



Installation et configuration de Breeze Edge Server

Marques commerciales

1 Step RoboPDF, ActiveEdit, ActiveTest, Authorware, Blue Sky Software, Blue Sky, Breeze, Breezo, Captivate, Central, ColdFusion, Contribute, Database Explorer, Director, Dreamweaver, Fireworks, Flash, FlashCast, FlashHelp, Flash Lite, FlashPaper, Flex, Flex Builder, Fontographer, FreeHand, Generator, HomeSite, JRun, MacRecorder, Macromedia, MXML, RoboEngine, RoboHelp, RoboInfo, RoboPDF, Roundtrip, Roundtrip HTML, Shockwave, SoundEdit, Studio MX, UltraDev et WebHelp sont des marques déposées ou des marques commerciales de Macromedia, Inc. et peuvent être déposées aux États-Unis et dans d'autres juridictions ou pays. Les autres noms de produits, logos, designs, titres, mot ou expressions mentionnés dans cette publication peuvent être des marques commerciales, des marques de service ou des noms commerciaux de Macromedia, Inc. ou d'autres entités et peuvent être enregistrées dans certaines juridictions, notamment internationalement.

Informations au sujet des parties tierces

Ce guide contient des liens vers des sites tiers qui ne sont pas sous le contrôle de Macromedia et Macromedia n'est pas responsable du contenu de ces sites. Si vous accédez à un site Web tiers mentionné dans ce guide, vous le faites à vos propres risques. Macromedia fournit ces liens à des fins pratiques et l'inclusion de ces liens n'implique pas que Macromedia parraine ou accepte la moindre responsabilité pour le contenu de ces sites Web tiers.

Copyright © 2005 Macromedia, Inc. Tous droits réservés. Ce manuel ne peut pas être copié, photocopié, reproduit, traduit ou converti sous forme électronique ou informatique, en partie ou en totalité, sans l'autorisation écrite préalable de Macromedia, Inc. Nonobstant les dispositions précédentes, le propriétaire ou l'utilisateur autorisé d'un exemplaire valide du logiciel accompagnant le présent manuel peut imprimer un exemplaire de ce manuel à partir de sa version électronique à des fins d'apprentissage d'utilisation de ce logiciel uniquement, sous réserve qu'aucune partie de ce manuel ne soit imprimée, reproduite, distribuée, revendue ou transmise à toute autre fin, y compris mais sans s'y limiter, à des fins commerciales, telle que la vente d'exemplaires de la présente documentation ou l'offre de services d'assistance technique payants.

Remerciements

Gestion du projet : Stephanie Gowin

Rédaction : John Norton

Révision : John Hammett

Gestion de la production : Patrice O'Neill

Conception et production : Adam Barnett, John Francis, Mario Reynoso

Première édition : Mai 2005

Macromedia, Inc.
601 Townsend St.
San Francisco, CA 94103

TABLE DES MATIÈRES

Macromedia Breeze Edge Server	5
Présentation des serveurs Edge.....	6
Connexion à Breeze par le biais de serveurs Edge.....	8
Configuration requise	8
Installation de Breeze Edge Server	9
Fichier de licence de Breeze Edge Server	13
Configuration de FCS pour Breeze Edge Server.....	13
Configuration de FCS pour SSL	15
Arrêt et démarrage de Breeze Edge Server	21
Déploiement d'un cluster de serveurs Edge	22
Planification de la maintenance.....	23

Macromedia Breeze Edge Server

Pour réussir l'installation et la configuration de Macromedia Breeze Edge Server, les informations présentées dans ce document vous seront utiles. Il comprend les sections suivantes :

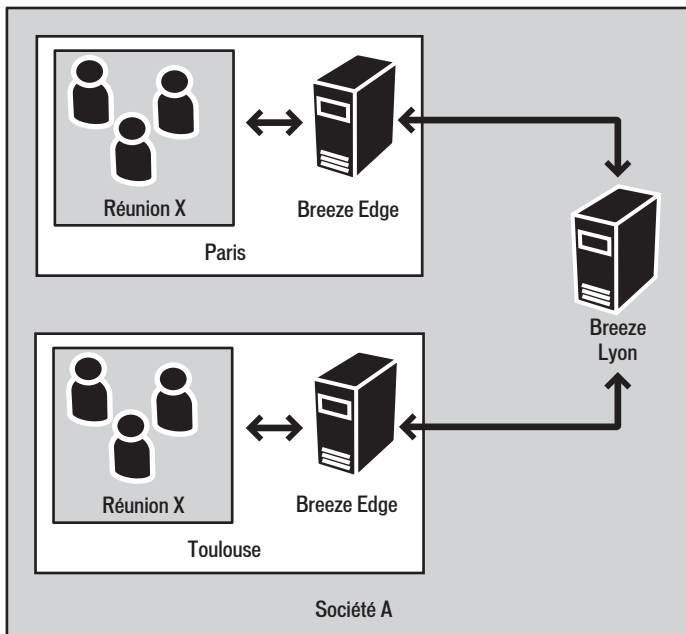
- *Présentation des serveurs Edge*, page 6
- *Connexion à Breeze par le biais de serveurs Edge*, page 8
- *Configuration requise*, page 8
- *Installation de Breeze Edge Server*, page 9
- *Fichier de licence de Breeze Edge Server*, page 13
- *Configuration de FCS pour Breeze Edge Server*, page 13
- *Mappage de l'entrée DNS pour un serveur Breeze Edge*, page 14
- *Configuration de FCS pour SSL*, page 15
- *Autres implémentations SSL*, page 16
- *Tunnellisation HTTP*, page 16
- *Ajout des balises SSL requises au fichier Adaptor.xml*, page 16
- *Repérage des balises SSL requises dans le fichier Server.xml*, page 16
- *Arrêt et démarrage de Breeze Edge Server*, page 21
- *Déploiement d'un cluster de serveurs Edge*, page 22
- *Planification de la maintenance*, page 23

