Server stocke les informations sur les utilisateurs et le contenu dans une base de données. Voici les configurations de Connect Enterprise Server et de bases de données prises en charge :

**Serveur unique avec moteur de base de données intégré** Installez Connect Enterprise Server sur un ordinateur et installez le moteur de base de données intégré (inclus dans le programme d'installation de Connect Enterprise Server) sur ce même ordinateur.

**Serveur unique avec base de données SQL Server** Installez Connect Enterprise Server sur un ordinateur, puis SQL Server 2000 ou SQL Server 2005 sur ce même ordinateur.

**Serveur unique avec base de données SQL Server externe** Installez Connect Enterprise Server sur un ordinateur, puis SQL Server 2000 ou SQL Server 2005 sur un autre ordinateur.

**Serveur unique avec bases de données SQL Server multiples externes** Installez Connect Enterprise Server sur un ordinateur unique et installez SQL Server 2000 ou SQL Server 2005 sur plusieurs ordinateurs externes (également appelés cluster) à Connect Enterprise Server.

**Serveurs multiples avec base de données SQL Server externe** Installez Connect Enterprise Server sur plusieurs serveurs (également appelés cluster), puis SQL Server 2000 ou SQL Server 2005 sur un autre ordinateur.

**Serveurs multiples avec bases de données SQL Server externes** Installez Connect Enterprise Server sur plusieurs serveurs (également appelés cluster), puis SQL Server 2000 ou SQL Server 2005 sur un autre cluster.

*Remarque : Microsoft SQL Server n'est pas fourni avec Connect Enterprise Server 6 et doit être acheté séparément.*

## Voir aussi

« Préparation de l'installation » à la page 10

« Installation de Connect Enterprise Server 6 » à la page 17

## Serveurs d'annuaire LDAP pris en charge

Vous pouvez importer les informations de l'annuaire dans Connect Enterprise depuis le serveur d'annuaire LDAP de votre organisation. Les serveurs d'annuaire LDAP suivants sont pris en charge pour une intégration avec Connect Enterprise :

- Active Directory Application Mode SP1 (ADAM)
- Active Directory (Windows Server 2000 et Windows Server 2003)
- IBM® 5.2
- Novell eDirectory 8.7.3 pour Win32
- OpenLDAP 2.3.19
- Sun™ Directory Server 5.2 pour Win32
- Netscape 6.02 pour Win32

### Voir aussi

« Intégration de Connect Enterprise dans un service d'annuaire » à la page 27

## Solutions d'authentification unique prises en charge

Vous pouvez configurer votre système Connect Enterprise pour qu'il fonctionne avec une authentification unique. L'authentification unique permet aux utilisateurs connectés au réseau de votre organisation d'utiliser d'autres ressources, y compris Connect Enterprise, sans devoir se connecter à nouveau. Connect Enterprise prend en charge les solutions d'authentification unique suivantes :

- Authentification des en-têtes HTTP
- Authentification Windows NT Lan Manager (NTLM)

### Voir aussi

« Authentification unique » à la page 38

## Périphériques de stockage de contenu pris en charge

Vous pouvez configurer votre système Connect Enterprise 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](http://www.adobe.com/go/connect_sysreqs_fr).

### Voir aussi

« Configuration du stockage partagé » à la page 35

# Préparation de la mise à niveau

## Chemins de mise à niveau

Les interfaces utilisateur graphiques du programme d'installation de Connect Enterprise Server et de la Console de gestion des applications vous guident tout au long de la mise à niveau. Les chemins de mise à niveau suivants sont pris en charge :

**5.1 vers 6.0** Exécutez le programme d'installation d'Adobe Connect Enterprise 6.0.

**5.0 vers 6.0** Exécutez le programme d'installation d'Adobe Connect Enterprise 6.0.

**4.1 vers 6.0** Exécutez le programme d'installation d'Adobe Connect Enterprise 6.0 et suivez les instructions relatives au chemin de mise à niveau 4.1.

**3.0.7 vers 6.0** Consultez la section Upgrade Documentation du Centre d'assistance Connect Enterprise sous licence ([www.adobe.com/go/connect\\_licensed\\_support\\_fr](http://www.adobe.com/go/connect_licensed_support_fr)) pour effectuer une mise à niveau vers 4.1, puis suivez le chemin de mise à niveau de 4.1 vers 6.0.

Pour plus d'informations sur la mise à niveau, contactez l'assistance d'Adobe : [www.adobe.com/go/connect\\_licensed\\_programs\\_fr](http://www.adobe.com/go/connect_licensed_programs_fr).

## Mise à niveau de Breeze vers Connect Enterprise

Pour effectuer une mise à niveau de Breeze vers Adobe Connect Enterprise Server 6, procédez comme suit.

### 1. Testez la mise à niveau 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 mise à niveau dans un environnement de test avant de mettre à niveau l'environnement de production. Lorsque vous avez réussi la mise à niveau dans l'environnement test, passez à l'étape 2.

### 2. Informez les utilisateurs de la mise à niveau.

Voir la section « Information des utilisateurs quant à la mise à niveau » à la page 9.

### 3. Arrêtez Connect Enterprise Server et sauvegardez les fichiers.

Voir la section « Sauvegarde des fichiers » à la page 9.

### 4. Sauvegardez la base de données.

Voir la section « Sauvegarde de la base de données » à la page 9.

### 5. Exécutez le programme d'installation d'Adobe Connect Enterprise Server 6.

Voir la section « Installation de Connect Enterprise Server 6 » à la page 17.

### 6. Configurez Connect Enterprise Server.

Voir la section « Configuration de Connect Enterprise Server à l'aide de l'Assistant de la Console de gestion des applications » à la page 18.

### 7. Vérification de l'installation

Voir la section « Vérification de votre installation » à la page 47.

## Mise à niveau de la base de données intégrée vers SQL Server

Procédez comme suit pour effectuer une mise à niveau et passer de l'utilisation de la base de données intégrée à celle de SQL Server sur un ordinateur différent.

### 1. Installez SQL Server.

Suivez les instructions fournies par Microsoft pour installer le serveur SQL.

### 2. Sauvegarde de la base de données intégrée

Voir la section « Sauvegarde de la base de données » à la page 9.

### 3. Copiez le fichier .bak du serveur Breeze sur le serveur qui héberge SQL Server.

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

### 4. Restaurez la base de données sur le serveur hébergeant SQL Server.

Pour plus d'informations sur la restauration 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.

Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Configurer Adobe Connect Enterprise Server.

### Information des utilisateurs quant à la mise à niveau

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 mise à niveau ou l'ajout de modules à votre installation Connect Enterprise Server, Adobe vous suggère d'effectuer les opérations suivantes :

- Prévoyez suffisamment de temps pour assurer une mise à niveau 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 Connect Enterprise pendant la mise à niveau.
- Informez-les également des types de changements auxquels ils doivent s'attendre (nouvelles fonctionnalités ou meilleures performances, par exemple) après la mise à niveau.

### Voir aussi

« Nouveautés » à la page 1

### Sauvegarde des fichiers

**1** Pour arrêter tous les services du serveur Breeze, sélectionnez Démarrer > Tous les programmes > Macromedia > Macromedia Breeze > Arrêter Breeze 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\.

### Sauvegarde de la base de données

Vous devez sauvegarder la base de données (le moteur de base de données intégré ou SQL Server 2000) utilisée par Connect Enterprise Server avant d'effectuer la mise à niveau.

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 présente pas d'interface utilisateur graphique.

**Remarque :** Vous pouvez configurer SQL Server Enterprise Manager pour qu'il sauvegarde le moteur de base de données intégré. Consultez la TechNote d'Adobe : [www.adobe.com/go/79895439](http://www.adobe.com/go/79895439).

Pour sauvegarder SQL Server 2000, utilisez SQL Server Enterprise Manager.

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

### Sauvegarde de la base de données SQL Server

Si vous utilisez Microsoft SQL Server 2000, vous pouvez utiliser SQL Server Enterprise Manager pour sauvegarder votre base de données.

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

**1** Dans Windows, choisissez Démarrer > Tous les 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 la restauration 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.

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

- 1 Connectez-vous au serveur hébergeant Connect Enterprise Server.
- 2 Créez un dossier pour stocker les fichiers de sauvegarde de la base de données.

Cet exemple utilise le dossier C:\Connect\_Database.

- 3 Dans le menu Démarrer de Windows, choisissez Exécuter.
- 4 Dans la boîte de dialogue Exécuter, tapez `cmd` dans la zone de texte Ouvrir.
- 5 A l'invite, indiquez le répertoire dans lequel vous avez installé la base de données. Par défaut, le répertoire est MSSQL\binn.
- 6 A l'invite MSSQL\Binn prompt, tapez `osql -E -Q "BACKUP DATABASE breeze TO DISK = 'c:\Connect_Database\breeze.bak'"` et appuyez sur la touche Entrée.

Le message qui apparaît indique si la sauvegarde a réussi.

Lorsque vous utilisez la commande `-E`, vous entrez dans SQL en mode « sa ».

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

- 7 A l'invite, tapez `quit`, puis appuyez sur Entrée.
- 8 Pour vérifier que la sauvegarde a réussi, assurez-vous que le fichier `breeze.bak` est bien présent dans le répertoire C:\Connect\_Database.
- 9 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 du bouton droit sur 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 « How to back up a Microsoft Data Engine database by using Transact-SQL ».

## Préparation de l'installation

### Présentation technique de Connect Enterprise Server

Une installation Connect Enterprise Server comprend plusieurs composants : Connect Enterprise Server, Macromedia® Flash® Media Server d'Adobe et une base de données.

Connect Enterprise Server est une version J2EE qui utilise des composants de Macromedia® JRun™ d'Adobe. Également 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'application, 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 en Flash. Le serveur d'application 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.

**Remarque :** Il comprend un serveur Web et est parfois appelé « serveur Web/application ».

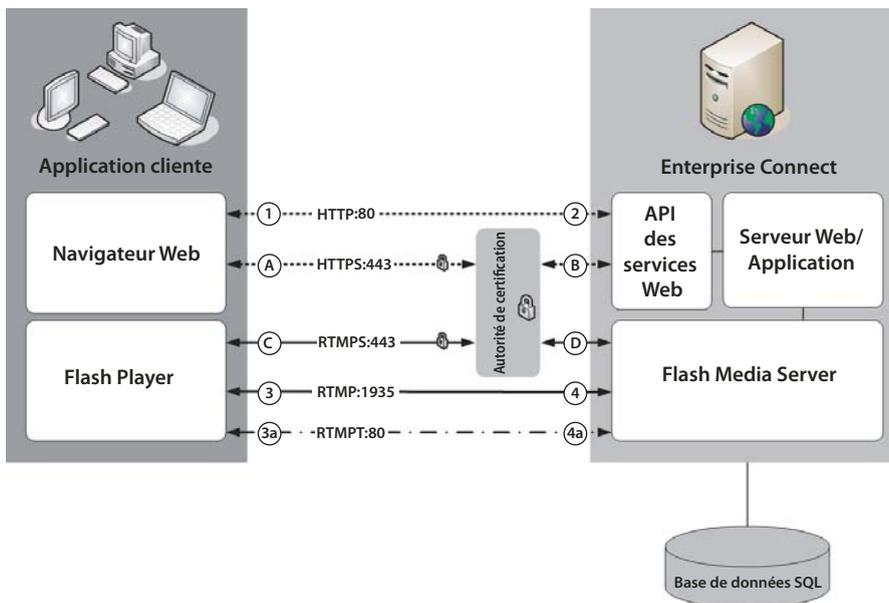
Flash Media Server, également appelé *serveur de réunion*, est installé avec Connect Enterprise Server pour gérer la diffusion audio et vidéo en temps réel, la synchronisation des données et la diffusion des contenus multimédia, ainsi que les interactions avec Acrobat Connect Professional. Certaines 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 Enterprise Server requiert une base de données pour le stockage permanent des métadonnées transactionnelles et d'application, ainsi que des 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 de Connect Enterprise Server ou installer une version complète de Microsoft SQL Server 2000 ou 2005. (Le moteur de base de données intégré est inclus dans l'installation de Connect Enterprise Server, mais pas dans Microsoft SQL Server.)

## Flux de données

Le diagramme suivant illustre la circulation des données entre une application cliente et Connect Enterprise Server.



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

### Connexion non cryptée

Les connexions non cryptées 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 transfère 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 cryptée

Les connexions cryptées 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 US	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 transfère le contenu sur une connexion sécurisée ou fournit au client les informations nécessaires pour qu'il se connecte à la réunion de manière sécurisée.
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.

## Déroulement de l'installation

La procédure suivante vous aide à concevoir, installer et configurer un système Connect Enterprise. 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 14.

