

WebSphere Application Server



Caching Proxy - Guide d'administration

Version 6.1

WebSphere Application Server



Caching Proxy - Guide d'administration

Version 6.1

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 295.

Première édition - mai 2006

Réf. US : GC31-6920-00

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- <http://www.fr.ibm.com> (serveur IBM en France)
- <http://www.can.ibm.com> (serveur IBM au Canada)
- <http://www.ibm.com> (serveur IBM aux Etats-Unis)

*Compagnie IBM France
Direction Qualité
Tour Descartes
92066 Paris-La Défense Cedex 50*

© Copyright IBM France 2006. Tous droits réservés.

© Copyright International Business Machines Corporation 2006. All rights reserved.

Table des matières

Figures	xi
--------------------------	-----------

A propos de ce guide	xiii
A qui s'adresse ce guide	xiii
Conventions et terminologie utilisées dans ce guide	xiii
Accessibilité	xiv
Comment envoyer vos commentaires	xiv
Informations connexes	xiv

Partie 1. Mise en route avec Caching Proxy	1
---	----------

Chapitre 1. Présentation	3
Configurations Caching Proxy de base.	3
Proxy inversé (par défaut).	3
Proxy d'acheminement	3
Prise en charge des nouvelles fonctionnalités	4

Chapitre 2. Utilisation des formulaires de configuration et d'administration	7
Ressources requises avec le navigateur.	7
Accès aux formulaires de configuration et d'administration	8
Configuration du mot de passe administrateur	9

Chapitre 3. Utilisation de l'assistant Configuration	11
---	-----------

Chapitre 4. Modification manuelle du fichier ibmproxy.conf	13
---	-----------

Chapitre 5. Démarrage et arrêt de Caching Proxy	15
Démarrage et arrêt automatiques sur les systèmes Linux et UNIX	15
Démarrage manuel sur les systèmes Linux et UNIX	16
Sur AIX :	16
Sous HP-UX :	16
Sous Linux :	17
Sous Solaris :	17
Démarrage en tant que service Windows	17
Démarrage en tant qu'application Windows	18
Utilisation du menu Démarrer	18
Utilisation de l'invite de commande	18
Lancement de plusieurs serveurs proxy	19
Arrêt manuel sur les systèmes Linux et UNIX	19
Limites des commandes d'arrêt.	20
Arrêt manuel sur un système Windows	21
Redémarrage après modifications de la configuration	21

Partie 2. Configuration et réglage du processus Caching Proxy.	23
---	-----------

Chapitre 6. Définition du serveur	25
Directives associées.	26
Formulaires de configuration et d'administration	26

Chapitre 7. Définition de l'appartenance des processus	27
Directives associées.	27
Formulaires de configuration et d'administration	28

Chapitre 8. Gestion de connexions	29
Directives associées.	30
Formulaires de configuration et d'administration	31

Chapitre 9. Configuration du processus du serveur proxy	33
Définition des directives liées aux performances	33
Examen d'autres applications	33
Vérification de l'espace de pagination	34
Configuration du système de fichiers	34
Réglage de la configuration TCP/IP	34
Réglage du délai d'attente TCP des environnements à forte charge (HP-UX, Linux, Solaris, Windows)	34
Ajustement du noyau Linux.	35
Variables d'ajustement des unités d'exécution AIX	36

Partie 3. Configuration du comportement de Caching Proxy	37
---	-----------

Chapitre 10. Gestion du traitement des demandes	39
Activation des méthodes HTTP/FTP	39
Directives associées.	40
Formulaires de configuration et d'administration	40
Méthodes Enable WebDAV, méthodes MS Exchange et méthodes définies par l'utilisateur	41
Directives associées.	42
Définition de règles de mappage	42
Règles de mappage.	42
Configuration d'un serveur de substitution.	44
Directives associées.	44
Formulaires de configuration et d'administration	44
Activation de la réécriture de jonction (facultatif).	45
Définition de la jonction sans l'option JunctionPrefix	45
Définition de la jonction avec l'option JunctionPrefix (méthode recommandée)	45
Directives associées.	46
Formulaires de configuration et d'administration	47

Utilisation de cookies à la place de JunctionRewrite	47
Exemple de plug-in transmogrier pour l'extension de la fonctionnalité JunctionRewrite	48

Chapitre 11. Gestion de la livraison de données locales. 49

Définition du répertoire principal des documents.	49
Directives associées.	49
Formulaires de configuration et d'administration	49
Définition de pages de bienvenue par défaut	50
Directives associées.	51
Formulaires de configuration et d'administration	51

Chapitre 12. Gestion de connexions FTP 53

Protection de fichiers FTP	53
Connexion au serveur via FTP	53
Gestion de chemins d'accès aux répertoires FTP	54
Gestion de chaînage FTP	55

Chapitre 13. Personnalisation du traitement sur le serveur 57

Inclusions côté serveur	57
Considérations sur les inclusions côté serveur	57
Configuration des inclusions côté serveur	57
Format à utiliser pour les inclusions côté serveur	58
Directives pour les inclusions côté serveur	58
Personnalisation des messages d'erreur	65
Réacheminement RTSP (Real Time Streaming Protocol)	65
A propos du réacheminement RTSP	65
Limites de la fonction RTSP	66
Amélioration de la fonction RTSP	66
Configuration du réacheminement RTSP.	66

Chapitre 14. Configuration des options d'en-tête 67

Directives associées.	67
Formulaires de configuration et d'administration	68

Chapitre 15. A propos de l'interface de programmation d'application 69

Directives associées.	69
Formulaires de configuration et d'administration	69

Partie 4. Configuration de fonction de mise en cache du serveur proxy. 71

Chapitre 16. Présentation de la mise en cache sur le serveur proxy 73

Stockage de la mémoire cache	73
Index de la mémoire cache	73
Mise en cache FTP	74
Mise en cache DNS.	74
Exclusions de la mémoire cache	75
Gestion de la mémoire cache	75

Chapitre 17. Configuration de la mise en mémoire cache de base 77

1. Activation de la mémoire cache	77
2. Configuration de l'espace de mémoire cache	77
Personnalisations optionnelles	79
Définition de la mémoire cache.	79
Sauvegarde ou chargement de la mémoire cache sur le disque	80
Définition de filtres de mise en mémoire cache	80
Configuration de la mise en mémoire cache pour les résultats de requête et les fichiers générés en dynamique	80
Configuration du délai d'expiration des fichiers en mémoire cache et de la récupération de place	80
Configuration du préchargement automatique.	80
Configuration du partage de la mémoire cache	80
Configuration de la journalisation	80

Chapitre 18. Contrôle du contenu de la mémoire cache 81

Configuration des filtres de mise en mémoire cache d'URL	81
Mise en cache de réponses de requêtes	82
Conditions supplémentaires pour la mise en mémoire cache des réponses de requêtes	82
Mise en cache de fichiers locaux	83
Stockage des fichiers en mémoire cache par URL partielle	83
Directives du fichier de configuration associées	83

Chapitre 19. Maintenance des données de la mémoire cache. 85

Expiration des fichiers.	85
Informations complémentaires sur la validité de la mémoire cache	86
Définition des dates avec FTP	87
Configuration de la validité de la mémoire cache	88
Récupération de place	90
Configuration de la récupération de place	90

Chapitre 20. Configuration de l'agent de la mémoire cache pour la régénération et le préchargement automatiques 91

Définition du nom d'hôte du serveur.	92
Préchargement de fichiers spécifiques dans la mémoire cache	93
Préchargement dans la mémoire cache des fichiers fréquemment consultés	93
Fonction de suivi logique des liens	94
Directives du fichier de configuration du proxy associées	97
Lancement manuel de l'agent de la mémoire cache	97

Chapitre 21. Utilisation d'une mémoire cache partagée 99

Remote cache access (RCA)	99
-------------------------------------	----

Configuration de la fonction RCA (Remote Cache Access)	100
Configuration du plug-in Internet Caching Protocol	100
Configuration du plug-in ICP	100

Chapitre 22. Stockage en mémoire cache d'un contenu généré dynamiquement 103

Configuration de IBM WebSphere Application Server pour la mise en mémoire cache du proxy	104
Configuration de la mise en mémoire cache dynamique sur le serveur d'applications	104
Configuration de l'adaptateur du serveur d'applications	104
Configuration des serveurs Caching Proxy pour la mise en mémoire cache dynamique	105
Configuration de la directive Service pour l'activation du plug-in de la mise en mémoire cache dynamique	105
Configuration de la directive ExternalCacheManager pour la spécification des sources des fichiers	106

Chapitre 23. Personnalisation de la mémoire cache du serveur proxy . . . 107

Choix du support de stockage de la mémoire cache	107
Optimisation des performances du cache disque	107
Récupération de place en mémoire cache	107
Optimisations pour chaque plateforme	108
AIX	108
HP-UX et Solaris	108
Windows	108

Partie 5. Configuration de la sécurité de Caching Proxy 109

Chapitre 24. A propos de la sécurité du serveur proxy 111

Chapitre 25. Configurations de protection du serveur 113

Utilisation des formulaires de configuration et d'administration pour définir les informations de protection	113
Utilisation des directives du fichier de configuration pour définir les informations de protection	114
Paramètres de protection par défaut	115

Chapitre 26. Secure Sockets Layer (SSL) 117

Etablissement d'une liaison SSL	117
Réglage des performances SSL	118
Etablissement de tunnels SSL	119
Configuration de l'établissement des tunnels SSL	120
Configuration de l'administration à distance sécurisée	121

Gestion des clés et des certificats	121
Autorités de certification	122
Utilitaire IBM Key Manager	123
Création d'un fichier de stockage, de mots de passe et d'une base de données de clés	125
Réception d'un certificat signé par une autorité de certification	129
Stockage d'un certificat signé par une autorité de certification	130
Spécifications de chiffrement autorisées	131

Chapitre 27. Support du matériel cryptographique 133

Chapitre 28. Utilisation du plug-in Tivoli Access Manager 135

Configuration	135
Etapes préalables à l'utilisation du script de configuration	135
Utilisation du script de configuration	135
Démarrage de Caching Proxy et du plug-in Access Manager	136

Chapitre 29. Utilisation de l'outil module d'autorisation PAC-LDAP . . . 137

Présentation	137
Authentification	137
Autorisation	137
LDAP (Lightweight Directory Access Protocol)	138
Installation	138
Restrictions et configuration supplémentaire requise pour les connexions du serveur sécurisé PACD-LDAP	139
Utilisation obligatoire de GSKit avec le client LDAP	139
Définition requise de la variable d'environnement LD_PRELOAD pour les systèmes Linux	139
Sur les systèmes Linux, le démarrage du processus PACD échoue lors de l'utilisation du client LDAP IBM Tivoli Directory Server (ITDS) 6.0	140
Sur les systèmes AIX, il est impossible de charger le module PAC-LDAP en utilisant le client LDAP ITDS (IBM Tivoli Directory Server)	140
Modification du fichier ibmproxy.conf pour activer le module d'autorisation PAC-LDAP	140
Modification des fichiers de configuration du module d'autorisation PAC-LDAP	142
paccp.conf	142
pac.conf	143
pacpolicy.conf	143
Création de pac_ldap.cred	144
Démarrage et arrêt de pacd	145

Partie 6. Contrôle de Caching Proxy 147

Chapitre 30. Configuration de la consignation. 149

A propos des journaux	149
Noms des fichiers journaux et options de base	149
Filtres des journaux des accès	150
Raisons justifiant le contrôle des données consignées	150
Configuration des filtres du journal des accès	151
Paramètres des journaux par défaut	152
Maintenance et archivage des journaux	153
Scénario de fichier journal	154

Chapitre 31. Utilisation du Moniteur de l'activité du serveur 157

Annexe A. Utilisation de commandes de Caching Proxy 161

cgiparse, commande	162
cgiutils, commande	165
htadm, commande	167
htcformat, commande	170
ibmproxy, commande	172

Annexe B. Directives du fichier de configuration 175

Directives non modifiées lors du redémarrage	175
Présentation des directives	175
Valeurs autorisées	176
Syntaxe des enregistrements du fichier de configuration	177
Directives Caching Proxy	177
AcceptAnything — Servir tous les fichiers	177
AccessLog — Nom du chemin d'accès du fichier journal des accès	177
AccessLogExcludeMethod — Supprime les entrées de fichier journal pour les fichiers et les répertoires demandés par une méthode donnée	178
AccessLogExcludeMimeType — Supprime les entrées de journal d'accès Proxy pour des types MIME spécifiques	179
AccessLogExcludeReturnCode — Supprime les entrées de fichier journal pour des codes retour spécifiques	179
AccessLogExcludeURL — Supprime les entrées de journal pour des répertoires ou des fichiers spécifiques	180
AccessLogExcludeUserAgent — Supprime les entrées de journal pour des navigateurs spécifiques	180
AddBlankIcon — Spécifie l'URL de l'icône utilisée pour aligner les en-têtes des listes de répertoires	181
AddDirIcon — Spécifie l'icône d'URL des répertoires au niveau des listes de répertoire	181
AddEncoding — Spécifie le codage du contenu MIME des fichiers avec des suffixes particuliers	182
AddIcon — Associe une icône à un type de contenu ou de codage MIME	182

AddParentIcon — Spécifie l'URL de l'icône pour un répertoire parent au niveau de la liste de répertoire	183
AddType — Spécifie le type de données des fichiers ayant une extension particulière	183
AddUnknownIcon — Spécifie l'URL d'icône pour les types de fichier inconnus au niveau des listes de répertoire	185
AdminPort — Spécifie le port pour les demandes de pages ou de formulaires d'administration	185
AggressiveCaching — Spécifie la mise en mémoire en cache des fichiers ne pouvant pas être mis en mémoire cache	186
AlwaysWelcome — Indique de rechercher les fichiers de bienvenue dans le répertoire demandé	186
appendCRLFtoPost — Ajoute CRLF aux demandes POST	187
ArrayName — Attribue un nom au tableau de la mémoire cache à distance	187
Authentication — Personnalise l'étape d'authentification	187
Authorization — Personnalise l'étape d'autorisation	188
AutoCacheRefresh — Spécifie si la régénération de la mémoire cache doit être utilisée	188
BindSpecific — Spécifie si le serveur est lié à une ou à plusieurs adresses IP.	189
BlockSize — Définit la taille des blocs sur l'unité de mémoire cache	189
CacheAccessLog — Spécifie le chemin des fichiers journaux des accès à la mémoire cache	189
CacheAlgorithm — Identifie l'algorithme de mémoire cache	190
CacheByIncomingUrl — Spécifie la base pour la génération des noms de fichier de mémoire cache	190
CacheClean — Indique la durée de conservation des fichiers en mémoire cache	191
CacheDefaultExpiry — Indique l'heure d'expiration par défaut des fichiers	191
CacheDev — Spécifie l'unité de stockage de la mémoire cache	192
CacheExpiryCheck — Indique si le serveur renvoie les fichiers expirés	192
CacheFileSizeLimit — Spécifie la taille maximale des fichiers à placer en mémoire cache	193
CacheLastModifiedFactor — Spécifie la valeur permettant de déterminer les dates d'expiration	193
CacheLocalDomain — Indique s'il est nécessaire de mettre le domaine local en mémoire cache	194
CacheMatchLanguage — Définition de la préférence de langue pour le contenu du cache renvoyé	194
CacheMaxExpiry — Spécifie la durée de vie maximale des fichiers en mémoire cache	195
CacheMemory — Spécifie la mémoire vive de la mémoire cache	196
CacheMinHold — Indique la durée de disponibilité des fichiers	196