Présentation des serveurs Edge

Les serveurs Edge sont configurés pour autoriser et équilibrer les demandes d'accès à un serveur Breeze par une utilisation plus efficace des ressources de bande passante disponibles. Lorsque des serveurs Edge sont déployés, les utilisateurs accèdent à Breeze par le biais de ces serveurs. Les serveurs Edge procèdent à l'authentification des utilisateurs et valident leurs demandes de services Web tels que Macromedia Breeze Meeting au lieu de transmettre chaque demande au serveur Breeze et de mobiliser ses ressources pour ce type d'opération. Si les données requises figurent dans la mémoire cache du serveur Edge, ce dernier renvoie les données Breeze Meeting au client (ordinateur) qui a émis la demande sans passer par le serveur Breeze. Ce détour est transparent pour les utilisateurs. Dans un tel cas de figure, aucune demande n'est envoyée au serveur Breeze d'origine.

Si les données requises ne figurent pas dans la mémoire cache du serveur Edge, ce dernier transmet la demande du client au serveur Breeze, lequel procède à l'authentification du client et valide la demande de services. Le serveur Breeze renvoie alors les résultats au serveur Edge qui lui a transmis la demande et ce dernier les fait suivre au client concerné. Le serveur Edge stocke également ces informations dans sa mémoire cache, permettant ainsi à d'autres utilisateurs authentifiés d'y accéder. Dans ce cas de figure, une quantité moins importante de demandes de services est transmise au serveur Breeze d'origine.

Un serveur Edge est configuré pour intercepter les demandes de services Breeze émanant d'une zone particulière, pour rassembler ou cumuler ces demandes et pour les transmettre au serveur Breeze d'origine. Le serveur Breeze renvoie les résultats au serveur Edge, qui les fait suivre à l'ordinateur client. Un déploiement Breeze en réseau peut comporter plusieurs serveurs Edge. Par exemple, un serveur Edge peut cumuler et transmettre les demandes provenant de Toulouse tandis qu'un autre peut cumuler et transmettre les demandes provenant de Paris. Chacun de ces serveurs rassemble les demandes émanant de ses clients et les envoie au serveur Breeze d'origine situé dans le centre de données de Lyon, puis il reçoit les réponses du serveur d'origine et les fait suivre aux clients de la zone qu'il dessert.



Connexion à Breeze par le biais de serveurs Edge

Lorsque des serveurs Edge sont présents sur le réseau d'une entreprise, les utilisateurs de Breeze se connectent à Breeze Meeting de manière indirecte, par le biais de ces serveurs (ou proxy). Cette connexion s'effectue de manière transparente. Les utilisateurs de Breeze ont l'impression d'être connectés directement au serveur Breeze qui héberge Breeze Meeting, bien qu'ils soient très probablement connectés par le biais du serveur Edge (serveur proxy) qui dessert leur réseau local. Les serveurs Edge allègent le trafic vers le serveur Breeze d'origine en mettant en mémoire cache les contenus statiques tels que les présentations et les réunions Breeze enregistrées.

Ces opérations s'effectuent en évitant la connexion réseau au serveur Breeze. Le client (ordinateur de l'utilisateur) se connecte au serveur Edge (proxy) au lieu de se connecter directement au serveur Flash Communication Server (FCS) (Breeze Meeting) et le serveur Edge se connecte au serveur Breeze d'origine. De nombreuses autres étapes, telles que l'authentification et la validation des autorisations, sont masquées pour l'utilisateur de Breeze.

Les serveurs Edge constituent une couche de défense supplémentaire entre la connexion Internet de l'utilisateur et le serveur Breeze. En effet, tout le trafic en provenance de l'Internet et en direction de Breeze passe par ces serveurs.

Configuration requise

Cette version de Breeze Edge Server est homologuée pour prendre en charge jusqu'à 500 utilisateurs ou 50 salles de réunion. Le tableau ci-après indique la configuration requise pour la mise en oeuvre de serveurs Edge.

Composant	Configuration requise
Système d'exploitation	Windows Server 2000 Windows Server 2003
Processeur du serveur	Pentium 4 3.6 GHz
Processeur à mémoire cache	Processeur à mémoire cache de 2 Mo
Mémoire	4 Go de RAM (configuration recommandée) 2 Go de RAM (configuration minimale)
Disque dur	80 Go à 10 000 tours/minute (configuration recommandée) 40 Go à 7 200 tours/minute (configuration minimale)
Adaptateur réseau	Adaptateur TCP/IP prenant en charge 1 Go via Ethernet CAT5
Affichage	SGVA prenant en charge une résolution de 800x600 ou supérieure
Lecteur	CD-ROM ou DVD-ROM

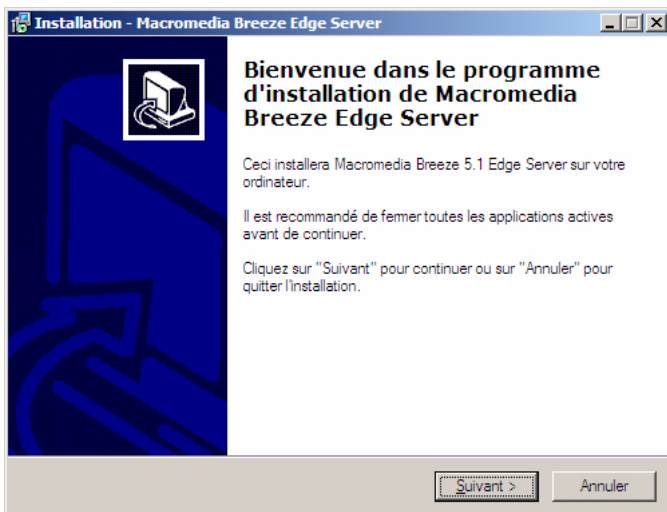
Installation de Breeze Edge Server

Pour installer Breeze Edge Server, suivez les procédures décrites dans cette section. Macromedia vous recommande de fermer toutes les autres applications avant de lancer l'installation.