### 2. Installez Connect Enterprise Server sur un seul serveur.

Pour plus d'informations, consultez la section « Installation de Connect Enterprise Server 6 » à la page 17. 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 de Connect Enterprise Server.

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

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

### 4. Déployez Connect Enterprise Server.

Pour plus d'informations, consultez la section « Déploiement de Connect Enterprise Server 6 » à la page 24.

### 5. Assurez-vous que Connect Enterprise Server soit correctement installé.

Pour plus d'informations, consultez la section « Tâches de vérification de l'installation » à la page 47.

### 6. (Facultatif) Intégrez Connect Enterprise à votre infrastructure.

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

**Intégration du service d'annuaire** Intégrez Connect Enterprise au serveur d'annuaire LDAP de votre organisation pour éviter de devoir gérer plusieurs annuaires d'utilisateurs. Voir la section « Intégration de Connect Enterprise dans un service d'annuaire » à la page 27.

**Configuration d'un protocole de communication sécurisé (SSL)** Sécurisez l'ensemble des communications de Connect Enterprise. Voir [www.adobe.com/go/connect\\_ssl\\_fr](http://www.adobe.com/go/connect_ssl_fr).

**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.

**Configuration de l'authentification unique** Si vous avez intégré Connect Enterprise à un serveur d'annuaire LDAP, laissez les utilisateurs accéder aux ressources Connect Enterprise sans qu'ils aient besoin de se reconnecter. Voir la section « Authentification unique » à la page 38.

**Configuration d'une infrastructure de clé publique (PKI)** Si vous avez intégré Connect Enterprise à un serveur d'annuaire LDAP, renforcez la sécurité en demandant des certificats client. Voir la section « Infrastructure de clé publique (PKI) » à la page 42.

**Hébergement d'Acrobat Connect Add-in** Les utilisateurs peuvent très facilement télécharger l'extension Acrobat Connect Add-in depuis les serveurs d'Adobe. Toutefois, si la stratégie de sécurité de votre organisation n'autorise pas les téléchargements externes, hébergez l'extension sur votre propre serveur pour améliorer le confort de vos utilisateurs. Voir la section « Hébergement d'Acrobat Connect Add-in » à la page 45.

#### **7. (Facultatif) Choisissez d'installer ou non Connect Enterprise Server dans un cluster.**

Pour plus d'informations, consultez les sections « Choix du déploiement de Connect Enterprise dans un cluster » à la page 13 et « Déploiement de Connect Enterprise Server dans un cluster » à la page 24.

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

Pour plus d'informations, consultez les sections « Choix du déploiement des serveurs Edge » à la page 15 et « Déploiement de Connect Edge Server » à la page 26.

### **Choix du déploiement de Connect Enterprise dans un cluster**

Il est possible d'installer tous les composants Connect Enterprise Server, y compris la base de données, sur un seul serveur, mais cette conception convient mieux aux tests qu'à la production.

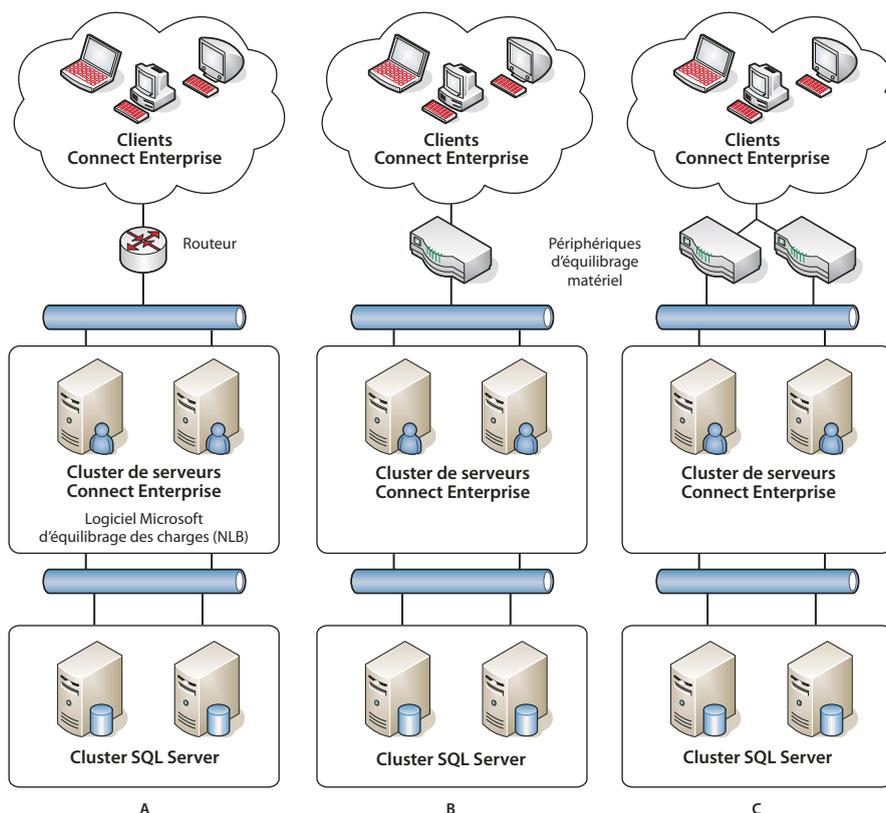
Un groupe de serveurs connectés, chacun faisant le même travail, est généralement appelé un *cluster*. Dans un cluster Connect Enterprise Server, vous installez une copie identique de Connect Enterprise Server sur chacun de ses serveurs.

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 Connect Enterprise Server.*

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.

Dans l'idéal, chaque composant d'un système doit être redondant, pas seulement le serveur Connect Enterprise. Par exemple, vous pouvez utiliser plusieurs périphériques matériels d'équilibrage de charge (tels que BIG-IP de F5 Networks), un cluster de serveurs hébergeant Connect Enterprise Server 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 de Connect Enterprise Server dans un cluster » à la page 24

« Configuration du stockage partagé » à la page 35

## Choix d'une base de données

Connect Enterprise Server 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 (fourni avec le programme d'installation) ou installer Microsoft SQL Server 2000 ou 2005 (vendus séparément).

### Base de données intégrée

Pensez à utiliser ce moteur de base de données pour les tests et le développement. Il utilise les mêmes structures de données que SQL Server, mais n'est pas aussi fiable.

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

- Du fait des restrictions de licence, vous devez installer ce moteur sur le même ordinateur que Connect Enterprise Server. 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.

Pour plus d'informations sur le moteur de base de données intégré (MSDE), consultez l'article de Microsoft « MSDE security and authentication ».

### Microsoft SQL Server

Vous pouvez installer SQL Server sur le même ordinateur que Connect Enterprise Server 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](http://www.adobe.com/go/2e86ea67).

Il est généralement préférable d'utiliser le moteur Microsoft SQL Server 2000 ou 2005 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 fournit également des interfaces utilisateur graphiques pour la gestion et les interrogations de la base de données.

Installez SQL Server en mode de connexion mixte afin de pouvoir utiliser l'authentification SQL. Définissez la base de données pour qu'elle respecte la casse et, si vous utilisez SQL Server 2000, appliquez le Service Pack 4.

Utilisez SQL Server dans les scénarios de déploiement suivants :

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

### Voir aussi

« Configurations de bases de données/serveur prises en charge » à la page 6

« Installation de Connect Enterprise Server 6 » à la page 17

### Choix du déploiement des serveurs Edge

Lorsque le réseau d'une organisation comprend des serveurs Edge, les clients se connectent à Connect Edge Server et ce dernier se connecte à Connect Enterprise Server. Cette connexion est transparente : les utilisateurs ont l'impression de se connecter directement au serveur qui héberge la réunion.

**Remarque :** Lorsque des serveurs Edge sont utilisés, le serveur sur lequel Connect Enterprise Server est installé est appelé serveur « origine ».

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.

**Les 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.

**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.

**Équilibrage 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.

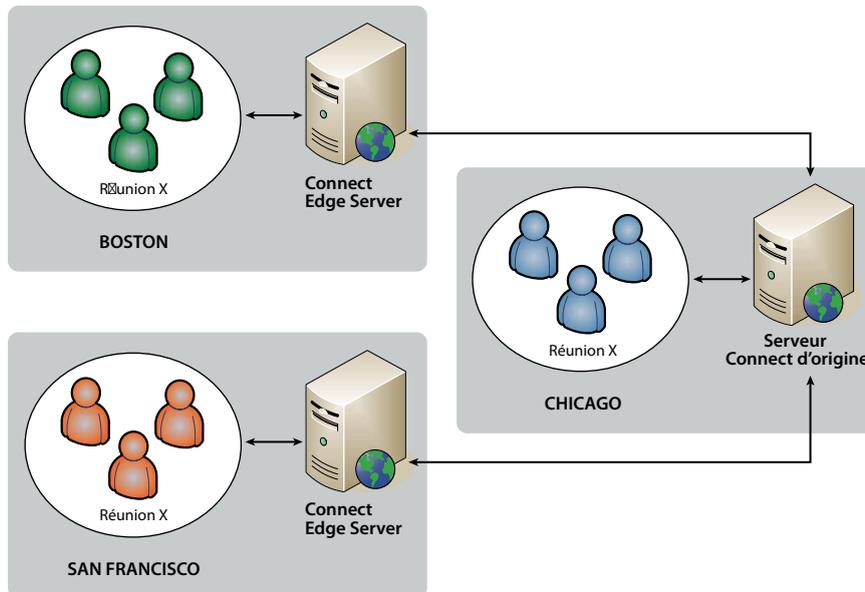
### Fonctionnement des serveurs Edge

Les serveurs Edge authentifient les utilisateurs et autorisent leurs requêtes de services Web, telles qu'Acrobat Connect Professional, 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 Connect Enterprise Server.

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 de Connect Edge Server 6 » à la page 21

« Déploiement de Connect Edge Server 6 » à la page 25

# Chapitre 3 : Installation et mise à niveau Connect Enterprise

Pour installer et configurer Adobe Connect Enterprise Server et Connect Edge Server, vous allez utiliser une suite de programmes d'installation et les écrans de la Console de gestion des applications. Conservez ce guide ouvert à ce chapitre lorsque vous procédez.

## Installation de Connect Enterprise Server 6

### Avant d'installer Connect Enterprise Server

Avant de commencer la procédure d'installation, assurez-vous de répondre à toutes les conditions requises répertoriées à la section « Configuration requise pour l'installation » à la page 4. Pour installer Connect Enterprise Server, vous devez disposer d'un numéro de licence. Adobe a dû vous envoyer un message électronique comportant un lien vers un site Web qui fournit le numéro de licence.

### Installation de Connect Enterprise Server

- 1** Fermez toutes les applications.
- 2** Insérez le CD d'installation dans votre lecteur. Dans l'écran de démarrage, cliquez sur le bouton Installation d'Adobe Connect Enterprise Server.  
  
Si le programme d'installation ne démarre pas automatiquement, double-cliquez sur le fichier setup.exe situé dans le dossier racine du CD d'installation.
- 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** Utilisez l'une des méthodes 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 Connect Enterprise Server 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 Enterprise Server. Cliquez sur Suivant.
- 7** Dans la fenêtre Informations sur la société, entrez votre numéro de série et cliquez sur Suivant.
- 8** Utilisez l'une des méthodes suivantes :
  - Si la fenêtre du moteur de base de données intégré apparaît, choisissez de l'installer ou non. Si vous souhaitez l'installer dans le répertoire par défaut (c:\MSSQL), 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, 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 cet ordinateur, une boîte de dialogue vous signale que le moteur de bases de données ne sera 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 installée correctement et que le programme d'installation s'en aperçoive. Suivez les instructions de la TechNote 18927 ([www.adobe.com/go/fr/tn\\_18927](http://www.adobe.com/go/fr/tn_18927)) et recommencez l'installation.

**9** Dans la fenêtre du choix du dossier de démarrage, cliquez sur Suivant pour accepter l'emplacement par défaut des raccourcis du menu Démarrer (Adobe Connect Enterprise Server), ou cliquez sur Parcourir pour choisir un autre emplacement et cliquez sur Suivant.

**10** Dans la boîte de dialogue Prêt pour l'installation, vérifiez les emplacements d'installation de Connect Enterprise Server et du dossier du menu de démarrage. 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 la fenêtre du service d'initialisation de Connect Enterprise Server, procédez de l'une des manières suivantes :

- Sélectionnez l'option Démarrer Connect Enterprise Server pour lancer l'Assistant de la Console de gestion des applications et continuer la configuration de Connect Enterprise Server. Cliquez sur Suivant.
- Sélectionnez l'option Do not start Connect Enterprise Server now. Cliquez sur Suivant.