CacheNoConnect — Spécifie le mode de mémoire cache autonome	197
CacheOnly — Met en mémoire cache uniquement les fichiers dont les URL correspondent à un modèle.	197
CacheQueries — Met en mémoire cache les réponses aux URL contenant le caractère ?	197
CacheRefreshInterval — Indique l'intervalle de temps pour la revalidation des objets placés en mémoire cache	198
CacheRefreshTime — Indique à quel moment démarrer l'agent de la mémoire cache	198
CacheTimeMargin — Indique la durée minimale de mise en mémoire cache d'un fichier	199
CacheUnused — Indique la durée de conservation des fichiers en mémoire cache et non utilisés	199
Caching — Active la mémoire cache du serveur proxy	200
CompressAge — Indique à quel moment compresser les fichiers journaux	200
CompressCommand — Spécifie la commande et les paramètres de compression	200
CompressDeleteAge — Indique à quel moment supprimer les journaux	201
CompressionFilterAddContentType — Indique le type de contenu de la réponse HTTP à compresser	202
CompressionFilterEnable — Active le filtre de compression pour qu'il compresse les réponses HTTP	203
ConfigFile — Spécifie le nom d'un fichier de configuration supplémentaire	203
ConnThreads — Définition du nombre d'unités d'exécution de connexions à utiliser pour la gestion des connexions	203
ContinueCaching — Indique quelle proportion du fichier est requise pour la mise en mémoire cache	204
DefinePicsRule — Fournit une règle de filtrage de contenu	204
DefProt — Spécifie la configuration de protection par défaut pour les demandes correspondant à un modèle.	204
DelayPeriod — Définit une pause entre les demandes	207
DelveAcrossHosts — Active la mise en mémoire cache dans les domaines.	207
DelveDepth — Indique jusqu'à quel niveau suivre les liens lors de la mise en mémoire cache	207
DelveInto — Indique si l'agent de la mémoire cache doit suivre les liens	207
DirBackgroundImage — Définit une image d'arrière-plan pour les listes de répertoire	208
DirShowBytes — Affiche le nombre d'octets des petits fichiers dans les listes de répertoires	208
DirShowCase — Différencie les majuscules et les minuscules lors du tri des fichiers des listes de répertoire.	209

DirShowDate — Affiche la date de dernière modification dans la liste de répertoire	209
DirShowDescription — Affiche la description des fichiers de la liste des répertoires	209
DirShowHidden — Affiche les fichiers cachés dans les listes de répertoire.	209
DirShowIcons — Affiche les icônes dans les listes de répertoire.	210
DirShowMaxDescrLength — Indique la longueur maximum des descriptions dans les listes de répertoire.	210
DirShowMaxLength — Définit la longueur maximale des noms de fichiers dans les listes de répertoire.	210
DirShowMinLength — Définit la longueur minimale des noms de fichiers dans les listes de répertoire.	210
DirShowSize — Affiche la taille des fichiers dans la liste de répertoire	211
Disable — Désactive les méthodes HTTP	211
DisInheritEnv — Spécifie les variables d'environnement ne devant pas être héritées par les programmes CGI	211
DNS-Lookup — Indique si le serveur recherche les noms d'hôte client	212
Enable — Active les méthodes HTTP	212
EnableTcpNodelay — Activation de l'option de socket TCP NODELAY	213
Error — Personnalise l'étape d'erreur	213
ErrorLog — Spécifie le fichier dans lequel sont consignées les erreurs du serveur.	213
ErrorMessage — Spécifie un message personnalisé pour une condition d'erreur particulière	214
Values — Valeurs par défaut.	215
EventLog — Spécifie le chemin du fichier journal des événements	216
Exec — Exécute un programme CGI pour les demandes ayant abouti	216
ExportCacheImageTo — Exportation de la mémoire cache sur le disque	218
ExternalCacheManager — Configure Caching Proxy pour la mise en mémoire cache dynamique à partir de IBM WebSphere Application Server	218
Fail — Rejette les demandes ayant abouti	219
FIPSEnable — Codes de chiffrement conformes à la norme FIPS (Enable Federal Information Processing Standard) pour SSLV3 et TLS	220
flexibleSocks — Active l'implémentation SOCKS flexible	220
FTPDirInfo — Génère un message de bienvenue ou de description pour un répertoire	220
ftp_proxy — Spécifie un autre serveur proxy pour les demandes FTP	221
FTPUrlPath — Indique comment interpréter les URL FTP	221
Gc — Spécifie la récupération de place en mémoire cache	221
GCAvvisor — Personnalise le processus de récupération de place.	222

GcHighWater — Indique le moment du lancement de la récupération de place	222
GcLowWater — Spécifie le moment d'arrêt de la récupération de place.	222
gopher_proxy — Spécifie un autre serveur proxy pour les demandes Gopher	223
GroupId — Spécifie l'ID de groupe	223
HeaderServerName — Indique le nom du serveur proxy retourné dans l'entête HTTP	224
Hostname — Spécifie le nom de domaine complet ou l'adresse IP du serveur	224
http_proxy — Spécifie un autre serveur proxy pour les demandes HTTP	224
HTTPSCheckRoot — Filtre les demandes HTTPS	225
ICP_Address — Spécifie l'adresse IP des requêtes ICP.	225
ICP_MaxThreads — Spécifie le nombre maximal d'unités d'exécution pour requêtes ICP.	225
Occupier — Spécifie un membre de cluster ICP	225
ICP_Port — Spécifie le numéro de port des requêtes ICP.	226
ICP_Timeout — Spécifie le délai d'attente maximal des requêtes ICP	226
IgnoreURL — Spécifie les URL qui ne sont pas régénérées	226
imbeds — Indique si le traitement côté serveur est utilisé.	227
ImportCacheImageFrom — Importation de la mémoire cache à partir d'un fichier	228
InheritEnv — Spécifie les variables d'environnement héritées par les programmes CGI	228
InputTimeout — Spécifie le délai d'entrée	229
JunctionReplaceUrlPrefix — Remplacement d'une URL au lieu d'insérer un préfixe lors de l'utilisation du plug-in JunctionRewrite.	229
JunctionRewrite — Active réécriture de l'URL	230
JunctionRewriteSetCookiePath — Réécriture de l'option dans l'en-tête Set-Cookie lors d'une utilisation avec le plug-in JunctionRewrite.	230
JunctionSkipUrlPrefix — Ignorer la réécriture d'URL contenant déjà le préfixe lors d'une utilisation avec le plug-in JunctionRewrite.	230
KeepExpired — Indique que la copie périmée de la ressource doit être renvoyée si cette dernière est mise à jour sur le proxy.	231
KeyRing — Spécifie le chemin du fichier de la base de données des fichiers de clés.	231
KeyRingStash — Spécifie le chemin du fichier des mots de passe de la base de données de clés	232
LimitRequestBody — Définition de la taille maximale du corps dans les demandes PUT ou POST	232
LimitRequestFields — Définition du nombre maximal d'en-têtes dans les demandes client	232
LimitRequestFieldSize — Définition de la longueur maximale d'un en-tête et d'une ligne de demande.	232
ListenBacklog — Spécifie le nombre de connexions client en file d'attente devant être gérées par le serveur	233

LoadInlineImages — Contrôle la régénération des images intégrées	233
LoadTopCached — Indique le nombre de pages préférées à régénérer	233
LoadURL — Spécifie les URL à régénérer	234
Log — Personnalise l'étape de personnalisation	234
LogArchive — Définit le comportement de la fonction d'archivage du journal	234
LogFileFormat — Spécifie le format du fichier journal des accès	235
LogToGUI (Windows uniquement) — Affiche les entrées de journal dans la fenêtre du serveur.	236
LogToSyslog — Envoi des informations d'accès au journal système (Linux et UNIX uniquement)	236
Map — Change les demandes ayant abouti en une nouvelle chaîne de demandes, à l'aide de la chaîne du chemin de demande pour correspondance avec la règle	237
MapQuery — Change les demandes ayant abouti en une nouvelle chaîne de demandes, à l'aide de la chaîne de demandes et du chemin de demande pour correspondance avec la règle	238
MaxActiveThreads — Spécifie le nombre maximal d'unités d'exécution actives	239
MaxContentLengthBuffer — Définit la taille de la mémoire tampon pour les données dynamiques	240
MaxLogFileSize — Spécifie la taille maximale de chaque fichier journal	240
MaxPersistRequest — Spécifie le nombre maximal de demandes à recevoir au niveau d'une connexion permanente	241
MaxQueueDepth — Indique le nombre maximal d'URL à placer en file d'attente	241
MaxRuntime — Identifie la durée maximale de l'exécution d'un agent de la mémoire cache	241
MaxSocketPerServer — Spécifie le nombre maximal de sockets inactives ouvertes pour le serveur	242
MaxUrls — Indique le nombre maximal d'URL à régénérer	242
Member — Spécifie un membre d'un tableau	242
Midnight — Identifie le plug-in API permettant d'archiver les fichiers journaux	243
NameTrans — Personnalise l'étape de conversion de nom	244
NoBG — Exécute le processus Caching Proxy en avant-plan	244
NoCaching — Ne met pas en mémoire cache les fichiers dont l'URL correspond à un modèle	245
NoLog — Supprime les entrées de journal pour des hôtes spécifiques ou des domaines correspondant à un modèle.	245
no_proxy — Spécifie les modèles pour la connexion directe aux domaines	246
NoCacheOnRange — Indique la non mise en cache pour les demandes Range	246
NoProxyHeader — Indique les en-têtes de client à bloquer.	247
NumClients — Indique le nombre d'unités d'exécution d'agent de la mémoire cache	247

ObjectType — Personnalise l'étape de type d'objet.	248
OptimizeRuleMapping — Optimise le processus de mappage de règle pour les demandes entrantes lors de l'augmentation du nombre de règles	248
OutputTimeout — Spécifie le délai de sortie	249
PacFilePath — Spécifie le répertoire contenant les fichiers PAC	249
Pass — Spécifie le modèle pour l'acceptation des requêtes.	249
PersistTimeout — Spécifie la durée d'attente avant que le client n'envoie une autre demande.	251
PICSDBLookup — Personnalise l'étape d'extraction de libellés PICS	251
PidFile (Linux et UNIX uniquement) — Définition du fichier utilisé pour stocker l'ID processus de Caching Proxy	252
PKCS11DefaultCert, PKCS11DriverPath, PKCS11TokenPassword — Prend en charge la carte IBM 4960 PCI Cryptographic Accelerator Card (AIX uniquement)	252
Directives de plug-in	253
Port — Spécifie le port sur lequel le serveur attend les demandes	254
PostAuth — Personnalise l'étape PostAuth	254
PostExit — Personnalise l'étape PostExit	255
PreExit — Personnalise l'étape PreExit	255
Protect — Active une configuration de protection pour les demandes correspondant à un modèle	255
Protection — Définit une configuration de protection nommée dans le fichier de configuration	260
Sous-directives de protection — Spécifie le mode de protection d'un ensemble de ressources	261
Proxy — Identifie les protocoles de proxy ou le proxy inversé	263
ProxyAccessLog — Indique le nom du chemin du fichier journal des accès au serveur proxy.	264
ProxyAdvisor — Personnalise le service des demandes de proxy	265
ProxyForwardLabels — Spécifie un filtrage PICS	265
ProxyFrom — Spécifie un client avec un en-tête "From:"	266
ProxyIgnoreNoCache — Ignore les demandes de rechargement	266
ProxyPersistence — Autorise les connexions permanentes.	266
ProxySendClientAddress — Génère l'en-tête "Client IP Address:"	267
ProxyUserAgent — Modifie la chaîne de l'agent utilisateur	267
ProxyVia — Spécifie le format de l'en-tête HTTP	267
ProxyWAS — Spécifie que les demandes sont envoyées à WebSphere Application Server.	268
PureProxy — Désactive un proxy dédié	268
PurgeAge — Spécifie la limite d'âge pour un journal	268

PurgeSize — Spécifie la taille limite d'un fichier journal d'archivage	269
RCAConfigFile — Spécifie un alias pour ConfigFile	270
RCAThreads — Spécifie le nombre d'unités d'exécution par port	270
ReadTimeout — Spécifie la durée limite pour une connexion	270
Redirect — Spécifie un modèle pour les demandes adressées à un autre serveur.	270
RegisterCacheIdTransformer — Met en cache plusieurs variantes d'une ressource sur la base de l'en-tête Cookie	272
ReversePass — Intercepte automatiquement les demandes redirigées	272
RewriteSetCookieDomain — Définition du modèle de domaine à remplacer	273
RTSPEnable — Active le réacheminement RTSP	273
rtsp_proxy_server - Spécifie les serveurs de réacheminement	274
rtsp_proxy_threshold — Spécifie le nombre de demandes avant réacheminement vers une mémoire cache	274
rtsp_url_list_size — Spécifie le nombre d'URL en mémoire de proxy.	274
RuleCaseSense — Mappe les demandes à partir d'URL d'applications ne faisant pas la distinction entre les minuscules et les majuscules	275
ScriptTimeout — Spécifie le paramètre de délai pour les scripts.	275
SendHTTP10Outbound — Spécifie la version du protocole pour les demandes traitées par un proxy	275
SendRevProxyName — Spécifie le nom d'hôte de Caching Proxy dans l'en-tête HOST	276
ServerConnGCRun — Spécifie l'intervalle d'exécution de l'unité d'exécution du processus de récupération de place	276
ServerConnPool — Spécifie la mise en pool des connexions avec les serveurs d'origine	277
ServerConnTimeout — Spécifie la période d'inactivité maximale.	277
ServerInit — Personnalise l'étape d'initialisation du serveur	277
ServerRoot — Spécifie le répertoire dans lequel est installé le programme du serveur	278
ServerTerm — Personnalise l'étape d'arrêt du serveur	278
Service — Personnalise l'étape Service	279
SignificantURLTerminator — Spécifie un code d'arrêt pour les demandes d'URL	280
SMTPServer (Windows uniquement)— Configure un serveur SMTP pour la routine sendmail	280
SNMP — Active et désactive la prise en charge de SNMP.	280
SNMPCommunity — Fournit un mot de passe de sécurité pour SNMP	281
SSLCaching — Active la mise en mémoire cache pour une demande sécurisée	281

SSLCertificate — Spécifie les libellés des clés pour les certificats	281	Transmogrier — Personnalise l'étape de manipulation des données	287
SSLCryptoCard — Spécifie la carte de chiffrement installée	282	TransmogriedWarning — Envoie un message d'avertissement au client	288
SSLEnable — Indique que les demandes sécurisées sont acheminées au port 443.	283	TransparentProxy — Active le proxy transparent sous Linux	288
SSLForwardPort — Spécifie le port auquel s'adresser dans le cas de mises à niveau SSL HTTP	283	UpdateProxy — Indique la destination de la mémoire cache	289
SSLOnly — Désactive les unités d'exécution à l'écoute pour les demandes HTTP	283	UserId — Spécifie l'ID utilisateur par défaut	289
SSLPort — Permet d'indiquer un port d'écoute HTTPS autre que celui par défaut	284	V2CipherSpecs — Indique les spécifications de chiffrement prises en charge par SSL version 2	290
SSLTunneling — Active l'établissement de tunnels SSL	284	V3CipherSpecs — Indique les spécifications de chiffrement prises en charge par SSL version 3	290
SSLVersion — Spécifie la version de SSL	284	WebMasterEMail — Définit une adresse électronique pour la réception des rapports d'un serveur sélectionné	291
SSLV2Timeout — Indique le délai d'inactivité au-delà duquel une session SSLV2 expire	285	WebMasterSocksServer (Windows uniquement)— Configure un serveur socks pour la routine sendmail	292
SSLV3Timeout — Indique le délai d'inactivité au-delà duquel une session SSLV3 expire	285	Welcome — Spécifie le nom des fichiers de bienvenue	292
SuffixCaseSense — Indique si les majuscules et les minuscules sont différenciées dans les définitions d'extension	285		
SupportVaryHeader — Met en cache plusieurs variantes d'une ressource sur la base de l'en-tête HTTP Vary	286		
TL SV1Enable — Active le protocole Transport Layer Secure (TLS)	287		

Remarques	295
Marques	297

Figures

- | | | | | | |
|----|--|----|----|--|-----|
| 1. | Fonction de suivi logique des liens. | 95 | 2. | Etablissement de tunnels SSL | 119 |
|----|--|----|----|--|-----|

A propos de ce guide

Cette préface explique à qui est destiné ce guide et décrit son objectif, son organisation, ses fonctions d'accessibilité, les conventions et la terminologie ainsi que les documents connexes.

A qui s'adresse ce guide

Le présent guide s'adresse aux administrateurs réseau et système qui connaissent bien leurs systèmes d'exploitation et la fourniture de services Internet. Une première expérience de Caching Proxy n'est pas nécessaire.

Le présent guide n'est pas destiné à prendre en charge les précédentes versions de Caching Proxy.

Conventions et terminologie utilisées dans ce guide

Ce document utilise les conventions et règles typographiques décrites ci-après.