Pour installer et configurer Breeze Edge Server :

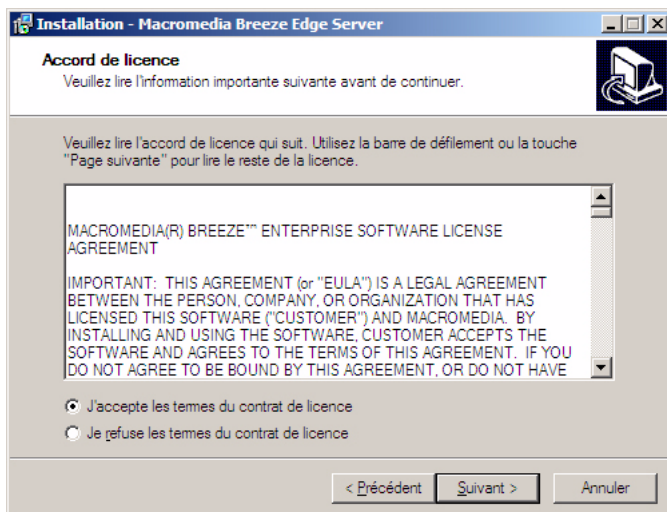
1. Insérez le CD d'installation dans le lecteur de CD-ROM. Si l'assistant d'installation Macromedia Breeze Edge Server ne démarre pas automatiquement, double-cliquez sur le fichier setup.exe dans le dossier racine du CD d'installation.

L'écran de bienvenue de l'assistant d'installation de Macromedia Breeze Edge Server apparaît.



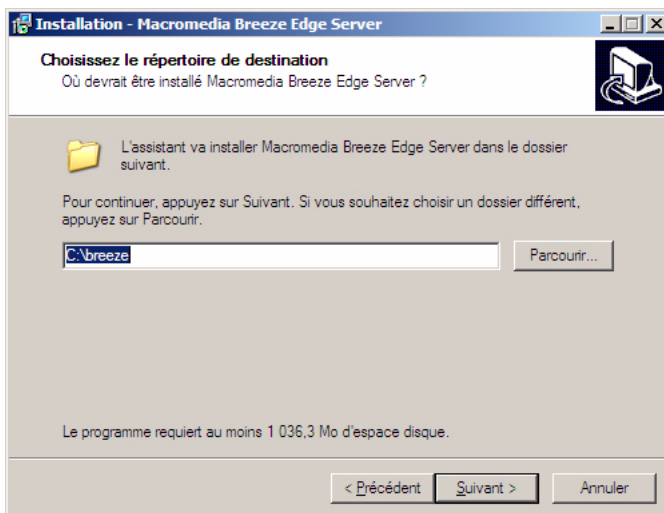
2. Cliquez sur Suivant pour continuer.

L'écran du contrat de licence apparaît.



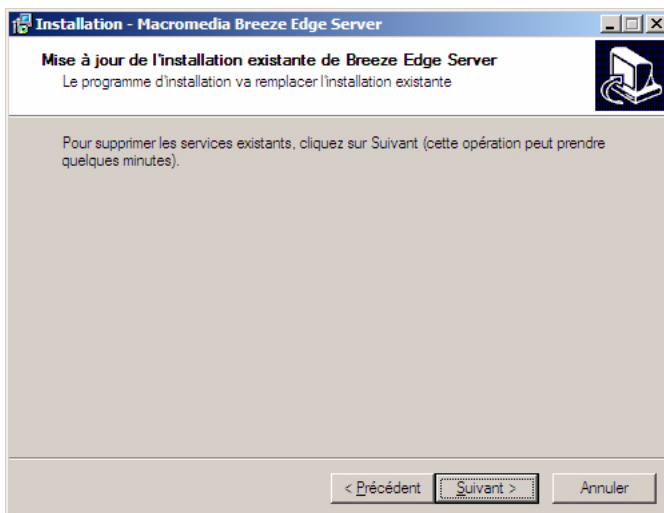
3. Lisez le contrat, indiquez que vous acceptez les termes de ce contrat en sélectionnant le bouton d'option correspondant, puis cliquez sur Suivant pour continuer.

L'écran de sélection de l'emplacement de destination apparaît.



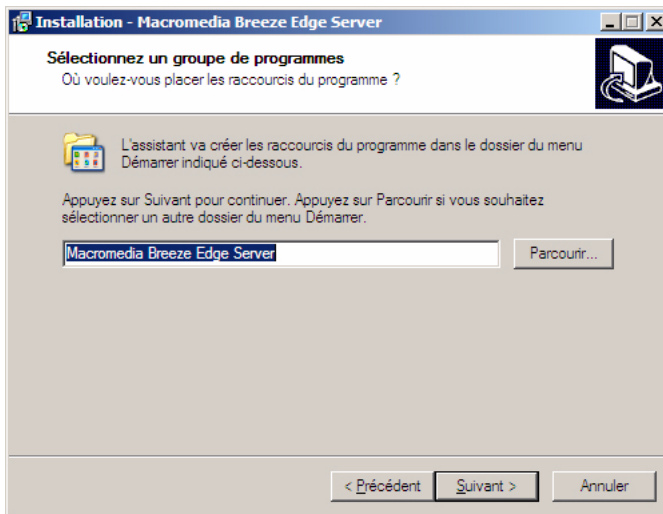
4. Cliquez sur Suivant pour accepter l'emplacement d'installation par défaut ou sélectionnez Parcourir pour choisir un autre emplacement, puis cliquez sur Suivant.