**13** Si vous avez démarré le serveur Connect Enterprise, un message vous signale que le service d'application démarre.

Connect Enterprise Server s'exécute sous forme de trois services Windows : Adobe Connect Enterprise Server, Flash Media Server et Flash Media Administration Server.

**14** Dans le dernier écran de l'assistant de configuration d'Adobe Connect Enterprise Server, cliquez sur Terminer.

Si vous avez choisi de démarrer Connect Enterprise Server, l'Assistant de la Console de gestion des applications s'ouvre dans un navigateur pour vous guider tout au long de la procédure de configuration du serveur.

## Configuration de Connect Enterprise Server à l'aide de l'Assistant de la Console de gestion des applications

Après l'installation de Connect Enterprise Server, 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 > Tous les programmes > Adobe Connect Enterprise Server > Configurer Adobe Connect Enterprise Server, 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 le serveur Connect Enterprise. La valeur par défaut est 1433. (Si vous utilisez le moteur de base de données intégré, la valeur par défaut est 1434.)

**Utilisateur de base de données** Nom de l'utilisateur de la base de données. Si vous avez installé le moteur de base de données intégré, 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 le moteur de base de données intégré, il s'agit de la valeur définie dans le programme d'installation.

### 3. Entrez les paramètres du serveur.

**Nom du compte** Nom qui identifie votre compte Connect Enterprise, par exemple « Compte Connect Enterprise 6 ».

**Hôte Connect Enterprise** Nom de domaine pleinement qualifié (FQDN) que les clients utilisent pour se connecter à Connect Enterprise. Par exemple, lorsque l'URL du compte est `http://connect.exemple.com`, la valeur de l'hôte Connect Enterprise serait `connect.exemple.com`.

**Port HTTP** Port utilisé par Connect Enterprise 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 Connect Enterprise.

**Mappages de l'hôte** Nom correspond au nom d'hôte de l'ordinateur qui héberge Connect Enterprise Server. Le Nom externe correspond au FQDN que les clients utilisent pour se connecter à Connect Enterprise.

*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 de Connect Enterprise.

**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 Connect Enterprise 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 Connect Enterprise Server. Le cache pouvant grossir au-delà du pourcentage spécifié, 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 Connect Enterprise Server et tous les volumes externes. Avant de configurer cette fonction, consultez la section « Configuration du stockage partagé » à la page 35.

### 4. Chargement du fichier de licence

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

### 5. Création d'un administrateur de compte

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

### 6. Continuez à utiliser Connect Enterprise Server.

Il s'agit là 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 Connect Enterprise Server), revenir dans la Console de gestion des applications (pour modifier ou vérifier vos paramètres) ou consulter la documentation pour en savoir plus sur Connect Enterprise Server.

## Démarrage et arrêt de Connect Enterprise Server

Vous pouvez démarrer ou arrêter Connect Enterprise Server depuis le menu Démarrer, la fenêtre Services ou la ligne de commande.

### Arrêt du serveur Connect Enterprise via le menu Démarrer

- 1 Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Enterprise Server.
- 2 Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Meeting Server.

### Démarrage du serveur Connect Enterprise via le menu Démarrer

- 1 Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Meeting Server.
- 2 Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Enterprise Server.

### Arrêt du serveur Connect Enterprise 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 Server.
- 3 Arrêtez le service Flash Media Server (FMS).
- 4 Arrêtez le service Flash Media Administration Server.

### Démarrage du serveur Connect Enterprise 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 Server.

### Arrêt du serveur Connect Enterprise 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 le serveur Connect Enterprise, tapez :

```
net stop BreezeApp
```

- 3 Pour arrêter Macromedia Flash Media Server d'Adobe, tapez :

```
net stop FMS
```

- 4 Pour arrêter le serveur Flash Media Server Administration, tapez :

```
net stop FMSAdmin
```

### Démarrage de Connect Enterprise 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, tapez :

```
net start FMS
```

- 3 Pour démarrer le serveur Flash Media Server Administrator, tapez :

```
net start FMSAdmin
```

- 4 Pour démarrer Connect Enterprise Server, tapez :

```
net start BreezeApp
```

## Désinstallation de Connect Enterprise Server

**1** Arrêtez les services Connect Enterprise Server dans l'ordre suivant : Flash Media Server (FMS), Flash Media Server Administration Server, Adobe Connect Enterprise Server.

**2** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Désinstaller Adobe Connect Enterprise Server.

**3** Supprimez le répertoire racine de Connect Enterprise Server. Par défaut, l'emplacement est C:\breeze.

Lorsque vous désinstallez Connect Enterprise, 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.

**4** (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'Editeur 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.

## Installation de Connect Edge Server 6

### Avant d'installer Connect Edge Server

Avant d'entamer la procédure d'installation, assurez-vous que toutes les conditions requises énumérées à la section [www.adobe.com/go/connect\\_sysreqs\\_fr](http://www.adobe.com/go/connect_sysreqs_fr) sont remplies. Pour installer Connect Edge Server 6, vous devez disposer d'un numéro de licence. Adobe a dû vous envoyer un message électronique comportant un lien vers un site Web qui fournit le numéro de licence.

### Voir aussi

« Choix du déploiement des serveurs Edge » à la page 15

### Installation de Connect Edge Server

**1** Fermez toutes les autres applications.

**2** Insérez le CD d'installation de Connect Enterprise Server 6 dans votre lecteur.

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

**3** Dans l'écran de démarrage, cliquez sur le bouton Installation d'Adobe Connect Edge Server 6.

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

**5** Utilisez l'une des méthodes 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 Connect Edge Server est déjà installé sur cet ordinateur, la fenêtre Update Existing Connect Edge Server Install apparaît. Cliquez sur Suivant.

**6** Acceptez le raccourci par défaut ou cliquez sur Parcourir pour sélectionner un emplacement différent, puis cliquez sur Suivant.

**7** Dans la fenêtre Select Start Menu Folder, cliquez sur Suivant pour accepter l'emplacement par défaut des raccourcis du menu Démarrer (Adobe Connect Edge Server), 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 de Connect Enterprise 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'assistant d'installation de Connect Edge Server.

### Voir aussi

« Déploiement de Connect Edge Server 6 » à la page 25

## Installation du fichier de licence de Connect Edge Server

Lors du traitement de votre commande de Connect Edge Server, Adobe vous envoie un message électronique contenant le fichier de licence du logiciel.

- 1 Ouvrez le message électronique d'Adobe.
- 2 Enregistrez le fichier de licence dans le dossier des licences : `[rep_install_racine]\edgeserver\win32\licenses`. Par défaut, le répertoire racine d'installation est `C:\breeze`.
- 3 Arrêtez et démarrez Connect Edge Server pour vérifier le bon fonctionnement de l'installation.

## Démarrage et arrêt de Connect Edge Server

Vous pouvez démarrer ou arrêter Connect Edge Server depuis le menu Démarrer, la fenêtre Services ou la ligne de commande.

### Arrêt du serveur Connect Edge via le menu Démarrer

❖ Choisissez Démarrer > Tous les programmes > Adobe Connect Edge Server > Arrêter Adobe Connect Edge Server.

### Démarrage du serveur Connect Edge via le menu Démarrer

❖ Choisissez Démarrer > Tous les programmes > Adobe Connect Edge Server > Démarrer Adobe Connect Edge Server.

### Arrêt du serveur Connect Edge via la fenêtre Services

- 1 Choisissez Démarrer > 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 de Connect Edge Server 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 Administration Server.
- 3 Démarrez le service Flash Media Server (FMS).

### Arrêt du serveur Connect Edge 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 de Connect 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 de Connect Edge Server**

- 1** Arrêtez les services Connect Edge Server dans l'ordre suivant : Flash Media Server (FMS), Flash Media Server Administration Server.
- 2** Choisissez Démarrer > Tous les programmes > Adobe Connect Edge Server > Désinstaller Adobe Connect Edge Server.
- 3** Supprimez le répertoire racine. Par défaut, l'emplacement est C:\breeze.

# Chapitre 4 : Déploiement et configuration de Connect Enterprise

Ce chapitre présente l'ensemble des tâches de déploiement et de configuration à effectuer après l'installation d'Adobe Connect Enterprise Server ou d'Adobe Connect Edge Server. Il vient compléter la première phase de configuration de Connect Enterprise via la Console de gestion des applications.

## Déploiement de Connect Enterprise Server 6

### Déploiement de Connect Enterprise Server

**1** Sur votre serveur DNS, définissez un nom de domaine pleinement qualifié (FQDN) pour Connect Enterprise Server (par exemple connect.masociete.com) et reliez ce nom à l'adresse IP statique de l'ordinateur hébergeant Connect Enterprise Server.

**2** Si vous souhaitez que Connect Enterprise soit disponible hors de votre réseau, configurez les ports suivants dans un pare-feu :

**80** Port associé par défaut au serveur d'application Connect Enterprise Server. Port tertiaire du serveur de réunions (Macromedia Flash Media Server d'Adobe).

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

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

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

Pour obtenir de l'aide pour le déploiement de Connect Enterprise Server, contactez l'assistance technique d'Adobe à l'adresse [www.adobe.com/go/breeze\\_licensed\\_support\\_fr](http://www.adobe.com/go/breeze_licensed_support_fr).

### Déploiement de Connect Enterprise Server dans un cluster

Avant de pouvoir déployer Connect Enterprise Server dans un cluster, vous devez réussir à l'installer sur un seul ordinateur. Il est également préférable de configurer les fonctionnalités supplémentaires (par exemple, SSL, une intégration de service d'annuaire, une authentification unique, un stockage de contenu partagé, etc.) et de vérifier qu'elles fonctionnent correctement sur ce serveur.

Cette procédure part du principe que vous effectuez une migration depuis une installation fonctionnant correctement sur un serveur unique vers une installation multi-serveurs.

**1** Installez SQL Server sur un serveur dédié (ou vérifiez qu'il a bien été installé).

Si vous installez Connect Enterprise Server dans un cluster, utilisez le moteur de base de données Microsoft SQL Server 2000 ou 2005 et non le moteur de base de données intégré. En effet, chaque serveur hébergeant Connect Enterprise Server doit pouvoir accéder à la base de données, et des restrictions de licence n'autorisent pas l'accès de plusieurs serveurs au moteur de base de données intégré.

**2** Installez et configurez Connect Enterprise Server sur un serveur dédié.

Utilisez les mêmes numéros de série et fichier de licence pour chaque installation de Connect Enterprise Server.

**Remarque :** Vous devez disposer d'un fichier de licence spécial cluster prenant en charge le nombre de noeuds de votre cluster. Pour plus d'informations, contactez votre représentant Adobe.

**3** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Configurer Adobe Connect Enterprise Server pour ouvrir la Console de gestion des applications. Dans la fenêtre Paramètres de la base de données, assurez-vous que l'option Hôte de base de données indique le serveur hébergeant SQL Server.

Tous les paramètres de la base de données doivent correspondre aux valeurs définies pour votre installation sur un serveur unique.

**4** Dans la fenêtre Paramètres du serveur de la Console de gestion des applications, définissez Nom Externe Mappages de l'hôte sur le nom de domaine pleinement qualifié de l'ordinateur que vous ajoutez au cluster.

**5** Assurez-vous que Connect Enterprise Server fonctionne correctement.

**6** Installez un équilibreur de charge sur le réseau et configurez-le pour écouter le port 80. Chaque serveur d'application Connect Enterprise doit écouter le port 8080.

Définissez les ports du serveur d'application dans la fenêtre Paramètres du serveur de la Console de gestion des applications. Entrez la valeur dans le champ Port HTTP.

Pour configurer l'équilibreur de charge, consultez la documentation du fournisseur.

**7** Incluez le serveur du cluster dans le pool équilibré.

Pour des instructions précises sur l'inclusion d'un serveur dans le pool équilibré, consultez la documentation du fournisseur.

**8** Répétez les étapes 2 à 7 pour chaque serveur du cluster.

**9** Si vous utilisez un stockage partagé, copiez l'ensemble du contenu du serveur d'origine dans le volume de stockage partagé.

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](http://www.adobe.com/go/connect_licensed_programs_fr).

### Voir aussi

« Installation de Connect Enterprise Server 6 » à la page 17

« Configuration du stockage partagé » à la page 35

## Déploiement de Connect Edge Server 6

### Déroulement de l'installation de Connect Edge Server

#### 1. Conception des régions de 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 Connect Enterprise. 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 Adobe Connect Edge Server.

Installez Connect Edge Server sur chaque ordinateur de chaque région. Par exemple, si vous avez un cluster de serveurs Edge dans une région, installez Connect Edge Server sur chaque ordinateur du cluster. Voir la section « Installation de Connect Edge Server 6 » à la page 21.