Tableau 1. Conventions utilisées dans ce guide

Convention	Signification
Gras	Les intitulés des menus, options de menu, libellés, boutons, icônes et dossiers des interfaces graphiques utilisateur apparaissent également en caractères gras. Les caractères gras permettent également de mettre en évidence les noms de commandes afin de les distinguer du texte qui les entoure.
Espacement fixe	Texte à entrer à une invite de commande, mais également texte affiché à l'écran, exemples de code et extraits de fichiers.
<i>Italique</i>	Variables à entrer (par exemple, le nom d'un fichier dans la zone <i>nom de fichier</i>). Les italiques sont également utilisés pour mettre en évidence les titres des manuels.
Ctrl- <i>x</i>	Où <i>x</i> est le nom d'une touche, indique une séquence de caractères de commande. Par exemple, Ctrl-c signifie maintenir la touche Ctrl enfoncée tout en appuyant sur la touche c.
Retour	Fait référence à la touche libellée Retour ou Entrée, ou à la flèche vers la gauche.
%	Représente l'invite de commandes du shell Linux et UNIX pour une commande qui ne requiert pas les droits d'accès root.
#	Représente l'invite de commandes du shell Linux et UNIX pour une commande qui requiert les droits d'accès root.
C:\	Représente l'invite Windows.
Entrée de commandes	Lorsque vous êtes invité à "entrer" ou à "émettre" une commande, tapez la commande et appuyez sur la touche Retour. Par exemple, l'instruction "Entrez la commande ls " signifie tapez ls à l'invite et appuyez sur Retour.
[]	Encadre les éléments facultatifs des descriptions de syntaxe.
{ }	Encadre les listes dans lesquelles vous devez choisir un élément dans les descriptions de syntaxe.
	Sépare les éléments d'une liste de choix encadrés par { } (accolades) dans les descriptions de syntaxe.
...	Dans les descriptions de syntaxe, indique que l'élément qui précède peut être répété une ou plusieurs fois. Dans les exemples, indique que des informations ont volontairement été omises par souci de concision.

Accessibilité

Les fonctions d'accessibilité permettent à un utilisateur ayant un handicap physique, telle qu'une mobilité restreinte ou une vision limitée, d'utiliser les produits logiciels. Les principales fonctions d'accessibilité de la structure WebSphere Application Server, Version 6.1 sont les suivantes :

- Logiciel de lecteur d'écran et synthétiseur vocal permettant d'entendre ce qui s'affiche à l'écran. Avec un logiciel de reconnaissance vocale tel que IBM ViaVoice, vous pouvez également entrer des données et naviguer dans l'interface navigateur.
- Contrôle des fonctions à partir du clavier au lieu de la souris.
- Configuration et administration des fonctions Application Server à l'aide des éditeurs de texte ou des interfaces de ligne de commande standard au lieu des interfaces graphiques fournies. Pour plus d'informations sur l'accessibilité de certaines fonctions, reportez-vous à leur documentation.

Comment envoyer vos commentaires

Vos remarques et suggestions nous permettent d'améliorer la fiabilité et la qualité des informations. Adressez vos commentaires sur cet ouvrage ou sur les composants Edge de WebSphere Application Server :

- Par courrier électronique, à l'adresse fsdoc@us.ibm.com. N'oubliez pas d'indiquer le nom et le numéro du manuel, la version de WebSphere Application Server, et, le cas échéant, l'emplacement exact du texte commenté (numéro de page ou de tableau, par exemple).

Informations connexes

- *Concepts, planification et installation pour Edge Components*, GC11-2539-00
- *Programming Guide for Edge Components*, GC31-6919-00
- *Load Balancer - Guide d'administration*, GC11-2541-00
- *IBM WebSphere Edge Services Architecture*
- Page d'accueil du site Web IBM : www.ibm.com/
- Site Web de IBM WebSphere Application Server : www.ibm.com/software/webservers/appserv/
- Site Web de la bibliothèque IBM WebSphere Application Server : www.ibm.com/software/webservers/appserv/library.html
- Site Web d'assistance IBM WebSphere Application Server : www.ibm.com/software/webservers/appserv/support.html
- Centre de documentation d'IBM WebSphere Application Server : www.ibm.com/software/webservers/appserv/infocenter.html
- Centre de documentation d'IBM WebSphere Application Server Edge Components : www.ibm.com/software/webservers/appserv/ecinfocenter.html

Partie 1. Mise en route avec Caching Proxy

Cette partie propose une présentation du composant Caching Proxy, des instructions d'utilisation des formulaires de configuration et d'administration et de l'assistant de configuration, des instructions de modification manuelle du fichier `ibmproxy.conf`, ainsi que des procédures de démarrage et d'arrêt du serveur proxy.

Cette partie comporte les chapitres suivants :

Chapitre 1, «Présentation», à la page 3

Chapitre 2, «Utilisation des formulaires de configuration et d'administration», à la page 7

Chapitre 3, «Utilisation de l'assistant Configuration», à la page 11

Chapitre 4, «Modification manuelle du fichier `ibmproxy.conf`», à la page 13

Chapitre 5, «Démarrage et arrêt de Caching Proxy», à la page 15

Chapitre 1. Présentation

Agissant comme un proxy inversé, ou comme un proxy d'acheminement, Caching Proxy intercepte les demandes de données émanant d'un client, extrait les informations demandées sur les hôtes de données et les fournit au client. Le plus souvent, les demandes concernent des documents stockés sur des serveurs Web (également appelés serveurs d'origine ou hôtes de données) et fournis à l'aide du protocole HTTP (Hypertext Transfer Protocol). Vous pouvez toutefois configurer Caching Proxy de sorte qu'il accepte d'autres protocoles, tels que FTP (File Transfer Protocol) et Gopher.

Le composant Caching Proxy stocke les données dans une mémoire cache locale avant de les fournir au demandeur. Les données pouvant être mises en mémoire cache incluent des pages Web statiques et des FICHIERS JSP comportant des fragments générés dynamiquement, mais lentement. La mise en mémoire cache permet au Caching Proxy de satisfaire les demandes ultérieures afférentes aux mêmes données, directement depuis la mémoire cache locale, ce qui nécessite bien moins de temps qu'une nouvelle extraction depuis l'hôte de données.

IMPORTANT: Caching Proxy est disponible avec toutes les installations d'Edge Components, sauf dans les cas suivants :

- Caching Proxy n'est pas disponible pour celles fonctionnant sur processeurs Itanium 2 ou Opteron AMD 64 bits.
- Caching Proxy n'est pas disponible pour les installations de Load Balancer pour IPv4 et IPv6.

Configurations Caching Proxy de base

Les deux configurations de proxy de base sont le serveur proxy inversé et le serveur proxy d'acheminement.

Proxy inversé (par défaut)

Par défaut, Caching Proxy est configuré comme un serveur proxy inversé. Dans une configuration à proxy inversé, un serveur proxy est situé entre un ou plusieurs serveurs de contenu et Internet. Il accepte les demandes émanant de clients Internet à propos des contenus stockés sur le site d'accueil du serveur proxy. Ce dernier se présente au client comme le serveur d'origine (de contenu) ; le client ne se rend pas compte que la demande a été envoyée à un autre serveur.

Proxy d'acheminement

Vous pouvez également configurer Caching Proxy comme un serveur proxy d'acheminement. Toutefois, les navigateurs client doivent être configurés individuellement pour utiliser le proxy. Dans une configuration à proxy d'acheminement, un serveur proxy est situé entre le client et Internet. Caching Proxy achemine la demande d'un client à des hôtes de données via Internet, met en mémoire cache les données extraites et les fournit au client.

Pour activer la configuration de serveur proxy d'acheminement, apportez les modifications suivantes au fichier de configuration `ibmproxy.conf` :

- Supprimez la mise en commentaire des lignes suivantes pour spécifier les protocoles que va acheminer Caching Proxy.

```
Proxy http:*  
Proxy ftp:*  
Proxy gopher:*
```

- Activez les tunnels SSL pour permettre la gestion des requêtes SSL dans une configuration de proxy d'acheminement.

```
SSLTunneling On
```

Pour plus d'informations sur les tunnels SSL, voir «Configuration de l'établissement des tunnels SSL», à la page 120.

- Activez la méthode CONNECT avec la directive Enable :

```
Enable CONNECT OutgoingPorts All
```

ou

```
Enable CONNECT OutgoingPorts 443
```

Pour des informations sur le format et les options disponibles pour la méthode Enable CONNECT, voir «Configuration de l'établissement des tunnels SSL», à la page 120.

Ces modifications permettent au proxy d'acheminement les actions suivantes :

- Répondre aux demandes des clients d'un protocole HTTP ou FTP.
- Répondre aux demandes du moteur de recherche gopher.
- Gérer l'affinité entre un client et son serveur actuel pendant la durée d'une transaction.

Proxy transparent (systèmes Linux uniquement)

Une variante de Caching Proxy d'acheminement est Caching Proxy transparent. Dans ce rôle, Caching Proxy exécute la même fonction qu'un proxy de mise en cache d'acheminement de base, mais sans que le client soit conscient de sa présence. La configuration de Caching Proxy transparent est prise en charge uniquement sur les systèmes Linux.

Comme dans le cas d'un proxy d'acheminement traditionnel, le proxy transparent est installé sur une machine se trouvant à proximité d'Internet/de la passerelle, mais les programmes du navigateur client ne sont pas configurés pour diriger les demandes vers un proxy d'acheminement. Les clients ne se rendent pas compte qu'un proxy existe dans la configuration. Un routeur est configuré pour intercepter les demandes du client et pour les diriger vers le proxy transparent.

Pour plus d'informations sur la directive pour cette configuration, voir «TransparentProxy — Active le proxy transparent sous Linux», à la page 288.

Prise en charge des nouvelles fonctionnalités

Le document *Caching Proxy - Guide d'administration*, version 6.1 contient des mises à jour correctives ainsi que des informations sur de nouvelles fonctionnalités.

Les fonctionnalités les plus importantes sont les suivantes :

- Prise en charge de proxy d'acheminement
Pour plus d'informations sur la configuration d'un proxy d'acheminement, voir «Proxy d'acheminement», à la page 3.
- Prise en charge d'un proxy transparent pour les systèmes Linux uniquement

Pour plus d'informations sur la directive de proxy transparent (d'acheminement), voir «TransparentProxy — Active le proxy transparent sous Linux», à la page 288.

- Prise en charge des méthodes WebDAV, des méthodes Microsoft Exchange Server et des méthodes définies par l'utilisateur
Pour plus d'informations sur ces méthodes, voir «Méthodes Enable WebDAV, méthodes MS Exchange et méthodes définies par l'utilisateur», à la page 41.
- Directives de filtre de compression HTTP
Pour plus d'informations sur ces directives, voir «CompressionFilterAddContentType — Indique le type de contenu de la réponse HTTP à compresser», à la page 202 et «CompressionFilterEnable — Active le filtre de compression pour qu'il compresse les réponses HTTP», à la page 203.
- Directive sur la non mise en cache pour les demandes Range
Pour plus d'informations sur cette directive, voir «NoCacheOnRange — Indique la non mise en cache pour les demandes Range», à la page 246.
- Directive de mappage de règle Optimize
Pour plus d'informations sur cette directive, voir «OptimizeRuleMapping — Optimise le processus de mappage de règle pour les demandes entrantes lors de l'augmentation du nombre de règles», à la page 248.
- Directive MapQuery
Similaire à la directive Map, la directive MapQuery utilise à la fois le chemin et la chaîne de requête pour trouver les occurrences correspondant à la règle.
Pour plus d'informations sur cette directive, voir «MapQuery — Change les demandes ayant abouti en une nouvelle chaîne de demandes, à l'aide de la chaîne de demandes et du chemin de demande pour correspondance avec la règle», à la page 238.
- Directive RuleCaseSense
Pour plus d'informations sur cette directive, voir «RuleCaseSense — Mappe les demandes à partir d'URL d'applications ne faisant pas la distinction entre les minuscules et les majuscules», à la page 275.
- Pour les systèmes AIX, d'autres directives permettent de prendre en charge la carte IBM 4960 PCI Cryptographic Accelerator Card.
Pour plus d'informations sur ces directives, voir «PKCS11DefaultCert, PKCS11DriverPath, PKCS11TokenPassword — Prend en charge la carte IBM 4960 PCI Cryptographic Accelerator Card (AIX uniquement)», à la page 252.
- Directive d'option d'expression logique sur le certificat SSLCertificate
Pour plus d'informations sur l'option d'expression logique sur cette directive, voir «SSLCertificate — Spécifie les libellés des clés pour les certificats», à la page 281.
- Options supplémentaires disponibles pour la règle Proxy ou ProxyWAS
Caching Proxy fournit des directives qui requièrent une forme de correspondance supplémentaire lors de l'exécution. Pour améliorer les performances de Caching Proxy, vous pouvez utiliser ces directives comme des options de la règle Proxy ou ProxyWAS. Pour plus d'informations sur ces options supplémentaires pour la règle Proxy ou ProxyWAS, voir «Proxy — Identifie les protocoles de proxy ou le proxy inversé», à la page 263.

Chapitre 2. Utilisation des formulaires de configuration et d'administration

Caching Proxy est fourni avec des formulaires HTML qui peuvent être servis aux clients demandeurs et utilisés pour configurer le serveur proxy. Ces formulaires exécutent des programmes CGI qui modifient le fichier de configuration du serveur proxy local, `ibmproxy.conf`. Pour pouvoir utiliser ces formulaires, le serveur proxy doit être en cours d'exécution et doit être configuré de manière à transmettre les formulaires à partir du répertoire local où ils résident.

Par défaut, Caching Proxy est installé avec des directives `PASS` incluses dans le fichier `ibmproxy.conf` pour permettre l'accès aux formulaires de configuration et d'administration. Lorsqu'un client demande la page d'accueil par défaut de ce serveur proxy, `Frntpage.html` est servie. Cette page contient un lien hypertexte vers la page de départ des formulaires de configuration et d'administration, `wte.html`.

Les formulaires de configuration et d'administration sont protégés et requièrent l'authentification du client pour être servis. Vous trouverez les instructions de configuration de l'ID et du mot de passe de l'administrateur dans la section «Configuration du mot de passe administrateur», à la page 9.

Ressources requises avec le navigateur

Un navigateur utilisé pour accéder aux formulaires de configuration et d'administration doit assurer les fonctions suivantes :

- *HTML 4.0* : Tous les formulaires sont conformes à la norme HTML 4.0. Votre navigateur Web doit prendre en charge HTML 4.0 et les jeux de cadres.
- *Java 1.1 et JavaScript* : les applets doivent être conformes aux spécifications Java 1.1. Votre navigateur Web doit supporter une machine virtuelle Java compatible avec Java 1.1. Les applets ne sont pas compatibles avec Java 2.0. JavaScript et Java doivent être activés.
- *256 couleurs* : Le poste de travail sur lequel s'exécute le navigateur Web doit prendre en charge 256 couleurs au minimum.

Il est **recommandé** d'utiliser les navigateurs Mozilla et Firefox (pour les systèmes Linux, UNIX et Windows) et Internet Explorer (pour les systèmes Windows). Pour des versions précises des navigateurs Mozilla, Firefox et Internet Explorer, consultez le site Web suivant et suivez les liens conduisant à la page Web voulue : <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

Remarques :

1. Sur les systèmes Linux PowerPC 64 bits, vous ne pourrez pas accéder aux formulaires de configuration et d'administration avec le navigateur Mozilla car aucun kit SDK n'est disponible pour cette architecture. Vous pourrez accéder à ces formulaires à partir d'une autre machine dotée d'un navigateur Web pris en charge.
2. Si vous êtes invité deux fois à vous connecter lorsque vous démarrez la console d'administration, le paramètre Java n'est peut-être pas défini correctement dans Internet Explorer. Pour le corriger, sélectionnez **Tools>Internet Options>Advanced** et décochez la case **Use Java 2 v1.4.X**.

Accès aux formulaires de configuration et d'administration

Pour accéder aux formulaires de configuration et d'administration :

1. Assurez-vous que le serveur proxy est actif. Pour plus d'informations sur le démarrage du serveur proxy, voir Chapitre 5, «Démarrage et arrêt de Caching Proxy», à la page 15.
2. Utilisez un navigateur HTTP pour demander la page d'accueil de votre serveur proxy (Frntpage.html) ou la page de départ de configuration et d'administration (wte.html).

Remarque : Cette page dépend des règles de mappage de votre serveur proxy et peut différer des pages par défaut mentionnées entre parenthèses.

`http://nom.du.serveur[:port][/répertoire][page.html]`

où

- *nom.du.serveur* correspond au nom complet de l'hôte (par exemple, `http://www.ibm.com/`).
 - *[:port]* Si le serveur proxy est à l'écoute des demandes d'administration sur un port autre que 80, indiquez le numéro du port après le nom du serveur : `http://nom.du.serveur:port`
 - *[/répertoire]* L'ajout d'un répertoire dans l'URL dépend des règles de mappage.
 - *[/page.html]* La page HTML ne doit être spécifiée que si elle n'apparaît pas en tant que page d'accueil. Pour plus d'informations sur les pages de bienvenue, voir «Définition de pages de bienvenue par défaut», à la page 50.
3. Cliquez sur les **formulaires de configuration et d'administration** pour afficher les formulaires de configuration du serveur. Vous êtes invité à indiquer le nom et le mot de passe de l'administrateur. Tapez le nom et le mot de passe d'un utilisateur autorisé. La fenêtre du client de configuration Caching Proxy apparaît.