Si l'assistant détecte une installation précédente de Breeze Edge Server, l'écran suivant s'affiche.



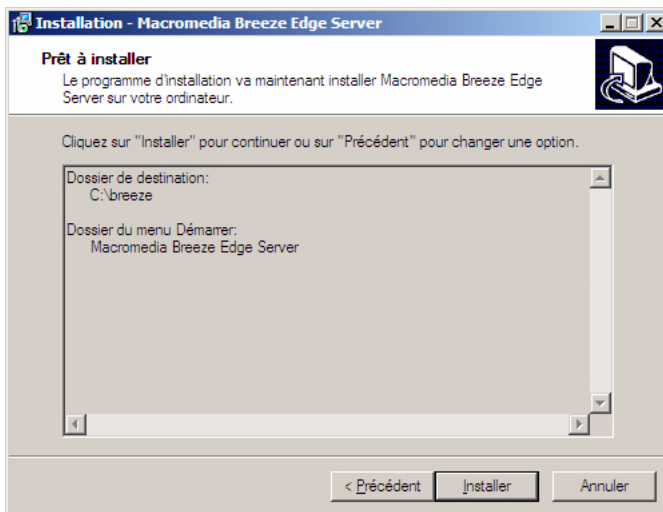
5. Cliquez sur Suivant pour continuer.

L'écran de sélection du dossier du menu Démarrer apparaît.



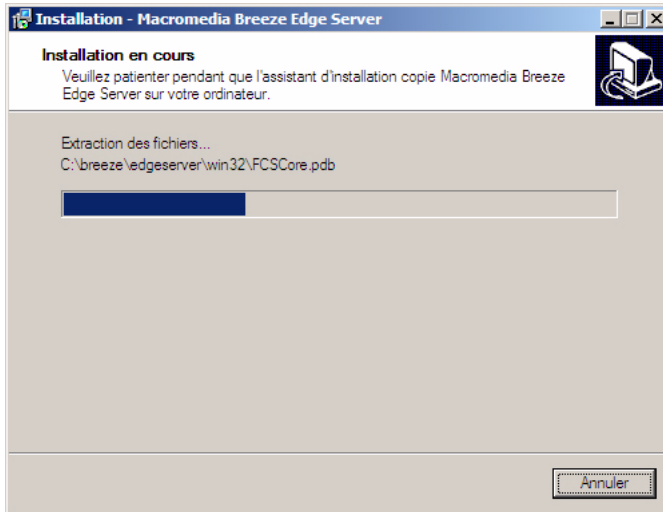
6. Acceptez le raccourci par défaut ou cliquez sur Parcourir pour sélectionner un emplacement différent, puis cliquez sur Suivant.

L'écran Prêt pour l'installation vous informe que l'installation de Breeze va démarrer.

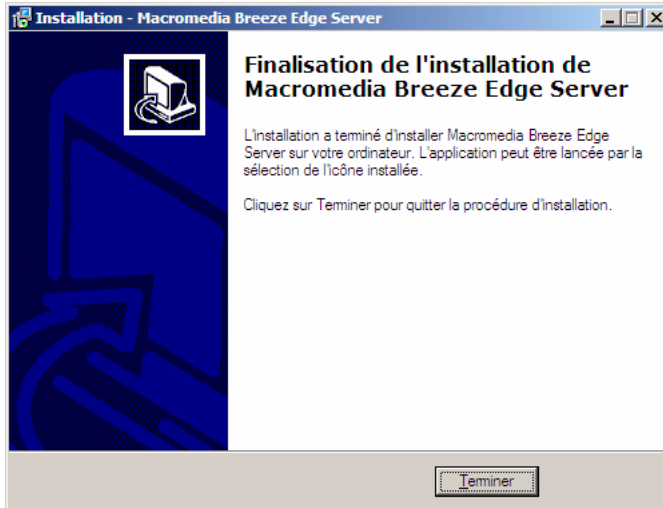


7. Vérifiez les choix effectués en ce qui concerne le dossier de destination pour l'installation de Breeze et le dossier du menu Démarrer pour Macromedia Breeze Edge Server.

8. Cliquez sur Précédent pour revoir ou modifier ces paramètres ou sur Installer pour continuer.
L'écran d'installation de Breeze s'ouvre. L'assistant commence à extraire les fichiers Breeze Edge Server du CD d'installation et à les installer. Cette opération dure moins de deux minutes.



9. Cliquez sur Annuler à n'importe quel moment pour abandonner ou annuler l'installation.
A l'issue de l'installation, un écran s'affiche, indiquant que l'installation de Macromedia Breeze Edge Server est terminée.



10. Cliquez sur Terminer pour quitter l'assistant d'installation de Macromedia Breeze Edge Server.

Fichier de licence de Breeze Edge Server

Lorsque vous commandez Breeze Edge Server, le service Macromedia chargé de la gestion des commandes vous envoie un courrier électronique avec, en pièce jointe, un fichier de licence Breeze Edge Server (license.lic).

Procédez comme suit pour installer le fichier de licence Breeze Edge Server :

1. Accédez au dossier `c:\breeze\edgeserver\conf\win32\licenses`.
2. Créez le dossier « licenses », si nécessaire.
3. Ouvrez le courrier électronique envoyé par Macromedia.
4. Enregistrez le fichier joint dans le dossier de licences.