#### 3. Modifiez le serveur DNS de chaque région.

Mappez le nom de domaine pleinement qualifié (FQDN) du serveur Connect Enterprise d'origine avec l'adresse IP statique du serveur Connect Edge de chaque région. Voir la section « Déploiement de Connect Edge Server 6 » à la page 25.

#### 4. Configurez le serveur Edge.

Vous devez ajouter les paramètres de configuration dans le fichier custom.ini de chaque serveur hébergeant Connect Edge Server. Voir la section « Déploiement de Connect Edge Server 6 » 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 hébergeant Connect Edge Server. 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 de Connect Edge Server 6 » à la page 25.

## 6. Configuration d'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 de Connect Edge Server

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

**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, tous les clients doivent disposer d'un fichier d'hôtes pointant vers l'adresse IP statique du serveur Edge.

**2** Dans Connect Edge Server, ouvrez le fichier [rép\_install\_racine]\edgeserver\win32\conf\HttpCache.xml et, dans la balise HostName, remplacez  `${%COMPUTERNAME%}`  dans la balise HostName par le nom pleinement qualifié (FQDN) du serveur Edge, par exemple  `edge1.exemple.com` .

```
<!-- The real name of this host. -->
<HostName>${%COMPUTERNAME%}</HostName>
```

**3** Si le répertoire racine (C:\breeze, par défaut) du serveur Connect Edge contient un fichier custom.ini, supprimez-le.

**4** Dans un éditeur de texte, par exemple le Bloc-notes, créez un nouveau fichier texte nommé custom.ini. Définissez les valeurs des paramètres suivants dans le fichier et enregistrez ce dernier :

**FCS.HTTPCACHE\_BREEZE\_SERVER\_NORMAL\_PORT** L'adresse IP ou le nom de domaine et le numéro de port de l'ordinateur sur lequel Connect Enterprise Server est installé, par exemple  `myConnectServer:80` . Le serveur Connect Edge se connecte à Connect Enterprise Server à cet emplacement.

**FCS\_EDGE\_HOST** Nom de domaine pleinement qualifié (FQDN) du serveur Edge, par exemple  
 `FCS_EDGE_HOST=edge1.exemple.com` .

**FCS\_EDGE\_REGISTER\_HOST** Nom de domaine pleinement qualifié (FQDN) du serveur d'origine Connect Enterprise Server, par exemple  `FCS_EDGE_REGISTER_HOST=connectserver.exemple.com` .

**FCS\_EDGE\_CLUSTER\_ID** Nom du cluster. Chaque cluster de serveurs Edge, ou *zone*, doit disposer d'un ID unique. Chaque ordinateur du cluster doit avoir le même identifiant. Le format recommandé est  `companyname-clustername` , par exemple,  
 `FCS_EDGE_CLUSTER_ID=adobe-apac` .

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

**FCS\_EDGE\_EXPIRY\_TIME** 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.

**FCS\_EDGE\_REG\_INTERVAL** 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.

**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.

**DEFAULT\_FCS\_HOSTPORT** (Facultatif) Pour configurer les ports des serveurs Edge, ajoutez les lignes suivantes dans le fichier custom.ini :  `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.

**5** Sur le serveur d'origine, ouvrez la Console de gestion des applications (Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Configurer Adobe Connect Enterprise Server). 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.

**6** Dans le fichier `custom.ini` du serveur d'origine, mappez la valeur du paramètre `FCS_EDGE_CLUSTER_ID` sur un identifiant de région et enregistrez le fichier. La région Edge est ainsi autorisée. La syntaxe est `edge.cluster-id=zone-id`.

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 quatre clusters mappés sur les régions 1 à 4 :

```
edge.adobe-emea=1
edge.adobe-apac=2
edge.adobe-sf=3
edge.adobe-boston=4
```

**Remarque :** Même si vous ne déployez qu'un seul serveur Connect Edge, vous devez mapper le nom d'identifiant du cluster sur un identifiant de région.

**7** Si vous définissez un paramètre `FCS_EDGE_PASSWORD` sur le serveur Edge, définissez le même mot de passe dans le fichier `custom.ini` du serveur d'origine et enregistrez le fichier.

**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 8 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..](http://www.adobe.com/go/connect_licensed_programs_fr..)

## Voir aussi

« Choix du déploiement des serveurs Edge » à la page 15

# Intégration de Connect Enterprise dans un service d'annuaire

## Présentation de l'intégration du service d'annuaire

Si votre société utilise un serveur d'annuaire, vous pouvez l'intégrer à Connect Enterprise pour ne pas devoir ajouter manuellement les utilisateurs et les groupes individuels. Les comptes d'utilisateurs sont créés automatiquement dans Connect Enterprise à travers des synchronisations manuelles ou planifiées avec l'annuaire de votre société.

Pour être intégré à Connect Enterprise, 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.

Connect Enterprise se connecte en tant que client LDAP à un annuaire LDAP, importe les utilisateurs et les groupes, et s'assure que les informations relatives à ces utilisateurs et groupes de la base de données restent synchronisées avec celles de l'annuaire LDAP externe.

Adobe a testé l'intégration de service d'annuaire avec les serveurs LDAP suivants :

- Active Directory Application Mode (ADAM) SP1

- Active Directory (Windows Server 2000 et Windows Server 2003)
- IBM Directory Server 5.2
- Novell eDirectory 8.7.3 pour Win32
- OpenLDAP 2.3.19
- Sun One Directory Server 5.2 pour Win32
- Netscape 6.02 pour Win32

Plusieurs concepts importants doivent être bien compris avant de configurer et d'effectuer l'intégration d'un service d'annuaire. Ces concepts sont décrits dans les sections suivantes. Si vous connaissez déjà la structure d'annuaire LDAP et l'intégration LDAP, vous pouvez passer directement à la section « Intégration de Connect Enterprise dans un annuaire LDAP » à la page 29.

## Présentation de la structure d'annuaire LDAP

Les annuaires LDAP organisent les informations selon le standard 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, telles que `ou` pour « organizational unit » ou `cn` pour « common name ». 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 organisation, contactez votre administrateur LDAP.

Chaque entrée présente un *nom unique* (DN, distinguished name) 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 Connect Enterprise, 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 organisation. Pour ce faire, vous devez savoir où sont situées les entrées de ce groupe dans la structure d'arborescence de l'annuaire.

Une technique courante consiste à utiliser le domaine Internet de l'organisation en tant que racine de la structure de l'arborescence. Par exemple, Acme, Inc. peut utiliser `dc=com` pour spécifier l'élément racine dans l'arborescence. Un nom unique spécifiant le bureau de vente de Singapour d'Acme, Inc. peut être `ou=Singapore, ou=Marketing, ou=Employees, dc=Acme, dc=com`. (Dans cet exemple, `ou` est une abréviation de l'unité organisationnelle et `dc` une abréviation du composant du 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 noeud d'une branche ou sous des branches différentes.

Si les utilisateurs et les groupes sont sous le même noeud 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 permettant de 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 groupe 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 des ventes, vous pouvez utiliser le nom unique de la branche suivante :

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

Toutefois, le personnel des ventes peut être stocké dans des sous-branches. Dans ce cas, dans la fenêtre Mappage du profil utilisateur, définissez le paramètre Recherche de sous-arborescence sur `true` pour vous assurer que les utilisateurs sont importés à partir des sous-branches situées au-dessous de 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 présentant l'attribut `organizationalPerson` sont sélectionnées pour l'importation.

**Remarque :** L'attribut `objectClass` doit être présent dans toutes les entrées d'un annuaire LDAP. Cet attribut définit les règles et les attributs obligatoires pour cette entrée.

## Utilisation des utilisateurs et groupes internes et externes

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

Pour que les groupes importés demeurent synchronisés avec l'annuaire LDAP externe, vous ne pouvez pas ajouter d'utilisateurs et de groupes internes dans les groupes externes. Vous pouvez cependant ajouter des utilisateurs et des groupes externes dans les groupes internes. Par exemple, pour ajouter tous les utilisateurs du bureau de Singapour à un groupe interne d'utilisateurs appelé Présentation, vous pouvez le faire même si ce dernier contient d'autres utilisateurs qui ne proviennent pas d'une importation par synchronisation.

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 répertoires transforme le groupe ou l'utilisateur importé d'interne en externe et place un avertissement dans le journal de synchronisation.

## Intégration de Connect Enterprise dans 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. Vous devez pour cela utiliser un compte Administrateur.

**Remarque :** Dans le cas d'une intégration avec un serveur LDAP sécurisé (LDAPS), importez le certificat du serveur dans Connect Enterprise Server avant de commencer. Voir la section « Configuration LDAPS » à la page 35.

### 1. Ouvrez la Console de gestion des applications.

Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Configurer Adobe Connect Enterprise Server.

### 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.

Champ	Valeur par défaut	Description
Adresse URL du serveur LDAP	Pas de valeur par défaut.	La forme habituelle est <code>ldap://[servername]:portnumber</code> . Si votre organisation utilise un serveur LDAP sécurisé, utilisez <code>ldaps://</code> .
Méthode d'authentification de connexion LDAP	Pas de valeur par défaut.	Mécanisme de transmission du nom d'utilisateur et du mot de passe LDAP via le réseau :  Anonyme : pas de mot de passe  Simple : transmet le mot de passe en clair  Résumé MD5 : transmet le mot de passe par un mécanisme plus sécurisé
Nom d'utilisateur de connexion LDAP	Pas de valeur par défaut.	Connexion administrative.
Mot de passe de connexion LDAP	Pas de valeur par défaut.	Le mot de passe administratif est masqué.
Expiration de la requête LDAP	Pas de 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.
Limite de taille de la page de requête d'entrée LDAP	Pas de 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.  Par exemple, si vous avez intégré un grand annuaire LDAP ne pouvant afficher que 1 000 utilisateurs et qu'il y a 2 000 utilisateurs 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://mycompany.com:636
UserName:MYCOMPANY\jdoe
Password:password123
Query timeout:(empty)
Authentication mechanism:Simple
Query page size:1000
```

### 3. Mappage des profils utilisateurs de l'annuaire LDAP avec Connect Enterprise

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

Champ	Valeur par défaut	Description
Connexion	Pas de valeur par défaut.	Attribut de connexion dans le service d'annuaire.
Prénom	Pas de valeur par défaut.	Attribut du prénom dans le service d'annuaire.
Nom	Pas de valeur par défaut.	Attribut du nom dans le service d'annuaire.
Adresse de messagerie	Pas de 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 intègre Active Directory à Connect Enterprise Server. Une entrée utilisateur LDAP est mappée avec un profil utilisateur Connect Enterprise et Connexion réseau est un champ personnalisé.

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

#### 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 les utilisateurs des sous-branches de la branche désignée à l'étape 2, 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	Pas de valeur par défaut.	DN (distinguished name - nom distingué) du nœud racine de la branche. Un lien vers la branche sélectionnée s'affiche.
Filtre	Pas de 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 utilisateurs de l'annuaire LDAP et de Connect Enterprise.

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

*Remarque :* Les profils de groupe Connect Enterprise ne prennent pas les champs personnalisés en charge.

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

Voici un mappage entre les attributs d'entrées de groupes LDAP et un profil de groupe Connect Enterprise :

```
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 organisation. Entrez les valeurs dans les champs Branche et Filtre, puis cliquez sur Enregistrer.

Si vous souhaitez importer des groupes provenant de sous-branches de la branche indiquée à l'étape 2, sélectionnez Vrai dans le menu Recherche de sous-arborescence ; dans le cas contraire, sélectionnez Faux.

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	Pas de valeur par défaut.	DN (distinguished name - nom distingué) du nœud racine de la branche. Chaque branche dans l'organisation possède son propre attribut DN LDAP. Un lien vers la branche sélectionnée s'affiche.
Filtre	Pas de valeur par défaut.	Chaîne du filtre de requête.
Recherche de sous-arborescence	True	Valeur Booléenne de true ou false. La valeur de true déclenche une recherche récursive dans toutes les sous-arborescences de la branche.

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

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

## 7. 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.

## 8. 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 32.

**Remarque :** Si vous activez la case à cocher de suppression des utilisateurs et groupes, durant la synchronisation, tous les utilisateurs externes qui ont été supprimés du serveur LDAP seront également supprimés du serveur Connect Enterprise.

## 9. Aperçu de la synchronisation

Ouvrez l'onglet Synchronize 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

Lorsque Connect Enterprise importe les informations des utilisateurs depuis un annuaire externe, il n'importe pas le mot de passe réseau des utilisateurs. Vous devez donc implémenter une autre méthode de gestion des mots de passe pour les utilisateurs importés dans l'annuaire Connect Enterprise.