Remarques :

- a. Après l'affichage de la page principale, il est possible que le chargement des données du cadre de navigation prenne quelques secondes.
 - b. Sous Windows 2003, les connexions demandant des formulaires d'administration (scripts CGI) peuvent être réinitialisées avant d'être complètement établies. Les navigateurs risquent donc d'afficher des messages indiquant que les données n'ont pas été reçues ou que la page n'est pas disponible. Pour éviter de rencontrer cette erreur, associez `MaxActiveThreads` à une valeur supérieure à 200 ou associez `ConnThreads` à une valeur supérieure à 50 afin de corriger les connexions réinitialisées. Pour plus d'informations sur les directives, voir «`MaxActiveThreads` — Spécifie le nombre maximal d'unités d'exécution actives», à la page 239 et «`ConnThreads` — Définition du nombre d'unités d'exécution de connexions à utiliser pour la gestion des connexions», à la page 203.
4. Le cadre de navigation de gauche affiche les cinq grandes catégories de formulaires de configuration :
 - **Configuration de proxy**
 - **Configuration de la mémoire cache**
 - **Configuration du serveur**
 - **Moniteur de l'activité du serveur**
 - **Configuration du plug-in**

Cliquez sur le pointeur triangulaire situé à gauche de chaque en-tête pour afficher les formulaires de configuration de cette catégorie. Cliquez sur un formulaire pour l'ouvrir. Le formulaire affiche les valeurs de configuration en cours (s'il y a lieu) dans les zones de saisie. Si vous n'avez pas redéfini la configuration depuis l'installation, les valeurs par défaut apparaissent.

5. Dans le formulaire de votre choix, entrez les données de configuration d'une fonction spécifique. Chaque formulaire donne des instructions pour vous aider à effectuer les modifications appropriées. Pour plus d'informations, cliquez sur l'icône d'aide, le point d'interrogation (?) en haut de chaque formulaire. Elle donne accès aux liens suivants :
 - **Aide de zone**—Description des zones de chaque panneau
 - **Procédures**—Instructions détaillées permettant d'effectuer des tâches spécifiques dans le formulaire
 - **Index**—Index des rubriques d'aide
6. Une fois le formulaire complété, vous devez cliquer sur **Validation** pour mettre à jour la configuration du serveur et valider les modifications effectuées. Le bouton **Validation** se trouve sous les zones de saisie du formulaire. Si vous ne voulez pas valider les modifications apportées au formulaire, cliquez sur **Restauration** afin de rétablir les valeurs initiales.
7. Si vous cliquez sur **Validation** et que vos modifications sont acceptées, le message suivant s'affiche dans le cadre supérieur :

Les modifications de configuration demandées ont été effectuées.

Si les modifications ne sont pas acceptées, un message d'erreur apparaît dans le cadre supérieur et indique quels paramètres ne sont pas acceptables.

8. Pour redémarrer le serveur proxy, cliquez sur l'icône correspondante (I) dans le cadre supérieur. Lorsque le serveur proxy reçoit la commande de redémarrage, il rejette les demandes envoyées par les clients mais il termine le traitement des demandes en cours. Après le rechargement du fichier de configuration mis à jour, le serveur proxy recommence à accepter les demandes des clients.

Remarque : Pour appliquer la modification de certaines directives (obtenues par l'utilisation des formulaires de configuration et d'administration ou par la modification du fichier `ibmproxy.conf`), il ne suffit pas de redémarrer le serveur ; il faut l'arrêter complètement et le relancer. Ces directives sont indiquées dans le tableau 6, à la page 175.

Configuration du mot de passe administrateur

Après avoir installé les modules Caching Proxy, vous devez créer une identification et un mot de passe administrateur pour accéder aux formulaires de configuration et d'administration. La configuration par défaut du serveur proxy authentifie les utilisateurs qui demandent les formulaires de configuration et d'administration à l'aide du fichier de mots de passe `webadmin.passwd` situé dans le répertoire `/opt/ibm/edge/cp/racine_serveur/protect/` sur les systèmes Linux et UNIX ou dans le répertoire `\Program Files\IBM\edge\cp\etc\` sur les systèmes Windows. L'installation d'un module n'écrase pas le fichier `webadmin.passwd` existant.

Utilisez les commandes suivantes pour ajouter une entrée d'administrateur dans le fichier `webadmin.passwd` :

- Sur les systèmes Linux et UNIX :

```
# htadm -adduser /opt/ibm/edge/cp/racine_serveur/protect/webadmin.passwd
```

A l'invite du système, indiquez pour le programme **htadm** le nom d'utilisateur, le mot de passe et le nom réel de l'administrateur.

- Sur les systèmes Windows :

```
cd "\Program Files\IBM\edge\cp\server_root\protect\"  
htadm -adduser webadmin.passwd"
```

A l'invite du système, indiquez pour le programme **htadm** le nom d'utilisateur, le mot de passe et le nom réel de l'administrateur.

Remarque : Les majuscules sont différenciées des minuscules dans le nom d'utilisateur de l'administrateur et son mot de passe même si elles ne sont pas différenciées dans le système d'exploitation. Veillez à saisir le nom d'utilisateur et le mot de passe exacts lorsque vous utilisez la commande **htadm** pour accéder aux formulaires.

Pour une description détaillée de la commande **htadm**, voir «htadm, commande», à la page 167.

Chapitre 3. Utilisation de l'assistant Configuration

L'assistant Configuration de Caching Proxy vous permet de configurer rapidement une machine Caching Proxy préalablement installée. Ce programme définit uniquement les directives principales nécessaires pour modifier le comportement de Caching Proxy de sorte qu'il joue le rôle de serveur de substitution. Le serveur proxy peut nécessiter une configuration supplémentaire.

Pour utiliser l'assistant Configuration de Caching Proxy :

1. Lancez l'assistant de configuration.

Sous Windows, cliquez sur **Démarrer -> Programmes -> IBM WebSphere -> Edge Components -> Caching Proxy -> Assistant de configuration**.

Sur les systèmes Linux et UNIX : entrez la commande `/opt/ibm/edge/cp/cpwizard/cpwizard.sh`

2. Sélectionnez le port réseau sur lequel le serveur proxy sera à l'écoute des demandes HTTP.
3. Entrez le nom du serveur de données cible.
4. Entrez l'ID utilisateur et le mot de passe de l'administrateur du serveur proxy.

Remarques :

1. L'assistant de configuration définit les directives suivantes :

`Port port`

`Proxy /* http://serveur de données :port`

2. Si vous utilisez l'assistant de configuration pour configurer le serveur proxy, une règle de correspondance doit être créée pour les demandes du proxy reçues sur le port 443 pour que SSL puisse être activé. Pour plus d'informations, voir «Définition de règles de mappage», à la page 42.

Exemples :

`Proxy /* http://serveur de données :443`

ou

`Proxy /* https://serveur de données :443`

Limitations sur les systèmes Linux : les raccourcis clavier ne fonctionnent pas dans l'assistant de configuration de Caching Proxy.

Chapitre 4. Modification manuelle du fichier ibmproxy.conf

Caching Proxy peut être configuré manuellement en modifiant le fichier de configuration ibmproxy ou en utilisant les formulaires de configuration et d'administration.

- Sur les systèmes Linux et UNIX, le fichier ibmproxy.conf se trouve dans le répertoire /etc/.
- Sur les systèmes Windows, le fichier ibmproxy.conf se trouve dans le répertoire C:\Program Files\IBM\edge\cp\etc\en_US\.

Le fichier de configuration se compose d'instructions appelées « directives ». Pour redéfinir la configuration, modifiez le fichier de configuration et les directives, puis sauvegardez les nouveaux paramètres. Pour éditer le fichier de configuration, vous pouvez utiliser presque tous les éditeurs de texte, y compris emacs et vi.

Remarque : Cependant, n'employez pas l'éditeur de texte inclus dans l'environnement Common Desktop Environment (CDE) de Solaris. Cet éditeur modifie parfois le groupe d'appartenance du fichier et change les propriétés du lien du fichier de telle sorte que les formulaires de configuration et d'administration ne peuvent plus y écrire.

Les modifications apportées au fichier de configuration prennent effet au redémarrage du serveur, sauf si vous avez modifié l'une des directives identifiées dans le tableau 6, à la page 175. Si vous avez modifié l'une de ces directives, vous devez arrêter, puis redémarrer le serveur. Pour plus d'informations, voir Chapitre 5, «Démarrage et arrêt de Caching Proxy», à la page 15.

L'Annexe B, «Directives du fichier de configuration», à la page 175 décrit toutes les directives du fichier de configuration et donne des explications sur la syntaxe à respecter.

Chapitre 5. Démarrage et arrêt de Caching Proxy

Caching Proxy est conçu pour s'exécuter en continu en tant que processeur d'arrière-plan nécessitant une intervention humaine minimale. Le serveur proxy démarre lors du cycle d'amorçage de l'ordinateur et ne s'arrête que lorsqu'une opération de maintenance est requise. Il peut être démarré manuellement lorsque cela est nécessaire. Le serveur proxy accepte également une instruction de démarrage, destinée à l'arrêter puis à la redémarrer sans interrompre les connexions client actives.

Démarrage et arrêt automatiques sur les systèmes Linux et UNIX

Sur les systèmes Linux et UNIX, un script d'initialisation **ibmproxy** et les liens symboliques associés sont placés dans les répertoires `/etc/` appropriés lors de l'installation de Caching Proxy. Ces scripts sont ensuite intégrés aux routines de démarrage et d'arrêt du système d'exploitation. Vous pouvez modifier les paramètres de configuration en vue d'un redémarrage automatique en modifiant le script **ibmproxy** et les options de commande **ibmproxy**.

Remarque : Limite du descripteur de fichier sous Solaris

Il se peut que le script de démarrage du système du Caching Proxy ne puisse pas définir le nombre maximal de descripteurs de fichiers souhaité en raison de la limite de Solaris à l'échelon du système en matière de descripteurs de fichiers. Si le nombre maximal de descripteurs à l'échelon du système est inférieur à celui défini dans le script de démarrage du système du Caching Proxy, c'est le nombre limite défini à l'échelon du système qui est utilisé. Vous pouvez modifier le nombre limite de descripteurs de fichiers afin d'éviter d'éventuels incidents de performance du proxy qui pourraient résulter d'une valeur limite trop petite (inférieure à 1024). Utilisez la commande **ulimit** pour afficher le nombre de descripteurs actuellement disponibles. Si cette valeur est inférieure à 1024, augmentez la valeur limite du descripteur de fichier. Pour augmenter cette dernière à 1024, ajoutez la ligne suivante dans le fichier `/etc/system` :

```
set rlim_fd_cur=0x400
```

Désactivation du démarrage et de l'arrêt automatiques

Pour désactiver le démarrage et l'arrêt automatiques :

- Sur les systèmes AIX, supprimez la commande **ibmproxy** du fichier d'initialisation.
- Sur les systèmes HP-UX, supprimez les liens suivants à **ibmproxy** :
 - `/sbin/rc1.d/K154ibmproxy`
 - `/sbin/rc2.d/S880ibmproxy`
- Sous Linux, supprimez les liens symboliques vers `/etc/rc.d/init.d/ibmproxy` dans les répertoires de niveau d'exécution.

Sous SUSE Linux, supprimez les liens suivants jusqu'à **ibmproxy** :

- `/etc/rc.d/rc3.d/S20ibmproxy`
- `/etc/rc.d/rc3.d/K20ibmproxy`

- /etc/rc.d/rc4.d/S20ibmproxy
- /etc/rc.d/rc4.d/K20ibmproxy
- /etc/rc.d/rc5.d/S20ibmproxy
- /etc/rc.d/rc5.d/K20ibmproxy

Sous Red Hat Linux, supprimez les liens suivants jusqu'à **ibmproxy** :

- /etc/rc.d/rc0.d/K54ibmproxy
- /etc/rc.d/rc1.d/K54ibmproxy
- /etc/rc.d/rc2.d/K54ibmproxy
- /etc/rc.d/rc6.d/K54ibmproxy
- /etc/rc.d/rc3.d/S88ibmproxy
- /etc/rc.d/rc5.d/S88ibmproxy

- Sous Solaris, supprimez la commande **ibmproxy start** et les deux scripts kill associés comme suit :
 - Supprimez S88ibmproxy dans le répertoire /etc/rc2.d.
 - Supprimez K54ibmproxy dans le répertoire /etc/rc0.d.
 - Supprimez K54ibmproxy dans le répertoire /etc/rc1.d.

Démarrage manuel sur les systèmes Linux et UNIX

Quelle que soit la méthode de démarrage, la commande **ibmproxy** est appelée, soit directement à partir de la ligne de commande, soit à partir d'un script. Pour une description détaillée de la commande **ibmproxy**, voir «ibmproxy, commande», à la page 172. Voici les arguments les plus couramment utilisés.

Sur AIX :

- Pour démarrer le serveur proxy configuré avec les paramètres régionaux par défaut à l'aide de la commande **startsrc**, tapez la commande suivante :
startsrc -s ibmproxy
- Pour démarrer le serveur proxy configuré avec les paramètres régionaux par défaut à l'aide de la commande **startsrc**, tapez la commande suivante :
startsrc -s ibmproxy -e "LC_ALL=locale"
- Pour démarrer le serveur proxy configuré avec les paramètres d'exécution par défaut à l'aide de la commande **startsrc**, tapez la commande suivante :
ibmproxy

Sous HP-UX :

- Pour démarrer le serveur proxy sans exécuter le script d'initialisation, tapez la commande suivante à l'invite root :
/sbin/init.d/ibmproxy start
- Pour démarrer le serveur proxy en tant que processus d'arrière-plan sans exécuter le script d'initialisation, tapez la commande suivante à l'invite root :
/usr/sbin/ibmproxy
- Pour démarrer le serveur proxy en tant que processus de premier plan sans exécuter le script d'initialisation, tapez la commande suivante à l'invite root :
/usr/sbin/ibmproxy -nobg

Sous Linux :

- Pour démarrer le serveur proxy sans exécuter le script d'initialisation, tapez la commande suivante à l'invite root :
`/etc/rc.d/init.d/ibmproxy start`
- Pour démarrer le serveur proxy en tant que processus d'arrière-plan sans exécuter le script d'initialisation, tapez la commande suivante à l'invite root :
`/usr/sbin/ibmproxy`
- Pour démarrer le serveur proxy en tant que processus de premier plan sans exécuter le script d'initialisation, tapez la commande suivante à l'invite root :
`/usr/sbin/ibmproxy -nobg`
- Pour démarrer le serveur proxy à l'aide d'un fichier de configuration SQUID préexistant, `squidConfig.file`, à l'invite de root :
`squidConfig.file -r /etc/errors_icons.conf`
où le fichier `errors_icons.conf` identifie les icônes correspondant aux types de fichiers indiqués lors de la navigation dans les répertoires.

Sous Solaris :

- Pour démarrer le serveur proxy sans exécuter le script d'initialisation, tapez la commande suivante à l'invite root :
`/etc/init.d/ibmproxy start`
- Pour démarrer le serveur proxy en tant que processus d'arrière-plan sans exécuter le script d'initialisation, tapez la commande suivante à l'invite root :
`/usr/sbin/ibmproxy`
- Pour démarrer le serveur proxy en tant que processus de premier plan sans exécuter le script d'initialisation, tapez la commande suivante à l'invite root :
`/usr/sbin/ibmproxy -nobg`

Démarrage en tant que service Windows

Si Caching Proxy est installé en tant que service Windows, le démarrage s'effectue de la même façon que pour les autres services Windows :

1. Cliquez sur **Démarrer** → **Paramètres (pour Windows 2000)** → **Panneau de configuration**.
2. Dans la fenêtre **Panneau de configuration**, cliquez deux fois sur **Outils d'administration** → **Services**.
3. Dans la fenêtre **Services**, mettez en évidence **Caching Proxy**.
4. Cliquez sur **Démarrer** pour lancer le service Caching Proxy.