Après avoir enregistré le fichier de licence à l'emplacement voulu, vous pouvez arrêter et redémarrer les services FCS et Breeze Edge Server afin de vous assurer que l'installation a réussi.

Pour plus d'informations, voir [Arrêt et démarrage de Breeze Edge Server, page 21](#).

Configuration de FCS pour Breeze Edge Server

Chaque entreprise configure son réseau différemment, en tenant compte de ses propres règles de fonctionnement et de son implantation géographique. Pour garantir la réussite du déploiement des serveurs Edge, il convient de s'assurer que les ordinateurs (clients Breeze) des utilisateurs reçoivent l'adresse IP d'un serveur Edge lors de la résolution de l'entrée DNS (Domain Name Server) pour la variable BREEZE_HOST (anciennement ADMIN_HOST).

Le scénario suivant décrit un déploiement à grande échelle de Breeze et se base sur l'illustration de la section [Présentation des serveurs Edge, page 6](#).

- Les clients sur site (utilisateurs basés à Lyon) peuvent directement accéder au serveur Breeze d'origine. Le mappage de l'entrée DNS pour l'hôte Breeze permet d'obtenir, pour ces clients, l'adresse IP du serveur Breeze d'origine.
- Les serveurs Edge rassemblent les demandes de services émanant des clients hors site (utilisateurs basés Paris et Toulouse) et les dirigent vers le serveur Breeze d'origine.
- Le mappage de l'entrée DNS pour l'hôte Breeze permet d'obtenir, pour ces clients distants, l'adresse IP du serveur Edge approprié.
- Les clients basés à Toulouse accèdent à Breeze par le biais du serveur Edge 1, ceux situés à Paris, par le biais du serveur Edge 2. Aucun des clients de ces zones ne peut communiquer directement avec le serveur Breeze d'origine.

L'accès à Breeze est défini en modifiant le serveur DNS le plus proche du client. Pour diriger les utilisateurs de Breeze vers le serveur Edge le plus proche, l'administrateur de Breeze crée une entrée DNS dans le fichier de configuration `custom.ini` de ce serveur. Dans le cas des serveurs Edge, c'est la variable `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT` qui contient l'entrée DNS.

Mappage de l'entrée DNS pour un serveur Breeze Edge

Le mappage de l'entrée DNS pour un serveur Edge est comparable au mappage de la variable BREEZE HOST pour le serveur Breeze sur la console de gestion des applications Breeze. Par exemple, si la valeur de BREEZE HOST (nom d'hôte à utiliser dans une URL pour accéder au serveur Breeze d'origine) correspond à *breeze.masociete.com*, l'entrée DNS d'un serveur Edge mappe *breeze.masociete.com* à l'adresse IP du serveur Edge le plus proche.

Remarque : Les valeurs définies dans le fichier custom.ini ont priorité sur celles contenues dans le fichier config.ini. La variable FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT apparaît également dans le fichier config.ini. Ne changez les valeurs d'aucune variable contenue dans le fichier config.ini.

Pour configurer Breeze Edge Server manuellement :

1. Ouvrez le répertoire d'installation racine. L'emplacement par défaut est c:\breeze\.
2. Supprimez le fichier custom.ini contenu dans ce répertoire, le cas échéant.
3. Ouvrez le dossier edgserver. L'emplacement par défaut est c:\breeze\edgserver\.
4. Si ce dossier ne contient pas un fichier custom.ini, créez un nouveau fichier texte et enregistrez-le sous le nom custom.ini.
5. Ouvrez le fichier custom.ini à l'aide d'un éditeur de texte tel que le Bloc-notes de Windows.
6. Ajoutez la ligne suivante au fichier custom.ini :

```
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=votreserveurbreeze:80
```

où *votreserveurbreeze:80* correspond à l'adresse IP ou au nom de domaine et au numéro de port de la machine sur laquelle le serveur Breeze est installé.

La valeur de cette variable permet de configurer le serveur Edge de sorte qu'il se connecte au serveur Breeze à cet emplacement.

Remarque : FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT est la seule entrée contenue dans le fichier custom.ini du serveur Edge.

7. Enregistrez le fichier custom.ini.
8. Arrêtez puis démarrez Breeze Edge Server.

Pour plus d'informations, voir [Arrêt et démarrage de Breeze Edge Server](#), page 21.

Configuration des ports Breeze Edge Server

Les serveurs Edge sont configurés pour écouter sur les ports 80 et 443, en plus du port par défaut, qui correspond à 1935. Vous configurez les ports en modifiant la variable `DEFAULT_FCS_HOSTPORT`. Si cette variable est introuvable dans le fichier de configuration `custom.ini`, vous devez ajouter la ligne suivante à ce fichier :

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

Cette ligne indique que les serveurs Edge écoutent sur les ports 1935, 80 et 443. Un port est défini en tant que port sécurisé lorsqu'un signe moins (-) précède son numéro dans une variable ou un fichier de configuration. Par exemple, vous pouvez configurer un port sécurisé en modifiant la balise `<HostPort>` du fichier `Adaptor.xml`.

```
<HostPort>:1935,80,-443</HostPort>
```

Le port 443 est défini comme port sécurisé qui reçoit uniquement les connexions RTMPS. Si vous soumettez une demande de connexion RTMPS via les ports 1935 ou 80, la connexion échoue. De même, une demande de connexion RTMP non sécurisée via le port 443 échoue.