### Authentification unique

La méthode recommandée pour gérer les mots de passe et l'authentification des utilisateurs importés est l'authentification unique. Cette méthode permet à l'utilisateur connecté au réseau de l'organisation d'accéder à Connect Enterprise (et aux autres ressources pour lesquelles il dispose d'autorisations) sans avoir à se connecter de nouveau.

Si vous envisagez d'utiliser l'authentification unique, définissez la stratégie d'authentification pour l'intégration au service d'annuaire sur Ne rien faire dans la fenêtre Paramètres de la stratégie de l'onglet Paramètres du service d'annuaire.

### 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.

### Voir aussi

« Authentification unique » à la page 38

### Recommandations relatives à la synchronisation

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

- Vous pouvez planifier la synchronisation pour qu'elle ait lieu régulièrement.
- Vous pouvez effectuer une synchronisation manuelle qui synchronise immédiatement l'annuaire de Connect Enterprise et l'annuaire LDAP de l'organisation.

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 provoquerait la suppression des utilisateurs ou des groupes dans Connect Enterprise Server.

### Synchronisations planifiées

Les synchronisations planifiées sont conseillées car elles permettent de s'assurer que Connect Enterprise dispose d'une image à jour des utilisateurs et des groupes importés depuis l'annuaire LDAP de l'organisation.

Si vous importez un grand nombre d'utilisateurs et de groupes, votre première synchronisation de l'annuaire Connect Enterprise et de l'annuaire LDAP externe risque de monopoliser d'importantes ressources. Dans ce cas, il est préférable de planifier cette première synchronisation en dehors des heures de pointe, par exemple tard dans la nuit. (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, Connect Enterprise compare les entrées de l'annuaire LDAP à celles de l'annuaire de Connect Enterprise et n'importe que celles dont au moins un champ a été 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 des groupes ne sont pas vraiment 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* 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 <i>aaaMMj'T'HHmss.SSS</i> .
Principal ID	Nom de connexion ou non du groupe.
Principal type	Caractère unique : U pour utilisateur, G pour groupe.
Event	L'action entreprise ou la condition rencontrée.
Detail	Informations détaillées sur l'événement.

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

Événement	Description	Détail
add	Le principal a été ajouté dans Connect Enterprise.	Paquet XML abrégé décrivant les champs mis à jour par l'intermédiaire d'une suite de paires de balises au format <code>&lt;fieldname&gt;value&lt;/fieldname&gt;</code> (par exemple, <code>&lt;first-name&gt;Joe&lt;/first-name&gt;</code> ). 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 :  <code>&lt;add&gt;ID list&lt;/add&gt;</code> <code>&lt;remove&gt;ID list&lt;/remove&gt;</code>  La liste des ID est une suite de paquets <code>&lt;id&gt;principal ID&lt;/id&gt;</code> , où <code>principal ID</code> est un ID qui apparaîtrait dans la colonne Principal ID, par exemple un nom d'identifiant utilisateur ou un nom de groupe. Lorsque la liste d'ID ne contient aucun membre, le nœud parent sort comme <code>&lt;add/&gt;</code> ou <code>&lt;remove/&gt;</code> .
delete	Le mandant a été supprimé dans Connect Enterprise.	
up-to-date	Le mandant est un mandant externe dans Connect Enterprise et est déjà synchronisé avec l'annuaire externe. Aucun changement n'a été effectué.	Un utilisateur ou un groupe créé dans Connect Enterprise 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 de Connect Enterprise 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.

## Configuration LDAPS

Vous pouvez configurer Connect Enterprise Server pour crypter toutes les communications échangées avec un serveur LDAP sécurisé. Par défaut, Connect Enterprise Server ne crypte pas ces communications.

Servez-vous de l'utilitaire Java Keytool pour importer le certificat du serveur LDAP dans l'emplacement de stockage approuvé de la machine virtuelle Java (JVM) de Connect Enterprise Server. Si le certificat du serveur est au format PEM (Privacy Enhanced Mail), il doit être converti en un format codé DER ou 64 bits. (DER signifie Règles de codage unique ou Distinguished Encoding Rules.)

### Voir aussi

« Démarrage et arrêt de Connect Enterprise Server » à la page 20

### Conversion du certificat du format PEM au format DER

1 Installez OpenSSL (si ce n'est pas déjà fait).

*Remarque :* OpenSSL est un outil tiers que vous pouvez télécharger en ligne.

2 Exécutez la commande suivante :

```
openssl x509 -in [original certificate filename and path].pem -out [target filename and path].der
```

### Importation d'un certificat de serveur LDAP

1 Pour copier (exporter) le fichier de certificat du serveur LDAP sur l'ordinateur qui héberge Connect Enterprise Server, localisez l'emplacement de stockage approuvé utilisé pour l'instance du serveur. Pour une installation par défaut, l'emplacement approuvé correspond au répertoire : `[rep_install_racine]/appserv/win32/jre/lib/security/cacerts`.

*Remarque :* `[rep_install_racine]` fait référence au répertoire racine de votre installation Connect Enterprise Server qui correspond à `C:\breeze` par défaut.

2 Pour importer le certificat du serveur LDAP dans l'emplacement de stockage approuvé, ouvrez une invite de commande vers ce répertoire. Dans le cas d'une installation par défaut, il s'agit du répertoire `[rep_install_racine]/appserv/win32/jre/lib/security`.

3 Entrez la commande suivante, qui fournit le chemin (relatif ou pleinement qualifié) d'accès au fichier de certificat du serveur LDAPS et l'emplacement du fichier de stockage approuvé :

```
[root_install_dir]/appserv/win32/jre/bin/keytool -import -alias [nickname for cert] -file [cert filename and path] -keystore [trustStore filename and path] -storepass [trustStore password]
```

Voici un exemple de commande valide :

```
keytool -import -alias ldapServerCert -file C:\Certs\ldapservcert.der -keystore cacerts -storepass changeit
```

*Remarque :* Le mot de passe du stockage approuvé par défaut est `changeit`. Il est préférable de le modifier pour plus de sécurité.

4 Si le certificat du serveur LDAPS a été créé par une autorité de certification inconnue (par exemple, un certificat auto-signé), vous êtes invité(e) à en vérifier les informations et à confirmer l'importation.

5 Redémarrez Connect Enterprise Server.

## Configuration du stockage partagé

### A propos du stockage partagé

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

Voici des 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 lorsque cela est 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 est nécessaire. Cette configuration libère des ressources sur le serveur d'application, 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 Taille du contenu mis en cache.)

**Remarque :** Si vous utilisez un cluster Connect Enterprise Server et que vous ne configurez pas les périphériques de stockage partagé, le cluster fonctionne en mode miroir complet (le contenu publié dans Connect Enterprise Server 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 Connect Enterprise Server, 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 7

« Déploiement de Connect Enterprise Server dans un cluster » à la page 24

### Configuration du stockage partagé

Avant de commencer, Connect Enterprise Server 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 une installation Connect Enterprise Server existante afin d'utiliser des volumes de stockage partagé, vous devez copier le contenu de l'un de ces serveurs sur le volume partagé.

**a** Arrêtez Connect Enterprise Server (Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Enterprise Server et Arrêter Adobe Connect Meeting Server).

**b** Copiez le dossier `[rep_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. Connect Enterprise 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 Connect Enterprise Server (Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Meeting Server et Démarrer Adobe Connect Enterprise Server).

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

**a** Cliquez du 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 Connect Enterprise Server (le serveur d'application uniquement).

**a** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Enterprise Server.

- b** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Enterprise Server.
  - 5** Ouvrez la Console de gestion des applications (Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Configurer Adobe Connect Enterprise Server).
  - 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 de Connect Enterprise Server de sorte qu'il agisse comme un cache (les ressources sont supprimées automatiquement lorsque l'espace est nécessaire et sont restaurées à la demande), entrez une valeur dans le champ 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 Connect Enterprise Server (le serveur d'application uniquement).
- a** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Enterprise Server.
  - b** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Enterprise Server.

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

- 1** Installez Connect Enterprise Server sans le démarrer. Si Connect Enterprise Server est installé et déjà en cours d'exécution, arrêtez-le.
- 2** Dans Connect Enterprise Server, choisissez Démarrer > Panneau de configuration > Outils d'administration > Services pour ouvrir la fenêtre Services, sélectionnez Adobe Connect Enterprise Server, puis procédez comme suit :
  - a** Cliquez du 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 Connect Enterprise Server.
  - a** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Meeting Server.
  - b** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Enterprise Server.
- 4** (Facultatif) Si vous installez Connect Enterprise Server pour la première fois, suivez les instructions de la section « Déploiement de Connect Enterprise Server dans un cluster » à la page 24.
- 5** Cliquez sur Enregistrer et fermez la Console de gestion des applications.

# Chapitre 5 : Configuration des fonctions avancées

La technologie prise en charge par Adobe Connect Enterprise Server 6 vous permet d'intégrer Connect Enterprise à votre infrastructure existante et de respecter les stratégies de sécurité de votre organisation.

## Authentification unique

### Choix d'un mécanisme d'authentification unique

L'authentification unique (SSO, ou Single sign-on) 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 n'aient pas besoin d'ouvrir une session dans Adobe Connect Enterprise. Si vous avez intégré Connect Enterprise à un annuaire LDAP, l'authentification unique se révèle très utile pour gérer les mots de passe et pour authentifier les utilisateurs importés.

Vous devez choisir l'un des deux mécanismes d'authentification unique suivants :

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

**Authentification NTLM (Microsoft NT LAN Manager)** Configurez le gestionnaire NTLM pour qu'il transmette les informations d'authentification à Connect Enterprise. Seul Microsoft Internet Explorer sous Microsoft Windows peut négocier une authentification NTLM sans demander ses informations de connexion à l'utilisateur.

*Remarque : NTLM2 et Kerberos ne sont pas pris en charge.*

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 Connect Enterprise sont acheminées vers un agent placé entre le client et Connect Enterprise Server. 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 Connect Enterprise Server. Sur Connect Enterprise Server, 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 de Connect Enterprise Server » à la page 20

### Configuration d'une authentification d'en-tête HTTP sur Connect Enterprise Server

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

**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 Arrêter Connect Enterprise :

- a** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Enterprise Server.
- b** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > 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 dans la requête HTTP envoyée à Connect Enterprise. Le nom de l'en-tête doit être `header_field_name`.

## 4 Enregistrez le fichier custom.ini et redémarrez Connect Enterprise :

- a** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Meeting Server.
- b** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Enterprise 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 Connect Enterprise Server.

- 1 Sélectionnez la valeur du champ d'en-tête `header_field_name` pour une connexion utilisateur à Connect Enterprise.
- 2 Envoyez une requête HTTP à Connect Enterprise Server à l'adresse URL suivante :

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

Le filtre Java sur Connect Enterprise Server intercepte la requête, recherche l'en-tête `header_field_name`, 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 de Connect Enterprise Server, recherchez la chaîne "OK" qui indique que l'authentification a réussi.

- 4 Dans la réponse de Connect Enterprise Server, recherchez le cookie `BREEZESESSION`.

- 5 Redirigez l'utilisateur vers l'URL requise sur Connect Enterprise Server 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 toutes les requêtes subséquentes à Connect Enterprise Server au cours de la session client.