Si Caching Proxy est installé en tant que service, il peut être configuré pour démarrer automatiquement lors du lancement de Windows. Dans ce cas, il n'est pas nécessaire de se connecter pour que le proxy traite les demandes. Pour que le serveur démarre automatiquement :

1. Cliquez sur **Démarrer** → **Paramètres (pour Windows 2000)** → **Panneau de configuration**.
2. Dans la fenêtre **Panneau de configuration**, cliquez deux fois sur **Outils d'administration** → **Services**.
3. Dans la fenêtre **Services**, mettez en évidence **Caching Proxy**.
4. Cliquez sur le bouton d'option **Automatique**, puis sur **Démarrer** pour lancer le service Caching Proxy automatiquement au démarrage de Windows.

Régénération de la variable d'environnement PATH

Si Caching Proxy est défini comme Démarré dans la fenêtre **Services** mais que le proxy ne fonctionne pas, il se peut que la machine n'ait pas été redémarrée après l'installation du proxy. Si le service Caching Proxy est paramétré de manière à interagir avec le bureau et que vous ne redémarrez pas la machine, le message d'erreur ci-après peut apparaître dans une boîte de dialogue en incrustation :
Message catalog error: the message catalog could not be loaded or is invalid

Vous devez alors redémarrer la machine de manière à ce que la valeur de la variable d'environnement PATH soit régénérée dans la base de registres Windows. Si cette valeur n'est pas régénérée, il est possible que la variable PATH affiche Caching Proxy et les chemins GSK7 corrects mais que le fonctionnement du serveur présente des anomalies.

Remarque : Une incompatibilité risque de se produire sur les systèmes Windows quand Caching Proxy et une application, telle qu'un système de fichiers en réseau, s'exécutent en tant que services. Il arrive que Caching Proxy n'interprète pas correctement un chemin contenant un pilote éloigné appartenant à une application de type système de fichiers, elle-même exécutée en tant que service.

Cet incident se produit si le chemin d'accès au service du système de fichiers apparaît avant celui du service Caching Proxy dans la variable d'environnement PATH de Windows. Vous pouvez remédier à cela en modifiant la variable PATH et en plaçant les services de systèmes de fichiers à la fin de la définition.

Cet incident n'a aucun effet sur les unités éloignées contrôlées par les applications qui ne sont pas exécutées en tant que services Windows. Par exemple, Caching Proxy peut accéder aux unités partagées sur d'autres machines Windows visibles via un réseau local (LAN).

Démarrage en tant qu'application Windows

Utilisation du menu Démarrer

Si Caching Proxy est installé en tant qu'application Windows, la procédure d'installation crée une entrée **Caching Proxy** comme sous-menu du menu **Démarrer**. Pour lancer Caching Proxy en tant qu'application, sélectionnez **Démarrer -> Programmes -> IBM WebSphere -> Edge Components -> Caching Proxy**.

Cette procédure de démarrage lance le serveur proxy à l'aide des paramètres de configuration en cours. Pour définir d'autres valeurs de paramètres lors du démarrage, utilisez la procédure de démarrage à partir de la commande (voir la section suivante).

Utilisation de l'invite de commande

Pour démarrer le serveur à partir de n'importe quelle invite de commande Windows ou DOS, utilisez la commande **ibmproxy**. Si vous n'avez pas arrêté et redémarré Windows depuis l'installation du serveur, vous devez entrer le nom du chemin complet de la commande, comme suit (par défaut) :

c:\Program Files\IBM\edge\cp\bin\ibmproxy.exe

La commande **ibmproxy** démarre le serveur à l'aide des paramètres de configuration en cours. Si vous n'avez pas modifié la configuration du serveur depuis l'installation, la configuration en cours est basée sur les informations entrées au cours de ce processus et sur les options par défaut.

La commande **ibmproxy** démarre le serveur en tant qu'application, même si vous avez installé Caching Proxy pour qu'il fonctionne en tant que service. Pour forcer l'exécution du serveur en tant qu'application, vous pouvez également indiquer l'option de commande **-noservice**. Toute autre option de commande modifie les paramètres de configuration au moment de l'exécution.

Lancement de plusieurs serveurs proxy

Plusieurs instances du serveur proxy peuvent s'exécuter simultanément mais chacune doit être connectée à un port distinct. Sur les systèmes AIX, une seule instance peut être lancée avec la fonction SRC. Des fichiers de configuration uniques doivent être indiqués pour toutes les instances du serveur, étant donné que le fichier de configuration identifie un numéro de port qui doit être différent pour chaque serveur sur une machine donnée. Pour démarrer une autre instance du serveur (une instance au moins étant en cours), tapez la commande suivante à l'invite :

- Sous Linux et UNIX :
`ibmproxy -r autre_fichier_config`
- Sous Windows :
`ibmproxy -noservice -r autre_fichier_config`

où *autre_fichier_config* est un fichier de configuration unique.

Lorsque vous démarrez plusieurs instances du serveur, enregistrez l'ID du processus affiché pour chacune d'elles. Ces ID sont requis pour arrêter des instances spécifiques du serveur.

Remarque : Sur les systèmes Linux exécutant plusieurs instances du serveur, la commande **/etc/rc.d/init.d/ibmproxy stop** permet d'arrêter le dernier serveur qui a été démarré. Les autres instances doivent être arrêtées séparément. Pour plus d'informations, voir «Arrêt manuel sur les systèmes Linux et UNIX».

Arrêt manuel sur les systèmes Linux et UNIX

Pour arrêter le serveur :

- Vous devez être l'utilisateur ayant démarré le processus ou le superutilisateur root.
- Vous devez employer la même méthode que celle utilisée pour démarrer le serveur. Le tableau suivant répertorie les méthodes de démarrage et les méthodes d'arrêt associées.

Tableau 2. Méthode de démarrage et méthodes d'arrêt pour systèmes Linux et UNIX

Méthode de démarrage	Méthode d'arrêt
A partir de /etc/inittab (sous AIX)	Entrez <code>stopsrc -s ibmproxy</code>
A partir de /sbin/init.d (sous HP-UX)	Entrez <code>/sbin/init.d/ibmproxy stop</code>
A partir de /etc/rc.d/init.d (sous Linux)	Entrez <code>/etc/rc.d/init.d/ibmproxy stop</code>

Tableau 2. Méthode de démarrage et méthodes d'arrêt pour systèmes Linux et UNIX (suite)

ibmproxy	<ol style="list-style-type: none"> 1. Pour rechercher l'ID processus ibmproxy : sous AIX, tapez <code>ps -aef grep "ibmproxy"</code>. Sous Linux, tapez <code>ps -aux grep ibmproxy grep ID_serveur</code>. Sous Solaris et HP-UX, entrez <code>ps -ef grep "ibmproxy"</code> 2. Pour arrêter le processus ibmproxy : tapez <code>kill id_processus</code> <p>Pour arrêter tous les serveurs sur cette machine : tapez <code>killall ibmproxy</code></p>
ibmproxy -nobg	Tapez <code>ctrl-c</code>
ibmproxy -r -autre_fichier_config(sous AIX)	Tapez <code>stopsrc -s ibmproxy -p id_processus</code>
ibmproxy -r -autre_fichier_config(sous Linux)	<ol style="list-style-type: none"> 1. Pour rechercher l'ID processus ibmproxy : tapez <code>ps aux grep ibmproxy grep id_processus</code> 2. Pour arrêter le processus ibmproxy : tapez <code>kill id_processus</code>

Remarque : Si vous avez démarré le proxy transparent, vous devez décharger l'extension du noyau du proxy transparent et les règles du pare-feu qui lui sont associées, après avoir arrêté le serveur Caching Proxy. En tant qu'utilisateur root, entrez la commande suivante :

```
ibmproxy -unload
```

Pour arrêter le serveur à l'invite root, tapez :

- Sous AIX : `stopsrc -s ibmproxy`
- Sous HP-UX : `/sbin/init.d/ibmproxy stop`
- Sous Linux : `/etc/rc.d/init.d/ibmproxy stop`
- Sous Solaris : `/etc/init.d/ibmproxy stop`

Limites des commandes d'arrêt

Les limitations suivantes s'appliquent lors de l'utilisation des commandes d'arrêt :

• AIX, HP-UX et Linux

Sur les systèmes AIX, HP-UX et Linux, il arrive que les commandes d'arrêt du système Caching Proxy arrêtent uniquement le processus Caching Proxy. La commande AIX à l'origine de ce comportement est la suivante : **stopsrc -s ibmproxy**. La commande HP-UX et Linux à l'origine de ce comportement est la suivante : **ibmproxy -stop**.

L'exécution du processus PACD, qui est utilisé par le serveur LDAP, peut continuer après l'arrêt du serveur proxy. Vous pouvez arrêter le processus PACD en toute sécurité en utilisant la commande **kill** de la manière suivante :

```
kill -15 id_processus_PACD
```

• Solaris

Le lancement de la commande **ibmproxy -stop** sur un système Solaris ne produit pas le même effet que sur d'autres systèmes d'exploitation. En raison d'une limitation liée au code sous Solaris, l'étape d'arrêt du serveur n'est pas exécutée lorsque la commande **ibmproxy -stop** est utilisée sur des plateformes Solaris.

Cette limitation a des incidences sur le logiciel serveur proxy, ainsi que sur les plug-ins implémentés par le client.

L'exécution du processus PACD, utilisé par le serveur LDAP, peut continuer après l'arrêt du serveur proxy. Vous pouvez arrêter le processus PACD en toute sécurité en utilisant la commande **kill** de la manière suivante :

```
kill -15 ID_processus_PACD
```

Arrêt manuel sur un système Windows

Vous pouvez arrêter le serveur Caching Proxy de la même manière que vous arrêtez les programmes Windows.

Si le serveur est installé en tant que service :

1. Cliquez sur **Démarrer -> Paramètres (pour Windows 2000) -> Panneau de configuration**.
2. Dans la fenêtre **Panneau de configuration**, cliquez deux fois sur **Outils d'administration -> Services**.
3. Dans la fenêtre **Services**, mettez en évidence **Caching Proxy**.
4. Cliquez sur **Arrêter** pour arrêter le service Caching Proxy.

Si le serveur proxy n'est pas installé en tant que service, effectuez l'une des opérations suivantes pour arrêter Caching Proxy :

- Cliquez sur l'icône x située dans l'angle supérieur droit.
- Dans le menu **Fichier**, cliquez sur **Quitter**.
- Appuyez sur les touches **Alt + F4**.

Redémarrage après modifications de la configuration

Après avoir modifié la configuration du serveur (à l'aide des formulaires de configuration et d'administration ou en modifiant le fichier `ibmproxy.conf`), vous devez le redémarrer pour que les modifications soient effectives. Dans la plupart des cas, vous pouvez redémarrer le serveur sans l'arrêter. Toutefois, cette procédure ne régénère pas certains paramètres. Pour plus d'informations, voir tableau 6, à la page 175.

Pour redémarrer le serveur sans l'arrêter au préalable, cliquez sur le bouton **Redémarrer** situé dans le formulaire de configuration et d'administration ou entrez la commande suivante : `ibmproxy -restart`

Partie 2. Configuration et réglage du processus Caching Proxy

Cette partie traite des interactions du composant Caching Proxy avec le système d'exploitation, les périphériques et le réseau. Elle propose également des procédures de configuration de ces interactions. Ces éléments de configuration du serveur proxy, gérés par l'administrateur système, doivent être coordonnés avec les ressources réseau, telles que les adresses IP et les noms d'hôte, ainsi qu'avec les ressources systèmes, telles que la mémoire disponible et les cycles du processeur.

Cette partie comporte les chapitres suivants :

Chapitre 6, «Définition du serveur», à la page 25

Chapitre 7, «Définition de l'appartenance des processus», à la page 27

Chapitre 8, «Gestion de connexions», à la page 29

Chapitre 9, «Configuration du processus du serveur proxy», à la page 33

Chapitre 6. Définition du serveur

Caching Proxy s'exécute généralement en tant que processus d'arrière-plan sur un système hôte configuré pour fonctionner comme serveur réseau. Ce processus est associé à (*lié à*) une ou toutes les adresses IP (Internet Protocol) actives de l'ordinateur hôte. Il est à l'écoute de différents protocoles Internet, tels que FTP et HTTP, sur des ports spécifiés et effectue des actions selon la configuration de son comportement. Pour plus d'informations, voir Partie 3, «Configuration du comportement de Caching Proxy», à la page 37.

Par défaut, Caching Proxy porte le nom du système hôte. Pour remplacer ce comportement par défaut, il suffit d'indiquer un nom d'hôte pour le serveur proxy. Afin de lier Caching Proxy à une adresse IP spécifique, le nom d'hôte du serveur proxy doit correspondre à cette adresse.

Remarque : Au cas où le serveur proxy tente de se connecter à une adresse IP et que le nom n'est pas associé à une adresse IP disponible, la liaison échoue et le serveur proxy sera à l'écoute de toutes les adresses IP disponibles.

Le nom d'hôte du serveur proxy n'a aucune incidence sur la résolution du trafic. Le serveur proxy ne compare pas son nom d'hôte avec la valeur de l'argument nom d'hôte dans l'entête de la demande HTTP. Le nom d'hôte du serveur proxy figure, le cas échéant, dans des pages de données locales dynamiques. Il est également renvoyé au client demandé sous la forme de valeur de l'argument Via de l'en-tête HTTP.

Il est possible de configurer le serveur proxy de manière à remplacer le nom d'hôte du client demandeur par le nom de celui-ci avant de transférer le serveur de destination. Ceci oblige le serveur de destination à établir une connexion indirecte via le serveur proxy, au lieu d'une connexion directe avec le client.

Pour définir le processus du serveur proxy, indiquez l'emplacement physique des fichiers sur le système hôte, le nom à l'aide duquel le serveur proxy fait référence à lui-même et les ports d'écoute, à l'aide des directives ServerRoot, Hostname et Port, respectivement. Si l'hôte possède plusieurs adresses IP, le serveur proxy peut être lié à une adresse spécifique en associant la valeur de la directive BindSpecific à On, et la valeur de la directive Hostname à cette adresse IP.

Un port d'administration fournit une méthode d'accès aux formulaires de configuration et d'administration et de gestion du serveur. Pour fournir un accès au serveur proxy via un port d'administration, associez une valeur à la directive AdminPort. Les demandes reçues sur le port d'administration ne sont pas placées en file d'attente avec les demandes reçues sur le port standard. Il est possible d'écrire des règles de mappage pour autoriser l'accès aux formulaires de configuration et d'administration sur ce port.

Lorsque la directive BindSpecific est activée, Caching Proxy est lié au port indiqué par la directive Port avec l'adresse IP définie à partir de la valeur de la directive Hostname. Le port indiqué par la directive AdminPort est lié à toutes les adresses IP disponibles sur le système.

Pour remplacer le nom par défaut du serveur en cours d'exécution, tel que IBM-PROXY ou IBM_HTTP_SERVER, associez une valeur à la directive HeaderServerName. Cette valeur figure dans la zone du serveur de réponse HTTP.

Pour améliorer les performances du proxy, la valeur de la directive PureProxy doit être fixée sur on. Ceci a pour effet de désactiver toutes les fonctions de mise en cache.

Directives associées

Les directives ci-dessous définissent le processus du serveur proxy :

- «Hostname — Spécifie le nom de domaine complet ou l'adresse IP du serveur», à la page 224
- «ServerRoot — Spécifie le répertoire dans lequel est installé le programme du serveur», à la page 278
- «HeaderServerName — Indique le nom du serveur proxy retourné dans l'entête HTTP», à la page 224
- «BindSpecific — Spécifie si le serveur est lié à une ou à plusieurs adresses IP», à la page 189
- «Port — Spécifie le port sur lequel le serveur attend les demandes», à la page 254
- «AdminPort — Spécifie le port pour les demandes de pages ou de formulaires d'administration», à la page 185
- «PureProxy — Désactive un proxy dédié», à la page 268

Pour plus d'informations, voir Chapitre 4, «Modification manuelle du fichier ibmproxy.conf», à la page 13.

Formulaires de configuration et d'administration

Les formulaires de configuration et d'administration suivants modifient les valeurs des directives associées :

- **Configuration du serveur -> Paramètres de base -> Nom d'hôte**
- **Configuration du serveur -> Paramètres de base -> Racine du serveur**
- **Configuration du serveur -> Paramètres de base -> Numéro(s) de port par défaut**
- **Configuration du serveur -> Paramètres de base -> Numéro de port de l'administrateur**
- **Configuration du serveur -> Paramètres de base -> Options de liaison**
- **Configuration du proxy -> Performances du proxy -> Exécuter en tant que proxy pur**

Remarque : Vous ne pouvez pas utiliser les formulaires de configuration et d'administration pour éditer la directive HeaderServerName.