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

Configuration de FCS pour SSL

Pour utiliser FCS dans le cadre de communications SSL (Secure Sockets Layer), un protocole sécurisé conçu pour la transmission de documents privés via Internet, vous devez configurer les fichiers `FCS Adaptor.xml` et `Server.xml` pour la prise en charge de SSL en mode natif en définissant les balises SSL adéquates.

Par exemple, si vous optez pour le paramétrage par défaut de la balise `<Redirect></Redirect>` disponible dans la section `HTTPTunneling` du fichier `Adaptor.xml`, FCS est configuré pour gérer uniquement le trafic avec les protocoles RTMP et RTMPS.

```
<Redirect enable="true">
  <Host port="80">:8080</Host>
  <Host port="443">:8443</Host>
</Redirect>
```

Par défaut, les fichiers FCS figurent à l'emplacement `c:\breeze\comserv`. Les fichiers de configuration de FCS se trouvent à l'emplacement `c:\breeze\comserv\win32\conf`.

Autres implémentations SSL

FCS prend également en charge les implémentations suivantes pour des transmissions sécurisées SSL :

- SSL par le biais d'un accélérateur matériel externe
- SSL par le biais d'une carte PCI interne

Remarque : L'implémentation basée sur l'utilisation d'une carte PCI n'a pas été testée au moment de la rédaction de ce document.

Tunnellisation HTTP

Pour que SSL fonctionne correctement, la tunnellation HTTP doit être activée. Elle permet aux clients de se connecter au serveur via SSL.

Remarque : La tunnellation HTTP est activée par défaut. Aucune intervention n'est requise de la part de l'utilisateur.

Ajout des balises SSL requises au fichier Adaptor.xml

Par défaut, toutes les balises SSL du fichier Server.xml sont incluses. Néanmoins, certaines des balises SSL requises dans le fichier Adaptor.xml sont manquantes.

Vous devez donc insérer les balises SSL suivantes dans le fichier Adaptor.xml.

```
<SSL>
  <SSLServerCtx>
    <SSLCertificateFile></SSLCertificateFile>
    <SSLCertificateKeyFile type="PEM"></SSLCertificateKeyFile>
    <SSLPassPhrase></SSLPassPhrase>
    <SSLCipherSuite></SSLCipherSuite>
    <SSLSessionTimeout>5</SSLSessionTimeout>
  </SSLServerCtx>
</SSL>
```

Placez cette section immédiatement après la balise de fin de la section HTTP Tunneling, qui correspond à </HTTP Tunneling>, mais avant la balise de fin </Adaptor> qui se trouve au niveau de la racine.

Repérage des balises SSL requises dans le fichier Server.xml

Les balises SSL contenues dans le fichier Server.xml se présentent dans l'ordre suivant :

- <SSLEngine>
- <SSLRandomSeed>
- <SSLSessionCacheGC>
- <SSLVerifyCertificate>
- <SSLCACertificatePath>
- <SSLCACertificateFile>
- <SSLVerifyDepth>
- <SSLCipherSuite>

Définition des balises SSL dans FCS

Le tableau suivant répertorie, par ordre alphabétique, toutes les balises SSL contenues dans les fichiers Adaptor.xml et Server.xml. Vous devez configurer ces balises pour activer SSL dans FCS.

Fichier FCS	Balise XML	Valeur par défaut	Description
Adaptor.xml	<Redirect>/Redirect	Aucune	Indique si des demandes inconnues sont renvoyées vers un serveur externe tel que Breeze. Lorsque FCS reçoit une demande inconnue, celle-ci est renvoyée vers l'hôte de renvoi spécifié. Pour que le renvoi fonctionne, la tunnellation HTTP doit être activée. Vous pouvez définir le port utilisé sur l'hôte de renvoi pour l'écoute du trafic renvoyé. Une demande de renvoi vers un hôte spécifique peut correspondre à : <Redirect enable=false> <Host port="80">:8080</Host> <Host port="443">:8443</Host> </Redirect>
Adaptor.xml	<SSLCertificateFile> </SSLCertificateFile>	Aucune	Indique l'emplacement du fichier de certificat à envoyer au client. Si aucun chemin absolu n'est défini, il est supposé que l'emplacement du certificat est relatif au répertoire Adaptor.
Adaptor.xml	<SSLCertificateKeyFile type = PEM> </SSLCertificateKeyFile>	PEM	Indique l'emplacement du fichier de clé privé pour le certificat. Si aucun chemin absolu n'est spécifié, il est supposé que l'emplacement du fichier de clé est relatif au répertoire Adaptor. Si le fichier de clé est crypté, la phrase de passe doit être spécifiée dans la balise SLPassPhrase. L'attribut type indique le type de codage utilisé pour le fichier de clé de certificat : PEM ou ASN1.
Adaptor.xml	<SSLCipherSuite> </SSLCipherSuite>		Indique les chiffres à utiliser. Il s'agit d'une liste de composants séparés par le signe : (deux-points). Un composant peut être un algorithme d'échange de clé, une méthode d'authentification, une méthode de cryptage, un type « digest » ou un alias pour des regroupements courants. Pour la liste des composants, consultez la documentation FCS. Le paramétrage par défaut de cette balise est : ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH Prenez contact avec l'assistance technique de Breeze avant de modifier le paramétrage par défaut.
Adaptor.xml	<SSLPassPhrase> </SSLPassPhrase>	Aucune	Indique la phrase de passe à utiliser pour décrypter le fichier de clé privé. Si le fichier de clé privé n'est pas crypté, laissez cette balise vide.