### Configuration de l'authentification d'en-têtes HTTP avec Apache

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

- 1 Installez Apache en tant que proxy inverse sur un autre ordinateur que celui qui héberge Connect Enterprise Server.
- 2 Choisissez Démarrer > Tous les 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 Connect Enterprise :

**a** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Enterprise Server.

**b** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Meeting Server.

**4** Sur l'ordinateur qui héberge Connect Enterprise Server, 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 dans 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 Connect Enterprise :

**a** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Meeting Server.

**b** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Enterprise 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>
-->
```

## Configuration de l'authentification NTLM

NTLM est un protocole Stimulation/Réponse qui permet à un client de faire la preuve de son identité sans fournir de mot de passe. Le navigateur Web envoie une requête à un serveur d'authentification NTLM pour obtenir les informations de connexion de l'utilisateur. La routine NTLM est masquée et transparente pour l'utilisateur.

Les utilisateurs doivent employer Internet Explorer sous Windows pour pouvoir bénéficier de l'authentification unique avec NTLM.

## Voir aussi

« Démarrage et arrêt de Connect Enterprise Server » à la page 20

### Ajout de paramètres de configuration

**1** Arrêtez Connect Enterprise :

**a** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Enterprise Server.

**b** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Meeting Server.

**2** Ajoutez le paramètre suivant dans le fichier custom.ini du répertoire racine d'installation :

```
NTLM_DOMAIN= [domain]NTLM_SERVER= [NTLM_server_IP_address]
```

Dans le code ci-dessus, *[domain]* est le nom de domaine NT, tel que acme.com, dans lequel les utilisateurs s'authentifient. La valeur *[NTLM\_server\_IP\_address]* est l'adresse IP du serveur d'authentification NTLM. L'adresse IP numérique doit être utilisée avec NTLM\_SERVER; le nom de l'hôte ne fonctionne pas.

**3** Enregistrez le fichier custom.ini et redémarrez Connect Enterprise :

**a** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Meeting Server.

**b** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Enterprise Server.

**4** Ouvrez le fichier *[rép\_install\_racine]\appserv\conf\WEB-INF\web.xml* et procédez comme suit :

**a** Retirez les commentaires du mappage NtlmAuthenticationFilter.

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

**b** Appliquez un commentaire au mappage du filtre HeaderAuthenticationFilter.

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

### Rapprochement des stratégies de connexion

Les stratégies de connexion de Connect Enterprise et NTLM diffèrent quant à l'authentification des utilisateurs. Ces stratégies doivent être rapprochées pour que les utilisateurs puissent bénéficier de l'authentification unique.

L'identifiant de connexion utilisé par le protocole NTLM peut être un nom d'utilisateur (jdoe), un numéro d'employé (1234) ou un nom codé, selon la stratégie de l'organisation. Par défaut, Connect Enterprise utilise une adresse électronique (jdoe@masociete.com) comme identifiant de connexion. Vous pouvez configurer Connect Enterprise de sorte qu'il partage le même identifiant unique avec NTLM.

**1** Ouvrez Connect Enterprise Manager.

Pour accéder à Connect Enterprise Manager, ouvrez une fenêtre de navigateur, puis entrez le nom de domaine pleinement qualifié de l'Hôte Connect Enterprise (ex. : http://connect.societe.com). Entrez la valeur de l'Hôte Connect Enterprise dans l'écran Paramètres du serveur de la console de gestion des applications.

**2** Ouvrez l'onglet Administration, cliquez sur Utilisateurs et Groupes, puis sur Modifier les stratégies de nom d'utilisateur et de mot de passe.

**3** Dans la section Stratégie de connexion, sélectionnez Non pour Utiliser l'adresse de messagerie comme identifiant de connexion.

# Infrastructure de clé publique (PKI)

## Présentation de l'infrastructure de clé publique (PKI)

Vous pouvez configurer une infrastructure de clé publique (PKI) pour gérer les informations d'identification dans le cadre de l'architecture de sécurité Connect Enterprise de vos clients. Dans le protocole SSL plus répandu, l'identité du serveur est vérifiée auprès du client ; dans une infrastructure PKI, l'identité du client est vérifiée auprès du serveur.

Un tiers approuvé, appelé Autorité de certification, vérifie l'identité du client et lui associe un certificat au format X.509 (également appelé *clé publique*). Lorsque le client se connecte à Connect Enterprise Server, un proxy négocie sa connexion pour l'infrastructure PKI. Si le client dispose d'un cookie issue d'une session précédente ou d'un certificat valide, il est connecté à Connect Enterprise Server.

Pour plus d'informations sur l'infrastructure PKI, consultez le Centre de technologie PKI de Microsoft.

## Configuration requise PKI

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 PKI. 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 l'extension Adobe Acrobat Connect Add-in pour participer aux réunions requérant des authentifications PKI. Les clients doivent installer cette extension 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 de PKI par Flash Player n'est pas aussi étendue que celle de l'extension. Cependant, pour afficher les archives de réunions, les clients doivent avoir installé la dernière version de Flash Player.

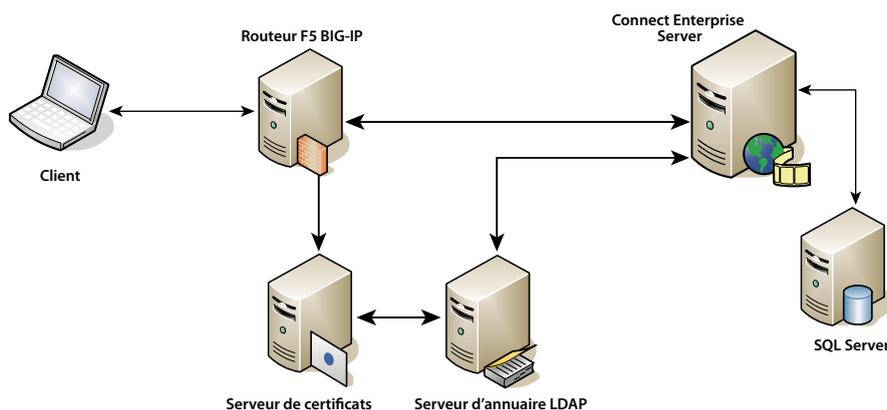
Vous pouvez concevoir un système PKI qui ne requiert que l'authentification des connexions HTTP ou des connexions HTTP et RTMP. Si vous exigez des certificats côté client pour les connexions HTTP et RTMP, le système interroge les utilisateurs à chaque nouvelle connexion au serveur. Par exemple, ils devront 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.

## Implémentation d'une infrastructure PKI pour Connect Enterprise

La procédure suivante vous guide tout au long de l'implémentation de l'infrastructure PKI 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 respecte des normes de sécurité rigoureuses, par exemple, elle exige un certificat coté client pour les connexions HTTP (serveur d'application) et RTMP (serveur de réunion).

**Remarque :** Adobe vous recommande fortement d'adopter une stratégie de sécurité avant d'implémenter l'infrastructure PKI. PKI exploite 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 :

- Connect Enterprise Server est installé.
- Connect Enterprise Server est intégré à un service d'annuaire LDAP.
- Un utilisateur importé depuis le service d'annuaire LDAP peut accéder à une réunion de Connect Enterprise.
- 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.

Le routeur F5 iRule recherche l'adresse électronique dans l'objet `X.509::subject` et insère la valeur dans l'en-tête HTTP utilisé par Connect Enterprise pour authentifier l'utilisateur.

**Remarque :** Cet exemple utilise l'attribut `email`, mais vous pouvez utiliser n'importe quel identifiant unique qui est exposé par le format `X.509`, d'une longueur maximale de 254 caractères et partagé par le service d'annuaire LDAP et Connect Enterprise.

### 2. Définition de la stratégie de connexion de Connect Enterprise

Connect Enterprise doit utiliser une adresse électronique comme identifiant de l'utilisateur. Dans Enterprise Manager, 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 devrait ressembler à cela :

```
E = adavis@asp.sflab.macromedia.com
CN = Andrew Davis
CN = Users
DC = asp
DC = sflab
DC = macromedia
DC = com
```

#### 4. Configurez Connect Enterprise Server pour qu'il utilise l'authentification d'en-tête 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>
```

Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Enterprise Server et Arrêter Adobe Connect Enterprise Meeting Server pour arrêter le serveur. 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 Connect Enterprise.

#### 5. Configurez la logique applicative du routeur F5.

Cette logique recherche l'adresse électronique dans le champ d'objet du certificat du client et la transmet à Connect Enterprise 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. OSCP (Online Certification Status Protocol) et la recherche LDAP sont des exemples de mécanismes d'authentification.

Après l'authentification du certificat, recherchez-y un identifiant unique connu de Connect Enterprise. 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. (Connect Enterprise 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 Connect Enterprise. Pour connecter un utilisateur, placez l'identifiant unique (dans ce cas, l'adresse électronique) dans le champ `HTTP_AUTH_HEADER` et redirigez la requête à la page de connexion de Connect Enterprise.

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 $emailAddr
}
elseif { [HTTP::uri contains "session" ] }
{
  #do nothing, Connect Enterprise verifies the token found in session=$token
}
else
{
  # URI encode the current request, and pass it to
  # the Connect Enterprise 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 de Connect Enterprise Server » à la page 20

« Configuration de l'authentification des en-têtes HTTP » à la page 38

# 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 Acrobat Connect Professional.

Lorsque l'extension Acrobat Connect Add-in est nécessaire, elle est téléchargée depuis un serveur Adobe par un processus transparent que l'utilisateur ne voit pas. Toutefois, si votre organisation 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 enregistrés 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 l'extension Acrobat Connect Add-in lorsqu'elle n'est pas installée 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 ou utiliser celle que fournit Adobe. La page d'Adobe est traduite dans toutes les langues prises en charge.

### Envoyer directement les utilisateurs vers les fichiers exécutables :

**1** Recherchez les fichiers de langue XML Connect Enterprise sur le serveur hébergeant Connect Enterprise. Les fichiers XML se trouvent dans ces deux répertoires :`[root_install_dir]\appserv\web\common\intro\lang` et `[root_install_dir]\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/AdobeConnectAddin.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'extension. Vous pouvez modifier ces emplacements sur votre serveur et modifier les chemins d'accès en conséquence dans la section `addInLocation`.

### Envoyer les utilisateurs vers les pages d'instructions de téléchargement fournies par Adobe :

**1** Recherchez les fichiers de langue XML Connect Enterprise sur le serveur hébergeant Connect Enterprise. Les fichiers XML se trouvent dans ces deux répertoires :`[root_install_dir]\appserv\web\common\intro\lang` et `[root_install_dir]\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#` que Connect Enterprise 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'extension sur Connect Enterprise Server (`/common/addin/setup.exe` et `/common/addin/AdobeConnectAddin.z`). Si

vous modifiez l'emplacement des fichiers exécutables, actualisez les liens de la page `addindownload.htm` pour chaque langue.

#### Envoyer les utilisateurs vers vos propres pages d'instructions de téléchargement :

**1** Recherchez les fichiers de langue XML Connect Enterprise sur le serveur hébergeant Connect Enterprise. Les fichiers XML se trouvent dans ces deux répertoires : `[root_install_dir]\appserv\web\common\intro\lang` et `[root_install_dir]\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'extension pour chaque plate-forme.

## Tampons de tableau blanc personnalisés

### A propos des tableaux blancs

Vous pouvez utiliser un tableau blanc dans Acrobat Connect Professional pour taper du texte, tracer des lignes, des cercles, des carrés ou d'autres formes libres en temps réel pendant une réunion.

Le tableau blanc comprend des tampons qui vous permettent de laisser une coche, une flèche, une étoile ou une croix sur l'écran. La coche est le tampon appliqué par défaut. Vous pouvez modifier l'image du tampon en cliquant sur les boutons coche, flèche et étoile. La couleur et la taille de l'image peuvent être personnalisées à l'aide du sélecteur de couleurs et du menu déroulant. Vous pouvez également créer vos propres tampons personnalisés.

### Création de tampons personnalisés

Pour créer des tampons personnalisés pour l'outil Tableau blanc, créez une bibliothèque de symboles d'animations dans Macromedia Flash d'Adobe. Créez un fichier ActionScript (.as) et rédigez du code pour relier l'intitulé de chaque tampon à son symbole d'animation. Publiez la bibliothèque de tampons personnalisés sous forme de fichier SWF et copiez ce dernier et le fichier AS dans Connect Enterprise Server.

Pour plus d'informations, consultez l'article « Création de tampons de tableau blanc personnalisés pour Connect Enterprise » sur le Centre des développeurs Adobe Connect Enterprise ([www.adobe.com/go/devnet\\_connect\\_stamps\\_fr](http://www.adobe.com/go/devnet_connect_stamps_fr)).

# Chapitre 6 : Vérification de votre installation

Les tâches de ce chapitre vous aideront à vérifier qu'Adobe Connect Enterprise Server est bien installé. Certaines ne sont applicables que si vous disposez d'une licence pour un module Connect Enterprise particulier.

## Tâches de vérification de l'installation

### Vérification de la connectivité de la base de données

Si vous pouvez vous connecter à Adobe Connect Enterprise Manager (application Web située dans Connect Enterprise Server), la base de données et Connect Enterprise Server 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 Enterprise 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 Enterprise Manager 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, Connect Enterprise Server n'enverra pas de notifications électroniques et vous pouvez ignorer cette section.

1 Dans l'onglet d'accueil de Connect Enterprise Manager, 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, Connect Enterprise Server 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 Connect Enterprise avec un hôte SMTP valide et que le service SMTP fonctionne en dehors de Connect Enterprise.

d Contactez l'Assistance technique d'Adobe à l'adresse [www.adobe.com/go/connect\\_licensed\\_programs\\_fr](http://www.adobe.com/go/connect_licensed_programs_fr).

## Vérification du bon fonctionnement du module Presenter

Pour vérifier le bon fonctionnement de Connect Enterprise Server, envoyez une présentation Microsoft PowerPoint à Connect Enterprise Server pour sa compilation en présentation Flash, puis affichez-la.

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

- 1 Insérez le CD d'Adobe Connect Enterprise.
- 2 Cliquez sur Installer Adobe Presenter 6 et suivez les instructions.
- 3 Si vous n'avez pas de présentation PowerPoint à envoyer à Connect Enterprise Server 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 Server en choisissant Publier dans le menu Adobe Presenter de PowerPoint.
- 5 Sélectionnez Connect Enterprise Server 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 Enterprise Manager).