Pour plus d'informations, voir Chapitre 2, «Utilisation des formulaires de configuration et d'administration», à la page 7.

Chapitre 7. Définition de l'appartenance des processus

Quand un utilisateur autre que le superutilisateur root démarre Caching Proxy, cet utilisateur devient propriétaire de tous les processus associés au serveur proxy. Cependant, si le superutilisateur root démarre Caching Proxy, une fonction ID utilisateur de groupe lit les directives UserId et GroupId du fichier de configuration afin d'associer les processus à l'utilisateur et au groupe indiqués. L'objectif est de limiter les accès aux fichiers et de protéger l'ordinateur. Si vous modifiez les directives UserId et GroupId, vous devez mettre à jour l'appartenance et les droits d'accès aux répertoires des journaux et d'autres fichiers utilisés par le serveur proxy, à l'aide d'une liste de contrôle d'accès (ACL).

Pour définir l'appartenance du processus du serveur proxy, indiquez l'identification de l'utilisateur, l'identification du groupe et l'emplacement du fichier de stockage de l'ID processus, à l'aide des directives UserID, GroupID et PidFile, respectivement.

Pour forcer le processus du serveur proxy à s'exécuter au premier plan, définissez la valeur de la directive NoBG sur on.

Sous Linux :

Sous Linux, seuls les processus et les unités d'exécution à l'écoute de connexions sont touchés par la modification de leur appartenance. Les processus et les unités d'exécution responsables d'autres activités dans le flux des travaux restent la propriété de root. Chaque processus et unité d'exécution reçoit un numéro d'identification de processus (PID). La commande **ps** permet de dresser la liste des PID, qu'ils soient ou non associés à un processus ou à une unité d'exécution.

Remarque : Avec certains noyaux Linux, Caching Proxy peut générer le message d'erreur suivant dans ce journal d'erreurs :

Cannot init groups for user nobody, errno: 1

Vous pouvez ignorer ce message d'erreur car il n'affecte pas le fonctionnement normal de Caching Proxy. Pour éviter que ce message d'erreur s'affiche, vous pouvez exporter les variables d'environnement suivantes avant de démarrer Caching Proxy :

```
export RPM_FORCE_NPTL=1
export LD_ASSUME_KERNEL=2.4.19:
```

Directives associées

Les directives ci-dessous permettent de définir l'appartenance du processus de serveur proxy :

- «UserId — Spécifie l'ID utilisateur par défaut», à la page 289
- «GroupId — Spécifie l'ID de groupe», à la page 223
- «NoBG — Exécute le processus Caching Proxy en avant-plan», à la page 244
- «PidFile (Linux et UNIX uniquement) — Définition du fichier utilisé pour stocker l'ID processus de Caching Proxy», à la page 252

Pour plus d'informations, voir Chapitre 4, «Modification manuelle du fichier ibmproxy.conf», à la page 13.

Formulaires de configuration et d'administration

Les formulaires de configuration et d'administration suivants modifient les valeurs des directives associées :

- **Configuration du serveur -> Paramètres de base -> ID utilisateur**
- **Configuration du serveur -> Paramètres de base -> ID groupe**
- **Configuration du serveur -> Paramètres de base -> Emplacement du fichier des ID de processus**

Remarque : Vous ne pouvez pas utiliser les formulaires de configuration et d'administration pour éditer la directive NoBG.

Pour plus d'informations, voir Chapitre 2, «Utilisation des formulaires de configuration et d'administration», à la page 7.

Chapitre 8. Gestion de connexions

Caching Proxy génère une nouvelle unité d'exécution pour chaque demande client. Si aucune unité d'exécution n'est disponible, le serveur proxy met les demandes en attente tant que celles-ci ne sont pas disponibles. La quantité de mémoire requise par le serveur proxy est proportionnelle au nombre d'unités d'exécution actives. Spécifiez le nombre maximal d'unités d'exécution actives pour la directive `MaxActiveThreads`.

Les connexions en file d'attente indiquent le nombre de connexions client que le serveur consigne avant de refuser les connexions d'autres clients. Ce nombre dépend du nombre de demandes que le serveur peut traiter en l'espace de quelques secondes. Un serveur doit répondre à une connexion client avant la durée d'expiration. A l'aide de la directive `ListenBacklog`, indiquez le nombre maximal de connexions admises en file d'attente.

Le serveur proxy peut gérer les connexions permanentes client-serveur. Les connexions permanentes permettent au serveur d'accepter plusieurs demandes du client et d'envoyer les réponses sur la même connexion TCP/IP. L'utilisation de connexions permanentes permet de réduire le délai d'attente des clients et de diminuer la charge de traitement du serveur proxy, tout cela au prix d'une petite augmentation de la mémoire du serveur. Une hausse globale du débit se produit lorsque le serveur n'établit pas une nouvelle connexion TCP/IP pour chaque demande et réponse et que les performances d'une connexion TCP/IP sont plus élevées lorsque la connexion est permanente.

Le regroupement de connexions côté serveur offre les avantages des connexions permanentes sur le serveur en permettant de réutiliser les connexions existantes entre un proxy inverse et les serveurs d'origine. Chaque connexion réutilisée économise trois paquets TCP (deux établissements de liaisons à trois voies pour ouvrir la connexion et un établissement de liaison pour la fermer). Parmi les avantages du regroupement de connexions côté serveur, on peut citer :

- Une réduction de l'encombrement du réseau (grâce au nombre moindre d'ouvertures et de fermetures de connexions)
- Une diminution du temps UC consacré aux routeurs, aux clients et aux serveurs
- Une diminution de l'utilisation de mémoire pour les clients et les serveurs
- Sur les demandes de mémoire cache non satisfaites, une réponse plus rapide du proxy (en raison du nombre moindre d'ouvertures et de fermetures de connexions)

Remarque : Le regroupement des connexions est recommandé uniquement dans un environnement contrôlé. Il peut en effet entraîner une baisse des performances si les serveurs d'origine ne sont pas compatibles avec HTTP 1.1. Il est également essentiel que les serveurs d'origine soient paramétrés correctement. Voici un exemple simple tiré du fichier de configuration d'Apache 1.3.19 :

- `#KeepAlive`: Indique s'il faut autoriser les connexions permanentes (plus d'une demande par connexion). Attribuez-lui la valeur `Off` pour désactiver cette fonction.
- `KeepAlive On`

- `#MaxKeepAliveRequests`: Nombre maximal de demandes à autoriser pendant une connexion permanente. Attribuez-lui la valeur 0 pour autoriser un nombre de demandes illimité. Ce nombre doit être élevé pour permettre des performances maximales.#
- `Max KeepAliveRequests` 0
- `#KeepAliveTimeout` : Nombre de secondes d'attente pour la demande suivante provenant du même client sur la même connexion
- `KeepAliveTimeout` 240

Ces paramètres maintiennent les connexions aux serveurs Web ouvertes tant qu'elles sont utilisées et permettent au proxy de gérer les connexions à la place du serveur d'origine. Par conséquent, les connexions seront regroupées uniquement dans la mesure des besoins.

Lorsque le regroupement des connexions côté serveur est activé, les connexions HTTP aux serveurs d'origine sont regroupées. Les connexions SSL sont également regroupées sur des configurations lorsque la directive `SSLEnable` du serveur proxy a la valeur on.

Vous pouvez configurer la gestion du regroupement des connexions en indiquant le nombre maximal de sockets inactives à conserver en permanence par serveur, le délai d'attente du serveur avant l'arrêt d'une connexion permanente inactive, et le délai après lequel l'unité d'exécution du processus de récupération de place recherche les connexions expirées (la valeur par défaut est deux minutes).

Définissez la durée d'activité des connexions à l'aide des directives `InputTimeout`, `OutputTimeout`, `PersistTimeout`, `ReadTimeout` et `ScriptTimeout`.

Directives associées

Les directives ci-dessous gèrent des connexions avec le processus du serveur proxy :

- «`MaxActiveThreads` — Spécifie le nombre maximal d'unités d'exécution actives», à la page 239
- «`ConnThreads` — Définition du nombre d'unités d'exécution de connexions à utiliser pour la gestion des connexions», à la page 203
- «`ListenBacklog` — Spécifie le nombre de connexions client en file d'attente devant être gérées par le serveur», à la page 233
- «`ProxyPersistence` — Autorise les connexions permanentes», à la page 266
- «`MaxPersistRequest` — Spécifie le nombre maximal de demandes à recevoir au niveau d'une connexion permanente», à la page 241
- «`ServerConnPool` — Spécifie la mise en pool des connexions avec les serveurs d'origine», à la page 277
- «`MaxSocketPerServer` — Spécifie le nombre maximal de sockets inactives ouvertes pour le serveur», à la page 242
- «`ServerConnTimeout` — Spécifie la période d'inactivité maximale», à la page 277
- «`ServerConnGCRun` — Spécifie l'intervalle d'exécution de l'unité d'exécution du processus de récupération de place», à la page 276
- «`PersistTimeout` — Spécifie la durée d'attente avant que le client n'envoie une autre demande», à la page 251
- «`InputTimeout` — Spécifie le délai d'entrée», à la page 229
- «`ReadTimeout` — Spécifie la durée limite pour une connexion», à la page 270

- «OutputTimeout — Spécifie le délai de sortie», à la page 249
- «ScriptTimeout – Spécifie le paramètre de délai pour les scripts», à la page 275

Pour plus d'informations, voir Chapitre 4, «Modification manuelle du fichier ibmproxy.conf», à la page 13.

Formulaires de configuration et d'administration

Les formulaires de configuration et d'administration suivants modifient les valeurs des directives associées :

- **Configuration du serveur → Gestion de système → Performances → Nombre maximal d'unités d'exécution actives**
- **Configuration du serveur → Gestion de système → Performances → Taille des connexions en file d'attente**
- **Configuration du proxy → Performances du proxy → Permettre les connexions persistantes**
- **Configuration du serveur → Gestion de système → Performances → Nombre maximal de demandes**
- **Configuration du serveur → Gestion de système → Performances → Délai de persistance**
- **Configuration du serveur → Gestion de système → Délais d'expiration → Délai d'expiration d'entrée**
- **Configuration du serveur → Gestion de système → Délais d'expiration → Délai de lecture**
- **Configuration du serveur → Gestion de système → Délais d'expiration → Délai de sortie**
- **Configuration du serveur → Gestion de système → Délais d'expiration → Délai de script**
- **Configuration du serveur → Gestion de système → Délais d'expiration → Délai de persistance**

Remarques :

1. Vous ne pouvez pas utiliser les formulaires de configuration et d'administration pour éditer les directives ServerConnPool, MaxsocketPerServer, ServerConnTimeout et ServerConnGCRun.
2. Le délai de persistance peut être modifié dans le formulaire **Configuration du serveur → Gestion de système → Performances** ou dans le formulaire **Configuration du serveur → Gestion de système → Délais d'expiration**.

Pour plus d'informations, voir Chapitre 2, «Utilisation des formulaires de configuration et d'administration», à la page 7.

Chapitre 9. Configuration du processus du serveur proxy

Vous pouvez améliorer les performances de Caching Proxy de manière sensible en configurant le système et en ajustant ses paramètres. Les suggestions suivantes portent sur l'amélioration de la configuration et l'ajustement des paramètres.

Définition des directives liées aux performances

Les directives ci-dessous influent notablement les performances du processus du serveur proxy :

- «PureProxy — Désactive un proxy dédié», à la page 268. Cette fonction améliore les performances système en désactivant la mise en mémoire cache.
- «ProxyPersistence — Autorise les connexions permanentes», à la page 266. Cette fonction permet d'établir des connexions permanentes entre clients et serveurs. Les connexions permanentes réduisent les retards liés à la demande de documents sur le serveur proxy mais requièrent une largeur de bande réseau supérieure et une unité d'exécution de serveur spécialisée pour chaque connexion. N'activez pas les connexions permanentes si la configuration limite le nombre des unités d'exécution disponibles.

Les zones de formulaire de configuration et d'administration suivantes modifient les valeurs des directives associées :

- **Configuration du proxy -> Performances du proxy : Exécuter en tant que proxy pur**
- **Configuration du proxy -> Performances du proxy : Permettre les connexions persistantes**

Examen d'autres applications

Examinez les services ou les démons qui s'exécutent sur le système, et, pour augmenter la mémoire et le nombre de cycles processeur, supprimez ceux qui ne sont pas nécessaires. Par exemple, si un serveur Web fournissant un nombre de pages réduit est installé sur le système, utilisez Caching Proxy en tant que serveur Web unique. Désactivez les autres serveurs Web de la manière suivante :

- Sous AIX : Examinez /etc/inittab
- Sous Linux : Examinez /etc/rc.d/rcx.d pour connaître le niveau d'exécution par défaut du système (2 en général).
- Sous HP-UX et Solaris : Examinez /etc/rcx.d pour connaître le niveau d'exécution par défaut de votre système (2 en général).
- Sur les systèmes Windows :
 1. Sélectionnez **Démarrer -> Paramètres (pour Windows 2000) -> Panneau de configuration -> Outils d'administration -> Services**.
 2. Recherchez les services non requis mais configurés sur Automatique.
 3. Modifiez le type de lancement de ces services en sélectionnant Manuel au lieu d'Automatique.

Vérification de l'espace de pagination

Assurez-vous que le système comporte un espace de pagination suffisant pour fonctionner correctement. L'espace de pagination du système doit être deux fois supérieur à la quantité de mémoire physique. Si possible, répartissez l'espace de pagination entre plusieurs unités physiques. Par exemple, un serveur Netfinity 5000 doté de 512 Mo de mémoire et de cinq unités SCSI doit comporter au total un gigaoctet d'espace de pagination, soit environ 200 Mo sur chaque unité.

Configuration du système de fichiers

Caching Proxy crée et détruit un grand nombre de fichiers au cours de son fonctionnement. Si le serveur proxy consigne les accès (dans le journal des accès, le journal des accès au proxy ou le journal des accès à la mémoire cache), transférez les journaux dans leurs systèmes de fichiers respectifs afin qu'ils n'occupent pas l'espace réservé à une autre fonction (la mémoire cache par exemple) si leur taille s'accroît de manière inattendue).

Réglage de la configuration TCP/IP

Caching Proxy est sensible aux modifications apportées aux configurations TCP/IP. Réduire les valeurs TCP/IP d'un système d'exploitation peut amener serveur proxy à fonctionner de manière inattendue. Plus précisément, si les valeurs TCP/IP sont trop faibles, les connexions risquent d'être réinitialisées par les clients qui se connectent à serveur proxy ou par les serveurs d'origine auquel le proxy se connecte. C'est notamment le cas pour les clients qui se connectent à serveur proxy via une connexion de faible largeur de bande (56700 bps ou moins). Soyez prudent si vous devez réduire les valeurs des paramètres TCP/IP.

Réglage du délai d'attente TCP des environnements à forte charge (HP-UX, Linux, Solaris, Windows)

Le délai d'attente TCP correspond au temps pendant lequel un socket attend un paquet FIN provenant de l'émetteur avant de provoquer la fermeture de la connexion. Dans les environnements à forte charge, le serveur proxy peut sembler bloqué lorsqu'un grand nombre de sockets restent à l'état TIME_WAIT une fois leurs connexions fermées. La réduction du délai d'attente TCP réduit le nombre de sockets en attente et, dans les environnements à forte charge, permet d'éviter que le serveur proxy semble bloqué. Il est préférable de fixer ce délai à 5 secondes.

Pour fixer le délai d'attente TCP à 5 secondes, procédez comme suit :

- Sous HP-UX :

Emettez la commande suivante :

```
ndd /dev/tcp -set délai_attente_tcp 5000
```

Utilisez l'utilitaire "sam" pour associer au moins la valeur 2048 au paramètre de noyau max_thread_proc.

Remarque : Pensez également à ajuster les paramètres de noyau suivants :
maxfiles, maxfiles_lim, maxproc, shmem, tcp_conn_request_max,
tcp_ip_abort_interval, tcp_keepalive_interval,
tcp_rexmit_interval_initial, tcp_rexmit_interval_max,
tcp_rexmit_interval_min, tcp_xmit_hiwater_def,
tcp_rcv_hiwater_def.

- Sous Linux :
Emettez les commandes suivantes :

```
echo "1024 61000" > /proc/sys/net/ipv4/fourchette_ports_local_ip  
echo "5" > /proc/sys/net/ipv4/délaiExpiration_fin_tcp
```
- Sous Solaris :
Emettez la commande suivante :

```
ndd /dev/tcp -set délai_attente_tcp 5000
```


Modifiez comme suit le fichier /etc/system :

```
set tcp:tcp_conn_hash_size=8129
```
- Sous Windows :
Vous devez créer une entrée de registre qui définit un délai d'attente TCP. Pour plus d'informations, reportez-vous à votre documentation Windows.