Fichier FCS	Balise XML	Valeur par défaut	Description
Adaptor.xml	<SSLSessionTimeout>/ SSLSessionTimeout	5	Indique la durée (en minutes) de validité d'une session.
Server.xml	<SSLCACertificateFile> </SSLCACertificateFile>		<p>Cette balise configure le serveur pour qu'il agisse en tant que client SSL (utilisée uniquement dans le cadre de connexions SSL sortantes).</p> <p>Cette balise indique le nom d'un fichier contenant un ou plusieurs certificats émis par une autorité de certification reconnue au format de cryptage PEM (Privacy Enhanced Mail).</p> <p>Une autorité de certification est un organisme tel que Verisign qui émet des certificats. En général, un certificat est signé par une autorité de certification, laquelle certifie ainsi l'identité du propriétaire du certificat. Avant d'accorder un certificat à une personne, l'autorité de certification effectue les recherches et les vérifications de base nécessaires pour confirmer son identité.</p> <p>Ce répertoire indique les certificats des autorités de certification qui sont considérées comme sûres. Dès lors qu'un certificat est signé par l'une de ces autorités, vous pouvez être certain de l'identité de la personne puisque vous faites confiance à l'autorité qui a émis ce certificat.</p> <p>Chacun des certificats contenus dans le répertoire doit être défini par un nom composé de la valeur de hachage de la personne et de l'extension « .O ».</p>

Fichier FCS	Balise XML	Valeur par défaut	Description
Server.xml	<SSLCACertificatePath> </SSLCACertificatePath>		<p>Cette balise indique le nom d'un répertoire contenant un ou plusieurs certificats.</p> <p>Windows uniquement : Etant donné que MS Windows installe les certificats dans le registre, aucun répertoire du système de fichiers ne contient la totalité des certificats émanant de certificats racine sûrs. Vous devez importer les certificats installés dans le Magasin de certificats Windows dans des certificats individuels placés dans un répertoire accessible par OpenSSL.</p> <p>Pour importer ces certificats, exécutez la commande <code>FCSMaster -console -initialize</code>. Les certificats sont importés du Magasin de certificats Windows dans le répertoire défini par cette balise de configuration.</p> <p>Si cette balise est vide, les certificats sont importés dans le répertoire <code>certs</code>, qui se trouve au même niveau que le répertoire <code>conf</code>.</p> <p>Lors de la vérification d'un certificat, FCS recherche des certificats racine sûrs dans le fichier défini par la balise <code><SSLCACertificateFile></code> ou dans le répertoire défini par la balise <code><SSLCACertificatePath></code>. Si la balise <code><SSLCACertificatePath></code> est vide, FCS recherche les certificats racine dans le répertoire par défaut <code>certs</code>.</p>
Server.xml	<SSLCipherSuite> </SSLCipherSuite>		<p>Indique les chiffres à utiliser. Il s'agit d'une liste de composants séparés par le signe : (deux-points). Un composant peut être un algorithme d'échange de clé, une méthode d'authentification, une méthode de cryptage, un type « digest » ou un alias pour des regroupements courants. Pour la liste des composants, voir la documentation FCS.</p> <p>Le paramétrage par défaut de cette balise est : <code>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</code></p> <p>Prenez contact avec l'assistance technique de Breeze avant de modifier le paramétrage par défaut.</p>

Fichier FCS	Balise XML	Valeur par défaut	Description
Server.xml	<SSLEngine> </SSLEngine>	Aucune	Indique l'accélérateur cryptographique à utiliser, le cas échéant. Les moteurs cryptographiques suivants sont autorisés : cswift, chil, atalla, nuron, ubsec, aep, surewave ou 4758cca. Chaque élément identifie un type d'accélérateur matériel cryptographique. Un accélérateur cryptographique est un composant matériel conçu pour libérer l'unité centrale de la charge que constituent les opérations cryptographiques, réduisant ainsi la demande en ressources et améliorant la souplesse du serveur.
Server.xml	<SSLCACertificatePath> </SSLCACertificatePath>	Aucune	Indique le nom d'un répertoire contenant les certificats émis par des autorités de certification. Chacun des fichiers de ce répertoire doit contenir un seul certificat et doit être défini par un nom composé de la valeur de hachage de la personne et de l'extension « .O ». Win32 uniquement : Si cette balise est vide, FCS tente de localiser les certificats émis par les autorités de certification dans le répertoire certs, qui se trouve au même niveau que le répertoire conf. Le Magasin de certificats Windows peut être importé dans ce répertoire en exécutant la commande FCSMaster -console -initialize à partir de la ligne de commande.
Server.xml	<SSLRandomSeed> </SSLRandomSeed>	16	Indique le nombre d'octets d'entropie à utiliser pour créer le germe pour le générateur de chiffres pseudo-aléatoires. L'entropie est une mesure du caractère aléatoire. Plus l'entropie est importante, plus les chiffres du générateur de chiffres pseudo-aléatoires sont aléatoires. La valeur par défaut est 16. Vous ne pouvez pas spécifier une valeur inférieure à 8 octets.
Server.xml	<SSLSessionCacheGC> </SSLSessionCacheGC>	5	Indique la fréquence (en minutes) avec laquelle les sessions expirées sont purgées du cache de session côté serveur.

Fichier FCS	Balise XML	Valeur par défaut	Description
Server.xml	<SSLVerifyCertificate> </SSLVerifyCertificate>	true	Configure le serveur pour qu'il agisse comme un client SSL (connexions SSL sortantes). Cette balise indique si le certificat renvoyé par le serveur auquel la connexion est établie doit être vérifié ou non. La vérification du certificat est activée par défaut. Pour désactiver la vérification du certificat, spécifiez false. Attention : la désactivation de la vérification du certificat peut présenter un risque pour la sécurité.
Server.xml	<SSLVerifyDepth> </SSLVerifyDepth>	9	Configure le serveur pour qu'il agisse comme un client SSL (connexions SSL sortantes). Cette balise indique la profondeur maximum acceptable dans la chaîne de certificat. Si un certificat racine auto-signé est introuvable dans les limites de cette profondeur, la vérification du certificat échoue.