Lorsque toutes les étapes de l'Assistant sont terminées, votre présentation PowerPoint est transférée dans le serveur Connect Enterprise Server et compilée en présentation Flash.

- 7 A la fin de la compilation, ouvrez l'onglet Contenu dans Connect Enterprise Manager et recherchez votre présentation.
- 8 Ouvrez votre présentation pour l'afficher.

## Vérification du bon fonctionnement du module Formation

*Remarque :* Adobe Connect Training 6 est une fonctionnalité optionnelle qui doit être activée dans votre licence.

❖ Dans Connect Enterprise Manager, cliquez sur l'onglet Formation.

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

## Vérification du bon fonctionnement d'Acrobat Connect Professional

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

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

- 1 Connectez-vous à Connect Enterprise Manager 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 enregistrés 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 enregistré.
- 6 Si la fenêtre Acrobat Connect Add-in apparaît, suivez les instructions pour installer cette extension.

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

## Vérification du bon fonctionnement du module Séminaires

*Remarque : Acrobat Connect Professional Seminars est une fonctionnalité optionnelle qui doit être activée dans votre licence.*

- 1 Connectez-vous à Connect Enterprise Manager en tant qu'utilisateur membre du groupe Hôtes de séminaires ou du groupe Administrateurs.
- 2 Dans Connect Enterprise Manager, ouvrez l'onglet Séminaires.
- 3 Naviguez jusqu'à un dossier dans la bibliothèque des séminaires, ou créez-en un nouveau, puis cliquez sur Nouveau séminaire.
- 4 Dans la page Entrer les informations sur la réunion, entrez les informations requises. Pour l'option Accès au séminaire, choisissez Seuls les utilisateurs enregistrés et les visiteurs acceptés sont admis à la réunion, puis cliquez sur Terminer.
- 5 Cliquez sur l'adresse URL du séminaire.
- 6 Identifiez-vous pour participer au séminaire en tant qu'utilisateur enregistré.

Si la salle du séminaire apparaît, le module fonctionne correctement.

## Vérification du bon fonctionnement du module Événements

*Remarque : Adobe Connect Events 6 est une fonctionnalité optionnelle qui doit être activée dans votre licence.*

- 1 Connectez-vous à Connect Enterprise Manager en tant qu'utilisateur membre du groupe Gestionnaire d'événements ou du groupe Administrateurs.
- 2 Dans Connect Enterprise Manager, ouvrez l'onglet Événements.

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

## Vérification de l'équilibrage de charge du cluster et du basculement des réunions

Lorsqu'une réunion commence, le serveur d'application 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.

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

Dans la procédure suivante, le cluster contient deux ordinateurs, Ordinateur1 et Ordinateur2.

- 1 Démarrez Connect Enterprise Server sur les deux ordinateurs.
  - a Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Meeting Server.
  - b Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Enterprise Server.
- 2 Connectez-vous à Connect Enterprise Manager depuis l'URL suivante :

`http://[nomhôte]`

Pour *nomhôte*, utilisez la valeur d'Hôte Connect Enterprise 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 Connect Enterprise Server sur Ordinateur2.
  - a Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Enterprise Server.
  - b Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Meeting Server.

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

**5** Dans Connect Enterprise Manager, cliquez sur un onglet ou un lien quelconque.

Si l'équilibreur de charge fonctionne, vous devez encore pouvoir envoyer des requêtes à Enterprise Manager et recevoir des réponses.

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

### Voir aussi

« Choix du déploiement de Connect Enterprise dans un cluster » à la page 13

### Vérification de la réplication de contenu

Il est préférable de vérifier que le contenu chargé sur un serveur Connect Enterprise d'un cluster est bien répliqué sur les autres ordinateurs du cluster. Dans la procédure suivante, le cluster contient deux ordinateurs sur lesquels est installé Adobe Presenter, Ordinateur1 et Ordinateur2.

**1** Démarrez Connect Enterprise Server sur Ordinateur1.

**a** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Meeting Server.

**b** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Démarrer Adobe Connect Enterprise Server.

**2** Arrêtez Connect Enterprise Server sur Ordinateur2.

**a** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Enterprise Server.

**b** Choisissez Démarrer > Tous les programmes > Adobe Connect Enterprise Server > Arrêter Adobe Connect Meeting Server.

**3** Connectez-vous à Connect Enterprise Manager depuis l'URL suivante :

`http://[nomhôte]`

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

**4** Transférez une image JPEG ou un autre contenu dans Connect Enterprise Server sur l'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 Enterprise Manager.)
- 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 conduisant au 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 l'Ordinateur2, attendez que Connect Enterprise ait pleinement démarré, puis arrêtez l'Ordinateur1.

Si vous avez configuré un périphérique de stockage externe, il n'est pas nécessaire d'attendre que l'Ordinateur2 s'arrête ; le contenu requis est copié depuis le 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 l'Ordinateur2 fonctionne. Une fenêtre vide ou un message d'erreur signifie que la réplication n'a pas fonctionné.

**Voir aussi**

« Choix du déploiement de Connect Enterprise dans un cluster » à la page 13

# Chapitre 7 : Sécurisation de Connect Enterprise

La sécurisation d'Adobe Connect Enterprise protège votre organisation contre les pertes de biens et les actes de malveillance. Il est important de sécuriser l'infrastructure de votre organisation, Adobe Connect Enterprise Server et le serveur de base de données utilisé par Connect Enterprise Server. Vous pouvez également choisir de configurer SSL afin de sécuriser toutes les connexions à Connect Enterprise Server. Pour plus d'informations, visitez la page [www.adobe.com/go/connect\\_ssl\\_fr](http://www.adobe.com/go/connect_ssl_fr). Connect Enterprise prend également en charge l'infrastructure PKI. Pour plus d'informations, consultez la section « Infrastructure de clé publique (PKI) » à la page 42.

## Sécurisation de l'infrastructure

### Sécurisation du réseau

Pour ses communications, Connect Enterprise Server s'appuie sur plusieurs services TCP/IP privés. Ces services ouvrent plusieurs ports et canaux qui doivent être protégés des utilisateurs extérieurs. Connect Enterprise Server 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 Connect Enterprise consiste à bloquer tous les ports du serveur à l'exception des ports 80, 1935 et 443. Un pare-feu matériel externe offre une couche de protection pour pallier les défauts du système d'exploitation. Vous pouvez configurer plusieurs couches de pare-feux matériels pour former des zones protégées (DMZ). Si votre service informatique applique scrupuleusement tous les patches de sécurité publiés par 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 Connect Enterprise Server sur votre réseau intranet, il est préférable de placer les serveurs Connect Enterprise et leur base de données sur un sous-réseau distinct, isolé par un pare-feu. Le segment de réseau interne sur lequel est installé Connect Enterprise Server 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'information, voir la rubrique RFC 1918. La configuration de ce pare-feu doit tenir compte de tous les ports de Connect Enterprise Server et de leur paramétrage pour un trafic entrant ou sortant.

### Accès Internet

Si certains de vos utilisateurs doivent accéder à Connect Enterprise Server par Internet, il est essentiel que vous isoliez les serveurs Connect Enterprise d'Internet par un pare-feu. Si vous ne prenez pas les mesures nécessaires pour sécuriser vos serveurs Connect Enterprise, vous exposez vos informations essentielles au vol et au piratage.

### Sécurisation du serveur de base de données

Que vous hébergiez ou non votre base de données sur le même serveur que Connect Enterprise Server, 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 organisation.
- Ne connectez jamais la base de données directement à Internet.

- Sauvegardez régulièrement toutes les données et stockez les copies dans un emplacement protégé hors-site.
- Installez les derniers patches publiés pour votre serveur de base de données.

Pour plus d'informations sur la sécurisation de SQL Server 2000 et 2005 et du moteur de base de données intégré, consultez le site Web relatif à la sécurité de Microsoft SQL.

Vous trouverez également une liste de procédures qui vous permettront de sécuriser votre base de données dans l'article de Microsoft « 10 Steps to Help Secure SQL Server 2000 ».

## Sécurisation de Connect Enterprise Server

### Création de comptes de service

La création d'un compte de service pour Connect Enterprise vous permet d'exécuter Connect Enterprise de façon plus sécurisée. Adobe recommande la création d'un compte de service Connect Enterprise Server et d'un compte de service MSDE. Pour plus d'informations, consultez les articles de Microsoft « How to change the SQL Server or SQL Server Agent service account without using SQL Enterprise Manager in SQL Server 2000 or SQL Server Configuration Manager in SQL Server 2005 » et « The Services and Service Accounts Security and Planning Guide ».

#### Création d'un compte de service Connect Enterprise

- 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 de Connect Enterprise (C:\breeze, par défaut).

Les sous-dossiers et les fichiers doivent disposer des mêmes autorisations. Dans le cas de clusters, vous devez modifier le chemin correspondant sur chaque nœud d'ordinateurs.

- 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, vous devez modifier le chemin correspondant sur chaque nœud d'ordinateurs.
- 5 Définissez les droits d'utilisateur suivants pour le service ConnectSqlService :

Agir comme faisant partie du système d'exploitation—SeTcbPrivilege Bypass traverse checking—SeChangeNotify Verrouillage des 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 de Connect Enterprise Server sur un ordinateur unique. Elle part du principe que la base de données est installée sur le même ordinateur et que les utilisateurs accéderont à Connect Enterprise par Internet.

### 1. Installez un pare-feu.

Si vous laissez les utilisateurs accéder à Connect Enterprise Server 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 uniquement le protocole TCP/IP.

La base de données étant située sur le même serveur que Connect Enterprise, il n'est pas nécessaire d'ouvrir le port 1434 sur le pare-feu.

### 3. Installez Connect Enterprise Server.

### 4. Vérifiez le bon fonctionnement des applications Connect Enterprise Server.

Après son installation, pensez à vérifier que Connect Enterprise Server 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.

## Voir aussi

« Vérification de votre installation » à la page 47

## Sécurisation des clusters

Les systèmes de clusters (multi-serveurs) sont par nature plus complexes que les configurations à serveur unique. Un cluster Connect Enterprise Server 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 Enterprise Server 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, pas le moteur de base de données intégré.

Voici quelques suggestions essentielles pour la sécurisation des clusters.

**Réseaux privés** La solution la plus simple pour les clusters situés dans le même site consiste à créer un sous-réseau supplémentaire pour le système Connect Enterprise. Cette approche offre un haut niveau de sécurité.

**Pare-feux logiciels locaux** Pour les serveurs Connect Enterprise situés dans un cluster mais partageant un réseau public avec d'autres serveurs, un pare-feu logiciel installé sur chaque serveur individuel peut être approprié.

**Systèmes VPN** Dans les installations multi-serveurs où plusieurs ordinateurs hébergeant Connect Enterprise Server sont situés dans des sites différents, vous pouvez envisager d'utiliser un canal crypté pour communiquer avec les serveurs distants. De nombreux fournisseurs proposent des technologies de VPN permettant de sécuriser les communications avec les serveurs distants. Si le trafic des données doit être crypté, Connect Enterprise s'appuie sur cette sécurité externe.

## Ressources et conseils en matière de sécurité

### Recommandations en matière de sécurité

La liste de vérification suivante présente des recommandations qui vous aideront à sécuriser votre système Connect Enterprise Server.

**Protection du trafic réseau par SSL** Pour plus d'informations, visitez la page [www.adobe.com/go/connect\\_ssl\\_fr](http://www.adobe.com/go/connect_ssl_fr).

**Exécution des 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 que Connect Enterprise. En réduisant le nombre d'applications et de services exécutés sur l'ordinateur qui héberge Connect Enterprise Server, vous limiterez les risques que ce serveur soit attaqué via les failles de sécurité d'une autre application.

**Mise à jour de la sécurité du système d'exploitation** Vérifiez régulièrement la publication de mises à jour critiques corrigeant des failles de sécurité et appliquez les patches requis. Un pare-feu permet d'éliminer certains de ces problèmes de sécurité. De façon générale, il est préférable d'appliquer à vos serveurs tous les patches de sécurité publiés et approuvés par Microsoft et les fournisseurs des autres plates-formes concernées.

**Sécurisation des systèmes hôtes** Si vous stockez des informations « sensibles » sur vos serveurs, veillez à la protection physique de vos systèmes. Connect Enterprise Server dépend de la sécurisation de l'ordinateur hôte. Ce dernier doit donc être protégé contre les intrusions s'il contient des données personnelles et confidentielles. Connect Enterprise Server est conçu pour tirer parti des fonctionnalités natives de l'environnement, telles que le cryptage du système de fichiers.