Ajustement du noyau Linux

Plusieurs limites du noyau Linux sont faibles et peuvent être modifiées. Certaines peuvent être modifiées par le biais du système de fichiers /proc, et pour d'autres une recompilation du noyau est nécessaire.

Remarque : Le système de fichiers /proc est virtuel, c'est-à-dire qu'il n'existe pas physiquement sur le disque. Il sert plutôt d'interface dans le noyau Linux. Le système de fichiers n'existant pas, les valeurs d'entrée définies sont perdues au redémarrage. Ainsi, placez les modifications que vous voulez apporter au système de fichiers /proc dans le fichier /etc/rc.d/rc.local sous RedHat ou dans le fichier /etc/rc.config sous SUSE. Ainsi, les modifications sont toujours activées au redémarrage.

Voici quelques recommandations :

- La valeur maximale du descripteur de fichier est 4096 par défaut. Il est possible de la modifier en ajoutant la ligne suivante dans le fichier rc.local :

```
echo 32768 > /proc/sys/fs/file-max
```
- La valeur inode maximale est de 16384 par défaut. Il est possible de la modifier en ajoutant la ligne suivante dans le fichier rc.local :

```
echo 65536 > /proc/sys/fs/inode-max
```
- Par défaut, les numéros de ports TCP et UDP sont compris entre 1024 et 4999. Il est possible de définir une fourchette de numéros de ports compris entre 32768 et 61000 en ajoutant la ligne suivante dans le fichier rc.local :

```
echo 32768 61000 > /proc/sys/net/ipv4/fourchette_ports_local_ip
```
- Par défaut, le nombre de tâches autorisées est de 512. Cette valeur a une incidence sur le nombre maximal d'unités d'exécution mises en oeuvre pour un processus lorsqu'un trop grand nombre d'autres tâches sont en cours. Il est possible de faire passer ce nombre à 2048 en modifiant la valeur de NR_TASKS dans le fichier *YourKernelSource/include/linux/tasks.h*.
- Il convient également d'attribuer la valeur 24 à MIN_TASKS_LEFT_FOR_ROOT. Vous devez recompiler le noyau pour que cette modification prenne effet.

Si vous voulez recompiler le noyau, activez uniquement les options dont vous avez réellement besoin. N'exécutez pas un démon dont vous ne vous servez pas.

Variables d'ajustement des unités d'exécution AIX

Sur les systèmes AIX, vous pouvez améliorer les performances de Caching Proxy à l'aide des unités d'exécution du système et en permettant aux unités d'exécution d'utiliser plusieurs segments. Les performances sont liées à la capacité de multitraitement du système d'exploitation et à la planification des unités d'exécution du système d'exploitation sous-jacent. Vous pouvez améliorer les performances en définissant les variables d'ajustement des unités d'exécution AIX de la façon suivante :

```
export AIXTHREAD_SCOPE=S
export SPINLOOPTIME=500
export YIELDLOOPTIME=100
export MALLOCMULTIHEAP=1
```

Vous pouvez définir ces variables d'environnement avant de lancer `/usr/sbin/ibmproxy` ou les ajouter à `/etc/rc.ibmproxy` si vous utilisez **startsrc -s ibmproxy** pour démarrer le serveur proxy. Une fois ces variables d'ajustement des unités d'exécution modifiées, l'amélioration des performances sera plus visible sur des systèmes SMP. Toutefois, dans certains cas, vous pourrez également la remarquer sur des systèmes monoprocesseur.

Remarque : Pour plus de détails sur les variables d'ajustement des unités d'exécution, consultez la documentation de votre système d'exploitation AIX.

Partie 3. Configuration du comportement de Caching Proxy

Cette partie décrit la manière dont le composant Caching Proxy répond aux demandes client, et propose des procédures de configuration de ce comportement. Ces éléments de la configuration du serveur proxy, généralement gérés par l'administrateur Web, n'ont aucun effet sur d'autres processus du système hôte ou d'autres ordinateurs du réseau.

Cette partie comporte les chapitres suivants :

Chapitre 10, «Gestion du traitement des demandes», à la page 39

Chapitre 11, «Gestion de la livraison de données locales», à la page 49

Chapitre 12, «Gestion de connexions FTP», à la page 53

Chapitre 13, «Personnalisation du traitement sur le serveur», à la page 57

Chapitre 14, «Configuration des options d'en-tête», à la page 67

Chapitre 15, «A propos de l'interface de programmation d'application», à la page 69

Chapitre 10. Gestion du traitement des demandes

Lors de la réception d'une demande client, Caching Proxy effectue l'action indiquée dans la zone méthode sur l'objet indiqué dans la zone URL, à condition que la méthode demandée ait été activée. Le serveur proxy résout l'URL à l'aide d'un jeu de règles de mappages définies par l'administrateur. Ces règles de mappage ordonnent à Caching Proxy de jouer le rôle d'un serveur Web et de récupérer l'objet à partir du système de fichiers local, ou de jouer le rôle d'un serveur proxy et de récupérer l'objet sur le serveur d'origine.

Ce chapitre traite de l'activation de méthodes, de la définition de règles de mappage et de la configuration d'un serveur proxy de substitution.

Activation des méthodes HTTP/FTP

Les demandes que les clients transmettent au serveur comprennent une zone Méthode indiquant l'action que le serveur doit effectuer sur l'objet indiqué.

La liste ci-après répertorie les méthodes acceptées par le serveur proxy, ainsi qu'une description de la réponse du serveur proxy à une demande contenant une méthode activée.

Remarque : Certaines méthodes s'appliquent aux demandes HTTP et FTP. L'activation de ces méthodes pour HTTP entraîne également leur activation pour FTP.

CONNECT

La méthode CONNECT permet d'acheminer par tunnel les demandes et les réponses via le serveur proxy. S'applique aux configurations avec proxy d'acheminement uniquement.

Pour des informations sur le format et les options disponibles pour la méthode Enable CONNECT, voir «Configuration de l'établissement des tunnels SSL», à la page 120.

DELETE

Le serveur proxy supprime l'objet identifié par l'adresse URL. DELETE permet aux clients de supprimer des fichiers de Caching Proxy. Vous devez utiliser les configurations de protection pour définir les personnes autorisées à lancer cette méthode, ainsi que le type de fichiers à traiter. Pour plus d'informations, voir Chapitre 25, «Configurations de protection du serveur», à la page 113.

GET Le serveur proxy renvoie les données identifiées par l'adresse URL. Si l'adresse URL fait référence à un programme exécutable, le proxy renvoie les données générées par ce programme. Cette méthode permet de gérer les connexions permanentes.

HEAD

Le serveur proxy ne renvoie que l'en-tête de document HTTP identifié par l'URL, mais pas le corps du document.

OPTIONS

Le serveur proxy renvoie des informations sur les options de communication de la chaîne demande-réponse identifiée par l'adresse URL.

Cette méthode permet au client de déterminer les options et les contraintes associées à un objet, ainsi que les fonctions du serveur sans avoir à intervenir ou à extraire l'objet.

POST La demande contient des données et une adresse URL. Le serveur proxy accepte les données de la demande comme le nouveau subordonné de la ressource identifiée dans l'adresse URL qui traite les données. La ressource peut être un programme d'acceptation des données, une passerelle vers un autre protocole ou un programme distinct acceptant les commentaires.

La méthode POST est conçue pour gérer l'annotation de ressources existantes. Elle permet notamment d'envoyer un message à un tableau d'affichage, un forum, une liste d'adresses ou un autre groupe de ressources similaire, d'envoyer un bloc de données, par exemple d'un formulaire vers un programme de gestion de données, ou encore d'étendre une base de données via une opération d'ajout **append**. Pour Caching Proxy, la méthode POST permet de traiter les formulaires de configuration et d'administration.

Cette méthode permet de gérer les connexions permanentes.

PUT La demande contient des données et une adresse URL. Le serveur proxy stocke les données dans la ressource identifiée dans l'URL. Si la ressource existe déjà, la méthode PUT la remplace par les données contenues dans la demande. Si la ressource n'existe pas, elle la crée et y entre les données contenues dans la demande. Cette méthode permet de gérer les connexions permanentes.

L'activation de la méthode PUT permet de copier les fichiers sur le composant Caching Proxy à l'aide des protocoles HTTP et FTP. Dans la mesure où la méthode PUT permet aux clients d'écrire sur Caching Proxy, vous devez utiliser les configurations de protection du serveur pour définir les personnes autorisées à utiliser cette méthode ainsi que le type de fichier traité. (Voir Chapitre 25, «Configurations de protection du serveur», à la page 113.)

TRACE

Le serveur proxy répercute le message de la demande envoyée par le client. Cette méthode permet au client de voir ce qui est reçu à l'autre extrémité de la chaîne et d'utiliser ces données à des fins de test ou de diagnostic. Le type de contenu de la réponse du proxy est message/http.

Directives associées

Les directives suivantes activent les méthodes HTTP/FTP :

- «Enable — Active les méthodes HTTP», à la page 212
- «Disable — Désactive les méthodes HTTP», à la page 211

Pour plus d'informations, voir Chapitre 4, «Modification manuelle du fichier ibmproxy.conf», à la page 13.

Formulaires de configuration et d'administration

Les formulaires de configuration et d'administration suivants modifient les valeurs des directives associées :

- **Configuration du serveur -> Traitement des demandes -> Méthodes HTTP -> GET**
- **Configuration du serveur -> Traitement des demandes -> Méthodes HTTP -> HEAD**

- Configuration du serveur -> Traitement des demandes -> Méthodes HTTP -> POST
- Configuration du serveur -> Traitement des demandes -> Méthodes HTTP -> PUT
- Configuration du serveur -> Traitement des demandes -> Méthodes HTTP -> DELETE
- Configuration du serveur -> Traitement des demandes -> Méthodes HTTP -> OPTIONS
- Configuration du serveur -> Traitement des demandes -> Méthodes HTTP -> TRACE
- Configuration du serveur -> Traitement des demandes -> Méthodes HTTP -> CONNECT

Remarque : Si vous désactivez la méthode POST, vous ne pourrez pas utiliser les formulaires de configuration et d'administration pour configurer Caching Proxy.

Pour plus d'informations, voir Chapitre 2, «Utilisation des formulaires de configuration et d'administration», à la page 7.

Méthodes Enable WebDAV, méthodes MS Exchange et méthodes définies par l'utilisateur

S'applique aux configurations avec proxy inversé uniquement.

Outre la prise en charge des méthodes HTTP standard, Caching Proxy accepte l'acheminement d'autres méthodes définies dans des spécifications RFC ou utilisées par certaines applications. Caching Proxy prend également en charge des méthodes définies par l'utilisateur et permet leur acheminement via le serveur proxy.

WebDAV (Web-based Distributed Authoring and Versioning) est un ensemble d'extensions du protocole HTTP qui vous permet de modifier et de gérer des fichiers sur des serveurs Web distants de façon collaborative. Caching Proxy prend en charge les méthodes WebDAV, les méthodes utilisées par Microsoft Exchange Server et les méthodes définies par l'utilisateur (personnalisées).

Ces méthodes sont définies dans le code et sont gérées par les directives Enable et Disable. Les administrateurs peuvent également utiliser le masque de méthode correspondant défini dans la directive PROTECT pour autoriser l'utilisation de ces méthodes.

Méthodes WebDAV prises en charge (RFC 2518) : PROPFIND , PROPPATCH , MKCOL, COPY, MOVE, LOCK, UNLOCK, SEARCH

Méthodes MS Exchange prises en charge : BMOVE, BCOPY, BDELETE, BPROPFIND, BPROPPATCH, POLL, NOTIFY, SUBSCRIBE, UNSUBSCRIBE, ACL, SUBSCRIPTIONS, X_MS_ENUMATTS

Lorsque la méthode WebDAV ou MS Exchange Server est activée, Caching Proxy achemine les demandes aux serveurs cible uniquement et ne réécrit aucun lien de ressource dans le corps de la demande.

Caching Proxy peut également acheminer au serveur dorsal des méthodes définies par l'utilisateur. Pour activer une méthode personnalisée, appliquez la syntaxe suivante à la directive Enable dans le fichier ibmproxy.conf :

Enable méthode définie par l'utilisateur [WithBody | WithoutBody]

La définition d'une valeur pour WithBody ou WithoutBody indique au proxy si la méthode définie par l'utilisateur exige un corps de demande.

Dans l'exemple suivant, la méthode définie par l'utilisateur Ma_METHODE est activée et le proxy est informé qu'elle a besoin d'un corps de demande :

Enable Ma_METHODE WithBody

Directives associées

Les directives suivantes activent les méthodes WebDAV, les méthodes MS Exchange ainsi que les méthodes définies par l'utilisateur :

- «Enable — Active les méthodes HTTP», à la page 212
- «Disable — Désactive les méthodes HTTP», à la page 211

Pour plus d'informations, voir Chapitre 4, «Modification manuelle du fichier ibmproxy.conf», à la page 13.

Définition de règles de mappage

Les règles de mappage sont des directives de configuration définissant la façon dont Caching Proxy traite les demandes client, comme leur transfert au serveur origine, leur redirection ou leur refus. La définition de règles de mappage adéquates est essentielle dans le fonctionnement de Caching Proxy. Les règles de mappage ont un effet sur les actions suivantes :

- Fonctionnement de base du proxy
- Accès aux formulaires de configuration et d'administration affichés dans le navigateur
- Capacité de placer en mémoire cache des résultats de servlet et de données générées en dynamique

Les directives de règles de mappage se présentent dans le format suivant :

règle modèle cible [adresse_IP | nom_hôte]:[port]

Seules les demandes correspondant au modèle et à la combinaison IP-port donnés sont concernées par cette règle. Un modèle peut contenir des caractères génériques ; https://**/*.asp, par exemple.

L'ordre d'apparition des règles dans le fichier de configuration est très important. Sauf pour les directives Map, dès qu'une demande correspond à un modèle, elle est traitée sans que les autres règles soient évaluées. La directive Map remplace l'URL dans la demande. Cette nouvelle demande est comparée aux autres règles de mappage.

Règles de mappage

Les règles de mappage suivantes s'appliquent aux demandes client correspondant au modèle donné :

- **Map, MapQuery** — réécrit la demande. Les règles Map et MapQuery remplacent une URL de demande (modèle) par une chaîne d'URL (cible). Après cette substitution, la demande contenant la nouvelle chaîne est comparée aux règles de mappage restantes.
- **RuleCaseSense** — permet le mappage de demandes à partir d'URL d'applications ne faisant pas la distinction entre les minuscules et les majuscules. Lorsqu'elle est désactivée, la directive RuleCaseSense permet au proxy de mapper des demandes par rapport à des règles définies dans le fichier `ibmproxy.conf` sans respect des majuscules et des minuscules.
- **Pass, Exec** — la demande est traitée localement. Les règles Pass et Exec traitent la demande sur le serveur proxy. La règle Pass mappe une URL de demande (modèle) à un fichier extrait du serveur proxy (cible) ; la règle Exec mappe une URL de demande avec un programme CGI qui s'exécute sur le serveur proxy.
- **Fail** — rejette la demande. La règle refuse une demande (modèle) sur le serveur proxy. Le traitement d'une demande correspondant au modèle d'une règle Fail s'arrête immédiatement. Les règles Fail ne possèdent pas d'arguments cible.
- **Redirect** — transfère la demande. La règle Redirect transfère une demande (modèle) à un autre serveur Web (cible). Du fait qu'une URL complète, indiquant le protocole de communication, est la cible de cette règle, il est possible de changer le protocole lors de cette redirection (pour chiffrer une requête HTTP à l'aide de SSL, par exemple). Une redirection ne vérifie pas la mémoire cache avant de satisfaire la demande.
- **Proxy, ProxyWAS** — transfère la demande. Les règles Proxy et ProxyWAS transmettent les demandes (modèles) à un autre serveur (cible). A la différence d'une règle Redirect simple, une règle Proxy permet au serveur proxy de consulter la mémoire cache, de placer en mémoire cache des données émanant de serveurs origine et d'écrire des en-têtes HTTP activant des fonctions avancées. Utilisez la règle ProxyWAS au lieu de la règle Proxy si le serveur origine est doté de IBM Application Server.