Arrêt et démarrage de Breeze Edge Server

Pour vérifier que l'installation a abouti, il convient d'arrêter et de démarrer Breeze Edge Server et les services FCS qui permettent sa prise en charge.

Pour démarrer Breeze Edge Server :

- Choisissez Démarrer > Programmes > Macromedia Breeze Edge Server > Démarrer le serveur Breeze Edge.

Pour vérifier que le serveur Edge fonctionne :

- Accédez au panneau de configuration.
- Sélectionnez le volet de services.
- Localisez les services suivants : Flash Communication Administration Server et Flash Communication Server.

Leur état doit être défini par « started » (démarré).

Pour arrêter Breeze Edge Server :

- Choisissez Démarrer > Programmes > Macromedia Breeze Edge Server > Arrêter le serveur Breeze Edge.

Pour vérifier que le serveur Edge est arrêté :

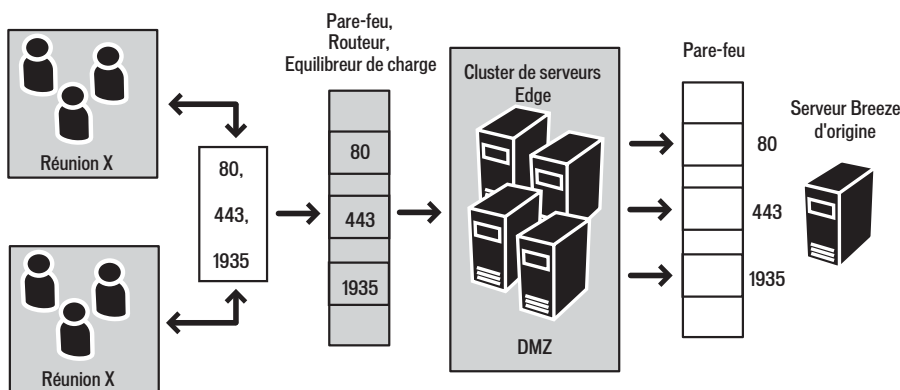
- Accédez au panneau de configuration.
- Sélectionnez le volet de services.
- Localisez les services suivants : Flash Communication Administration Server et Flash Communication Server.

Leur état doit être défini par « stopped » (arrêté).

Déploiement d'un cluster de serveurs Edge

Macromedia Breeze prend en charge la mise en cluster de serveurs Edge. Si votre licence le permet, vous pouvez préparer, installer et configurer un cluster de serveurs Edge sur plusieurs ordinateurs en réseau. Le déploiement de serveurs Edge sous la forme d'un cluster présente de nombreux avantages :

- Les serveurs Edge en cluster augmente la capacité d'accès des utilisateurs à Breeze et améliore les performances du serveur Breeze d'origine en ce qui concerne le traitement des demandes de services émanant des utilisateurs.
- Les serveurs Edge en cluster permettent aux utilisateurs de Breeze de continuer à accéder à Breeze sans interruption, y compris en cas d'échec d'un des serveurs du cluster, voire de la totalité du cluster.



La procédure de base pour l'installation et la configuration d'un cluster de serveurs Edge est décrite ci-après.

1. Assurez-vous que la configuration matérielle, logicielle et réseau de chaque ordinateur inclus dans le cluster répond aux exigences décrites à la section [Configuration requise, page 8](#).
2. Installez le fichier de licence de Breeze Edge Server sur chaque serveur Edge en procédant comme indiqué à la section [Fichier de licence de Breeze Edge Server, page 13](#).
3. Configurez FCS pour chaque serveur Edge du cluster en procédant comme indiqué à la section [Configuration de FCS pour Breeze Edge Server, page 13](#).
4. Si vous prévoyez d'utiliser le protocole SSL sécurisé, configurez FCS comme indiqué à la section [Configuration de FCS pour SSL, page 15](#).
5. Installez un équilibreur de charge sur le réseau et configurez-le pour écouter sur le port 80.
 - Voir la documentation du fournisseur pour obtenir des instructions sur la configuration de l'équilibreur de charge.

Planification de la maintenance

Macromedia recommande de créer une tâche planifiée hebdomadaire pour effacer la mémoire cache des serveurs Edge.

Pour créer cette tâche :

1. Créez un fichier cache.bat afin de supprimer le répertoire de cache. La syntaxe de l'entrée contenue dans ce fichier doit être :

```
del /Q /S <répertoire cache>\*.*
```

Le répertoire cache par défaut se trouve à l'emplacement

C:\breeze\edgeserver\win32\cache\http. La commande est :

```
del /Q /S c:\breeze\edgeserver\win32\cache\http\*.*
```

2. Exécutez le fichier cache.bat et vérifiez qu'il permet la suppression des fichiers présents dans le répertoire cache.
 - Notez que la structure de répertoires est conservée, ce qui est normal.
 - Les fichiers actuellement verrouillés par le serveur Edge ne sont pas supprimés, ce qui est également normal.
3. Sélectionnez Panneau de configuration > Tâches planifiées > Ajouter une tâche planifiée.
4. Sélectionnez le fichier cache.bat en tant que nouveau fichier à exécuter.
5. Macromedia recommande l'exécution de cette tâche planifiée une fois par semaine, en dehors de heures de bureau (le dimanche matin de bonne heure, par exemple).
6. Répétez cette procédure sur chaque serveur Edge installé.