**Utilisation de mots de passe renforcés** Les utilisateurs Connect Enterprise sont protégés par des mots de passe. Il est recommandé que tous les utilisateurs, en particulier les administrateurs, choisissent des mots de passe difficiles à décrypter pour mieux protéger leurs données. Les administrateurs de Connect Enterprise peuvent définir des stratégies de mot de passe et de connexion dans le gestionnaire Connect Enterprise Manager. Les installations Connect Enterprise Server utilisent souvent Microsoft SQL Server, qui requiert également une protection par des mots de passe difficiles à décrypter.

**Exécution régulière d'audits de la sécurité** Il est recommandé d'effectuer périodiquement 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 sécurisation

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 sécurisation 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 2000. 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. L'application Connect Enterprise Server n'est pas conçue pour assurer la sécurité de votre serveur ou des informations qu'il contient. Pour plus d'informations, consultez le Dédit de garantie énoncé dans le CLUF (Contrat de Licence d'Utilisateur Final) qui accompagne Connect Enterprise Server.

# Index

## A

Acrobat Connect Add-in *Voir* Adobe Acrobat Connect Add-in  
 Active Directory 27  
 Add-in, extension *Voir* Adobe Acrobat Connect Add-in  
 Administrateur de compte, création 19  
 Administrateur, création 19  
 Adobe Acrobat Connect Add-in hébergement 1, 45  
 PKI 42  
 Adobe Acrobat Connect Enterprise Manager  
 stratégie de connexion 41  
 vérification de la connectivité 47  
 Adobe Acrobat Connect Professional, vérification de l'installation 48  
 Adobe Acrobat Connect Professional Seminars, vérification de l'installation 49  
 Adobe Connect Edge Server  
 à propos de 15  
 démarrage et arrêt 22  
 déploiement 15, 25  
 équilibrage de charge 26  
 fichier de licence 22  
 installation 21  
 mappages de l'hôte 27  
 mise en cluster 1  
 Adobe Connect Enterprise Server  
 administrateur de compte 19  
 chemins de mise à niveau 7  
 configuration avec la Console de gestion des applications 18  
 configuration logicielle requise 5  
 configuration matérielle requise 4  
 connectivité de la base de données, vérification 47  
 démarrage et arrêt 20  
 déploiement 24  
 désinstallation 21  
 fichier de licence 19  
 Flash Media Server 10  
 installation 17  
 intégration du service d'annuaire 27  
 intégration LDAP 29  
 mise en cluster 13, 24  
 service 20

Adobe Connect Events, vérification de l'installation 49  
 Adobe Connect Training, vérification de l'installation 48  
 Adobe Presenter, vérification de l'installation 48  
 Apache 39  
 Assistance technique 3  
 Authentification  
 en-tête HTTP 7, 38  
 NTLM 38, 40  
 PKI 42, 44  
 présentation 38  
 Authentification d'en-tête HTTP  
 authentification unique 38  
 Authentification des en-têtes HTTP  
 à propos de 7, 38  
 PKI 42, 44  
 Authentification NTLM (NT LAN Manager)  
 à propos de 38  
 configuration 40  
 stratégie de connexion 41  
 Authentification unique  
 authentification 38  
 solutions prises en charge 7  
 stratégie de connexion 41  
 authentification unique  
 présentation 38  
 Autorité de certification 42, 43

## B

Basculement, vérification 50  
 Base de données  
 à propos des 11  
 choix 14  
 cluster 24  
 configuration 18, 25  
 configurations de serveur prises en charge 6  
 intégrée, installation 17  
 mise à niveau 8  
 ports 5  
 sauvegarde 9, 52  
 sécurité 52  
 SQL Server 24  
 vérification de sa connectivité 47  
 Base de données intégrée *Voir* Base de données

BIG-IP, routeur 42  
 BREEZESESSION, cookie 39, 44

## C

CA (autorité de certification) 42, 43  
 Cache, configuration 19  
 Certificat client 42  
 Certificats  
 client 1, 42  
 numériques 42  
 Certificats numériques 42  
 certificats numériques  
*Voir aussi* certificats  
 Clusters  
 déploiement 13  
 déploiement de Connect Enterprise Server 24  
 équilibrage de charge 25, 49  
 ports 5, 25  
 réplication de contenu 50  
 sécurisation 54  
 serveurs Edge 1  
 Comptes de service 53  
 Configuration logicielle requise  
 ordinateur hôte 5  
 Configuration matérielle requise  
 Connect Enterprise Server 4  
 Configuration requise  
 Connect Enterprise Server 4  
 PKI 42  
 Connect Add-in, extension *Voir* Adobe Acrobat Connect Add-in  
 Connect Edge Server *Voir* Adobe Connect Edge Server  
 Connect Enterprise Manager. *Voir* Adobe Acrobat Connect Enterprise Manager  
 Connect Enterprise Server *Voir* Adobe Connect Enterprise Server  
 Connect Events, vérification de l'installation 49  
 Connect Professional, vérification de l'installation 48  
 Connect Training, vérification de l'installation 48  
 Console de gestion des applications  
 onglet Créer un administrateur 19  
 onglet Paramètres de la base de données 18, 25  
 onglet Paramètres de licence 19

- onglet Paramètres du serveur 19, 25
  - onglet Paramètres du service d'annuaire 29
  - Paramètres du stockage partagé 35
  - Paramètres LDAP 29
  - présentation 18
  - Console de gestion *Voir* Console de gestion des applications
  - Contenu
    - mise en cache, configuration 19
    - périphériques de stockage pris en charge 7
    - stockage partagé 1, 19, 35
  - Créer un administrateur, onglet 19
  - custom.ini, fichier
    - paramètre HTTP\_AUTH\_HEADER 38
- D**
- DEFAULT\_FCS\_HOSTPORT, paramètre 26
  - Démarrage et arrêt de Connect Edge Server 20
  - Démarrage et arrêt de Connect Enterprise Server 20
  - Démarrer, menu 20
  - Dépannage 2
  - Désinstallation 21
  - DMZ (zone démilitarisée) 52
- E**
- eDirectory 27
  - Enterprise Manager. *Voir* Adobe Acrobat Connect Enterprise Manager
  - Équilibrage de charge
    - serveurs Edge 26
    - vérification 49
  - Événements, vérification de l'installation 49
- F**
- F5
    - iRule 44
    - routeur BIG-IP 42
  - FCS.HTTPCACHE\_BREEZE\_SERVER\_NORMAL\_PORT, paramètre 26
  - FCS\_EDGE\_CLUSTER\_ID, paramètre 26
  - FCS\_EDGE\_EXPIRY\_TIME, paramètre 26
  - FCS\_EDGE\_HOST, paramètre 26
  - FCS\_EDGE\_PASSWORD, paramètre 26
  - FCS\_EDGE\_REG\_INTERVAL, paramètre 26
  - FCS\_EDGE\_REGISTER\_HOST, paramètre 26
  - Fichier custom.ini
    - authentification d'en-tête HTTP 40
    - paramètre NTLM\_DOMAIN 40
    - paramètres de configuration du serveur Edge 26
  - Fichier de licence
    - Connect Edge Server 22
    - Connect Enterprise Server 19
  - Fichiers
    - custom.ini *Voir* Fichier custom.ini
    - licence 19, 22
  - Filtres
    - Java 38, 40
    - LDAP 29
  - Flash Media Server 10
    - Voir aussi* Adobe Connect Enterprise Server
  - Flash Media Server (FMS), service 20
  - Flash Media Server Administration Server, service 20
  - Flash Player 45
  - flux de données 11
  - FMS, service 20
  - Formation, vérification de l'installation 48
- G**
- Gestion de la mémoire *Voir* Contenu
  - Groupes, LDAP 28, 31
- H**
- HTTP
    - port 19
  - HTTP *Voir* HTTP
  - HTTP\_AUTH\_HEADER, paramètre 38
- I**
- IBM Directory Server 27
  - Infrastructure de clé publique (PKI)
    - Voir* PKI
  - Installation
    - Connect Edge Server 21
    - Connect Enterprise Server 17
    - vérification 47
  - Intégration du service d'annuaire
    - Voir* LDAP
  - iRule 44
- J**
- Java
    - filtre 38, 40
    - serveur d'application 10
  - Journaux, synchronisation 33
- L**
- LDAP
    - attribut 28
    - authentification unique 38
    - filtrage 29
    - gestion des mots de passe 32
    - groupes 31
    - importation d'utilisateurs et de groupes 28
    - importation de branches 28
    - intégration du service d'annuaire 27
    - intégration PKI 42
    - mappage du profil utilisateur 30
    - pagination des requêtes 1
    - sécuriser 1, 35
    - serveurs d'annuaire pris en charge 7
    - stratégie de mot de passe 32
    - structure d'annuaire 28
    - suppression de stratégie 32
    - synchronisation 32, 33
  - LDAPS 1, 35
  - Ligne de commande, démarrage et arrêt des services depuis 20
- M**
- Manager, stratégies de connexion 41
  - Mappage des profils utilisateur 30
  - Mappages de l'hôte 19, 25, 27
  - Mappages, hôte 19, 25, 27
  - Microsoft Active Directory 27
  - Microsoft SQL Server 5, 24
  - Microsoft Windows Server 5
  - Mise à niveau
    - base de données 8
    - chemins 7
    - information des utilisateurs 9
    - sauvegarde de la base de données 9
    - sauvegarde des fichiers 9
  - Moteur de base de données Microsoft (MSDE) *Voir* Base de données
  - Mots de passe
    - gestion (LDAP) 32
    - renforcés 55
    - stratégie (LDAP) 32
  - MSDE *Voir* Base de données

- N**
- NAS, périphérique 35
  - Netscape, serveur 27
  - NMap, outil 55
  - Nom de domaine pleinement qualifié (FQDN) 19, 25, 26
  - Nom unique 28
  - Notifications électroniques 47
  - Notifications électroniques, vérification 47
  - Nouveautés 1
  - Novell eDirectory 27
  - NTLM (Gestionnaire NT LAN) 7
  - NTLM\_DOMAIN, paramètre 40
- O**
- One Directory Server 27
  - OpenLDAP 27
- P**
- Paramètres de la base de données, onglet 25
  - Paramètres de licence, onglet 19
  - Paramètres du serveur, onglet 19
  - Paramètres du service d'annuaire, onglet 29
  - Paramètres LDAP 29
  - Pare-feux, configuration 52, 54
  - PKI
    - configuration requise 42
    - implémentation de référence 42
    - présentation 1, 42
  - Ports
    - base de données 18
    - HTTP 19
    - liste 5
    - outil de scanner 55
    - protection 52
    - pour un cluster Connect Enterprise 25
  - Présentation technique 10
  - Présentation technique d'Adobe Connect Enterprise Server 10
  - Presenter, vérification de l'installation 48
  - Profils, utilisateurs et groupes LDAP 30
  - Protocoles
    - HTTP 11, 19
    - HTTPS 11
    - LDAP 7, 27
    - LDAPS 35
    - RTMP 11
    - RTMPS 11
    - SMTP 5, 19
  - protocoles
- R**
- Ressources de sécurité 55
  - Réunion *Voir* Adobe Acrobat Connect Professional
  - Routeur F5 42
  - RTMP (real-time messaging protocol) 5, 11
  - RTMP *Voir* RTMP
- S**
- SAN, périphérique 35
  - Sécurité
    - clusters 54
    - comptes de service 53
    - installation à serveur unique 54
    - liste de vérification 55
    - PKI 1, 42
    - réseau 52
  - Sécurité du réseau 52
  - Séminaires, vérification de l'installation 49
  - Serveur d'application 10
  - Serveur de réunions 10
  - Serveur Edge *Voir* Adobe Connect Edge Server
  - Serveurs d'annuaire pris en charge 7
  - Serveurs Web 5, 39
  - Service, comptes 53
  - Services, fenêtre 20, 22
  - session, paramètre 39
  - SMTP
    - paramètres 19
    - présentation 5
  - SMTP *Voir* SMTP
  - SQL Server 5, 24
  - Stockage partagé
    - configuration 36
    - paramètre du serveur 19
    - présentation 1, 35
  - Stockage partagé *Voir* Contenu
  - Stratégies de connexion 41, 43
  - Sun One Directory Server 27
  - Support technique 3
  - Synchronisation 33
  - Système d'exploitation 64 bits 1
  - Systèmes d'exploitation
    - 64 bits 1
    - sécurité 55
- T**
- Tableau blanc, tampons personnalisés 1, 46
  - Tampons personnalisés, tableau blanc 1, 46
  - Tampons, tableau blanc 1, 46
- U**
- Utilisateurs et groupes, LDAP 28
- W**
- Windows Server 5
- X**
- X.509, standard 42