La règle de mappage suivante s'applique à la réaction du serveur origine :

- **ReversePass** — intercepte automatiquement les demandes redirigées. Dans le cadre de l'acheminement des données au client, une règle ReversePass transfère la demande du serveur origine au modèle via le serveur proxy. La directive ReversePass est conçue pour détecter un code d'état de redirection dont l'effet pour le client serait de contacter directement le serveur origine. Le client a pour ordre de contacter le serveur défini dans l'argument cible.

Les règles de mappage suivantes s'appliquent aux applications d'API :

- **nameTrans** — accepte la demande et exécute une application d'API définie par le chemin du fichier de remplacement au cours de l'étape Name Translation (conversion de nom) de la demande.
- **service** — accepte la demande et exécute une application d'API définie par le chemin du fichier de remplacement au cours de l'étape Service de la demande.

Configuration d'un serveur de substitution

Pour configurer un serveur de substitution standard, procédez comme suit :

- Affectez le numéro 80 au port du serveur proxy.
Port 80
- Ajoutez une règle Proxy au début de la liste des règles destinée à transférer au serveur origine toutes les demandes reçues sur le port 80.
Proxy /* http://serveur.de.données.com/* :80
- Activez un port d'administration sur un port autre que le port 80.
AdminPort 8080

Ceci permet de transmettre au serveur origine tout le trafic HTTP du port 80. Le trafic entrant sur le port d'administration n'est pas concerné par cette opération car il ne correspond pas à la règle de proxy générique initiale. La demande est traitée par les autres règles de mappage.

Directives associées

Les directives suivantes définissent des règles de mappage :

- «Map — Change les demandes ayant abouti en une nouvelle chaîne de demandes, à l'aide de la chaîne du chemin de demande pour correspondance avec la règle», à la page 237
- «MapQuery — Change les demandes ayant abouti en une nouvelle chaîne de demandes, à l'aide de la chaîne de demandes et du chemin de demande pour correspondance avec la règle», à la page 238
- «RuleCaseSense — Mappe les demandes à partir d'URL d'applications ne faisant pas la distinction entre les minuscules et les majuscules», à la page 275
- «Pass — Spécifie le modèle pour l'acceptation des requêtes», à la page 249
- «Exec — Exécute un programme CGI pour les demandes ayant abouti», à la page 216
- «Redirect — Spécifie un modèle pour les demandes adressées à un autre serveur», à la page 270
- «Proxy — Identifie les protocoles de proxy ou le proxy inversé», à la page 263
- «ProxyWAS — Spécifie que les demandes sont envoyées à WebSphere Application Server», à la page 268
- «ReversePass — Intercepte automatiquement les demandes redirigées», à la page 272

Pour plus d'informations, voir Chapitre 4, «Modification manuelle du fichier ibmproxy.conf», à la page 13.

Formulaires de configuration et d'administration

Le formulaire de configuration et d'administration suivant modifie les valeurs des directives associées :

- Sélectionnez **Configuration du serveur -> Traitement des demandes -> Acheminement des demandes.**

Remarque : L'argument numéro de port n'est pas pris en charge par les formulaires de configuration et d'administration.

Pour plus d'informations, voir Chapitre 2, «Utilisation des formulaires de configuration et d'administration», à la page 7.

Activation de la réécriture de jonction (facultatif)

S'applique aux configurations avec proxy inversé uniquement.

La directive `JunctionRewrite` active la routine de réécriture de jonction au sein de `Caching Proxy` pour réécrire les réponses provenant des serveurs d'origine et garantir le mappage des URL de serveur au serveur d'origine approprié lors de l'utilisation de jonctions. Le plug-in de réécriture de jonction doit également être activé. Les jonctions sont définies à l'aide des règles de mappage du proxy.

Lorsque vous utilisez les règles de mappage du serveur proxy pour définir la jonction, vous pouvez utiliser la directive `Proxy` avec ou sans l'option `JunctionPrefix`.

Définition de la jonction sans l'option `JunctionPrefix`

Voici des exemples de jonctions correctes que la routine de réécriture de jonction est capable de traiter :

- `Proxy /shop/* http://shopserver.acme.com/*`
- `Proxy /auth/* http://authserver.acme.com/*`

L'exemple suivant est un exemple de jonction valide qui n'est *pas* traité par la routine de réécriture de jonction :

- `Proxy /* http://defaultserver.acme.com/*`

Les jonctions suivantes sont incorrectes :

- `Proxy /images/*.gif http://imageserver.acme.com/images/*.gif`
- `Proxy /cgi-bin/* http://cgiserver.acme.com/cgi/perl/*`

Ces règles de mappage ont créé des jonctions pour `shopserver`, `authserver` et `b2bserver`. Supposons que `shopserver` renvoie un document HTML avec les URL suivantes dans les codes HTML appropriés :

- `/index.html` (référence liée au serveur)
- `/images/shop.gif` (référence liée au serveur)
- `buy/buy.jsp` (référence liée au répertoire)
- `http://ebay.com` (référence absolue)

La routine de réécriture de jonction réécrit les références liées au serveur à l'aide des règles de mappage du proxy, comme suit :

- `/shop/index.html` (modifié)
- `/shop/images/shop.gif` (modifié)
- `buy/buy.jsp` (non modifié)
- `http://ebay.com` (non modifié)

Définition de la jonction avec l'option `JunctionPrefix` (méthode recommandée)

Lorsque vous utilisez l'option `JunctionPrefix` avec la directive `Proxy`, vous pouvez déclarer le préfixe de jonction dans la règle `Proxy` en utilisant le format ci-dessous au lieu de déduire l'élément `JunctionPrefix` en fonction du premier modèle d'URL.

`Proxy modèle1_url modèle2_url JunctionPrefix:préfixe_url`

Lorsque vous utilisez JunctionPrefix, il n'y a pas de limitation pour le format du premier modèle d'URL. Pour permettre la prise en charge de la réécriture de jonction lorsque vous n'utilisez *pas* l'option JunctionPrefix, l'URL de proxy doit posséder le format suivant : Proxy /market/partners/*.html http://b2bserver.*/.html. Toutefois, lorsque vous utilisez JunctionPrefix, la règle Proxy suivante s'applique à la réécriture de jonction :

```
Proxy /market/partners/*.html http://b2bserver.acme.com/*.html
junctionprefix:/market/partners
```

La routine de réécriture de jonction affecte les codes suivants :

Tableau 3. Codes affectés par la routine de réécriture de jonction

Code	Attributs
!—	URL
a	href
applet	archive, codebase
area	href
base	href
body	background
del	cite
embed	pluginspage
form	action
input	src
frame	src, longdesc
iframe	src, longdesc
ilayer	src, background
img	src, usemap, lowsrc, longdesc, dynsrc
layer	src, background
link	href
meta	url
object	data, classid, codebase, codepage
script	src
table	background
td	background
th	background
tr	background

Remarque : La routine de réécriture de jonction n'affecte pas les codes générés par JavaScript ou par des plug-ins au sein du navigateur.

Directives associées

Les directives suivantes permettent d'activer le plug-in et la routine de réécriture de jonction.

- «ServerInit — Personnalise l'étape d'initialisation du serveur», à la page 277
- «Transmogrifier — Personnalise l'étape de manipulation des données», à la page 287

- «JunctionRewrite — Active réécriture de l'URL», à la page 230
- «JunctionRewriteSetCookiePath — Réécriture de l'option dans l'en-tête Set-Cookie lors d'une utilisation avec le plug-in JunctionRewrite», à la page 230
- «JunctionReplaceUrlPrefix — Remplacement d'une URL au lieu d'insérer un préfixe lors de l'utilisation du plug-in JunctionRewrite», à la page 229
- «JunctionSkipUrlPrefix — Ignorer la réécriture d'URL contenant déjà le préfixe lors d'une utilisation avec le plug-in JunctionRewrite», à la page 230

Pour plus d'informations, voir Chapitre 4, «Modification manuelle du fichier ibmproxy.conf», à la page 13.

Formulaires de configuration et d'administration

Le formulaire de configuration et d'administration suivant permet d'activer le plug-in de réécriture de jonction :

- **Configuration du serveur → Traitement des demandes → Traitement des demandes API**

Remarque : La directive JunctionRewrite n'est pas prise en charge par les formulaires de configuration et d'administration.

Pour plus d'informations, voir Chapitre 2, «Utilisation des formulaires de configuration et d'administration», à la page 7.

Utilisation de cookies à la place de JunctionRewrite

Vous pouvez utiliser des cookies pour stocker les informations de serveur dorsal de la façon suivante : un cookie est envoyé au navigateur client. Lorsque le navigateur envoie des requêtes aux ressources de la page HTML, il y associe un cookie pour que le composant Caching Proxy transmette les requêtes au serveur dorsal approprié.

Pour utiliser des cookies à la place de la directive JunctionRewrite, apportez les modifications ci-dessous au fichier ibmproxy.conf.

1. Remplacez **JunctionRewrite on** par **JunctionRewrite on UseCookie**.
2. Mettez entre commentaires le plug-in JunctionRewrite.

Vous trouverez ci-après une comparaison du plug-in JunctionRewrite et de l'implémentation des cookies.

- plug-in JunctionRewrite
 - La page HTML est réécrite.
 - Il ne prend pas en charge la réécriture des langages de script et des applets, sauf si vous utilisez le plug-in transmogrifier. Voir «Exemple de plug-in transmogrifier pour l'extension de la fonctionnalité JunctionRewrite», à la page 48.
 - Performances réduites.
 - Aucune limitation pour les configurations des serveurs dorsaux. Le client peut accéder à plusieurs serveurs dorsaux dans une session.
- Implémentation des cookies
 - La page HTML n'est *pas* réécrite. Un cookie est envoyé au client.
 - Le navigateur client doit activer la fonction de prise en charge des cookies.
 - Performances améliorées.

- Il existe des limitations pour les configurations des serveurs dorsaux. Elle ne peut être utilisée que lorsqu'un client accède à un serveur dorsal dans une session.

Remarque : Une limitation connue apparaît lorsque vous utilisez JunctionRewrite avec l'option UseCookie. Les URL de toutes les demandes ne sont pas correctement converties même si le cookie s'applique à un seul sous-répertoire de l'hôte. Pour traiter correctement les adresses URL qui sont situées sous ROOT et qui ne requièrent pas de jonction, vous disposez de deux méthodes :

- Placez les règles proxy avant la directive JunctionRewrite dans le fichier ibmproxy.conf. (Toutes les règles proxy situées avant la directive JunctionRewrite directive ne seront pas réécrites.)
- Mappez explicitement chaque adresse URL au lieu d'utiliser un caractère générique (*). Par exemple :

```
Proxy /no-junction.jpg http://login-server/no-junction.jpg
```

Exemple de plug-in transmogrifier pour l'extension de la fonctionnalité JunctionRewrite

Un exemple de code personnalisable est fourni et permet de réécrire et d'analyser les blocs de balises JavaScript (SCRIPT) et d'applet (APPLET) dans les fichiers HTML. Seul, le plug-in JunctionRewrite ne peut pas traiter les liens de ressources dans JavaScript ou dans les valeurs de paramètres de Java.

Une fois Caching Proxy installé, vous pouvez compiler le même code et le configurer de sorte qu'il s'exécute avec JunctionRewrite.

Les fichiers exemple ci-dessous se trouvent dans le sous-répertoire ...samples/cp/, dans le répertoire dans lequel vous avez téléchargé le correctif (fix pack).

- Makefile (Makefile pour ce plug-in exemple)
- junctionRewrite2.h (interface pour le gestionnaire analyseur personnalisé)
- junctionRewrite2.c (implémentation pour l'interface ci-dessus)
- scriptHandler.c (gestionnaire rewrite JavaScript exemple)
- appletHandler.c (gestionnaire de blocs Applet exemple)
- junctionRewrite2.def (fichier de définitions de plug-in Windows)
- junctionRewrite2.exp (fichier d'exportation de plug-in Linux et UNIX)

Chapitre 11. Gestion de la livraison de données locales

Les règles de mappage Pass et Exec permettent de fournir des données locales à un client demandeur. Par défaut, toute règle Pass comportant un modèle générique figure à la fin de la liste des règles de mappage. Cette règle dirige toutes les demandes ne correspondant pas aux modèles précédents afin d'extraire des fichiers d'un répertoire cible, généralement désigné sous le nom de répertoire principal des documents.

Lorsqu'il reçoit une URL sans nom de fichier, Caching Proxy traite la demande en recherchant dans le répertoire indiqué ou dans le répertoire principal des documents (si aucun répertoire n'est indiqué) un fichier correspondant à la liste des pages de bienvenue définie dans le fichier de configuration. Si plusieurs pages de bienvenue sont définies, le serveur proxy recherche les pages par ordre de définition. Ainsi, la première page de bienvenue trouvée est fournie.

La page d'accueil du serveur est la page Web affichée par défaut lorsque le serveur reçoit une demande comportant uniquement son adresse URL, sans nom de répertoire ou de fichier. Comme nous l'avons vu précédemment, la règle de mappage générique par défaut requiert que la page de bienvenue du serveur soit stockée dans le répertoire principal des documents et que le nom de fichier de la page de bienvenue corresponde à une page de bienvenue définie.

Remarque : Certains navigateurs Web utilisent le terme *page d'accueil* pour désigner la première page chargée lors du lancement du navigateur. Ce document n'utilise le terme que pour la page de bienvenue du serveur.

Ce chapitre traite de la définition du répertoire principal des documents et des pages de bienvenue.

Définition du répertoire principal des documents

Par défaut, les répertoires principaux de documents sont les suivants :

- Sous Linux et UNIX : `/opt/ibm/edge/cp/racine_serveur/pub/lang/`
- Sous Windows : `drive:\Program Files\IBM\edge\cp\server_root\pub\lang\`, ou le répertoire spécifié comme répertoire HTML lors de l'installation.

Directives associées

La directive suivante définit le répertoire principal des documents :

- «Pass — Spécifie le modèle pour l'acceptation des requêtes», à la page 249

Pour plus d'informations, voir Chapitre 4, «Modification manuelle du fichier `ibmproxy.conf`», à la page 13.

Formulaires de configuration et d'administration

Pour modifier le répertoire principal des documents dans les formulaires de configuration et d'administration, procédez comme suit :

1. Sélectionnez **Configuration du serveur** → **Traitement des demandes** → **Acheminement des demandes**.

2. Dans le tableau d'acheminement des demandes, recherchez la ligne contenant la chaîne /* (barre oblique et astérisque) dans la colonne **Modèle requête**. Cette zone définit le répertoire principal des documents. Dans la zone **Index** sous le tableau, cliquez sur le numéro correspondant à la colonne **Index** pour cette ligne.
3. Cliquez sur **Remplacer**.
4. Dans la boîte à liste déroulante **Action**, cliquez sur **Transmettre**.
5. Entrez /* dans la zone Modèle de demande d'URL.
6. Entrez le nouveau répertoire principal des documents dans la zone **Chemin du fichier de remplacement**.
7. Cliquez sur **Validation**.
8. Une fois les modifications validées, cliquez sur l'icône **Redémarrage du serveur** (I) dans le cadre du haut.

Une fois redémarré, le serveur utilise le nouveau répertoire principal des documents.

Pour plus d'informations, voir Chapitre 2, «Utilisation des formulaires de configuration et d'administration», à la page 7.

Définition de pages de bienvenue par défaut

Le serveur recherche la page d'accueil dans le répertoire principal des documents mais le fichier qu'il renvoie est déterminé par la liste de pages de bienvenue disponibles.

Pages de bienvenue

Lorsque le serveur reçoit une demande d'URL qui ne comporte pas de nom de fichier, il tente de la traiter en utilisant la liste de pages de bienvenue définies dans le fichier de configuration. Cette liste définit les fichiers à utiliser pour les pages de bienvenue par défaut. Le serveur identifie le fichier contenant la page d'accueil en comparant la liste de pages de bienvenue aux fichiers stockés dans le répertoire principal des documents. La première entrée concordante correspond au fichier présenté comme page d'accueil. Si aucune entrée concordante n'est identifiée, le serveur affiche la liste des répertoires principaux de documents.

Pour utiliser un fichier spécifique comme page d'accueil du serveur et l'afficher lorsqu'une demande ne comporte pas de répertoire ni de nom de fichier, vous devez placer le fichier dans le répertoire principal des documents et vérifier que son nom ne correspond pas à celui de l'un des fichiers figurant dans la liste des pages de bienvenue.

Le fichier de configuration par défaut définit les noms de fichiers suivants comme page de bienvenue, dans l'ordre indiqué ci-dessous :

1. welcome.html ou welcome.htm
2. index.html ou index.htm
3. Frntpage.html

Le serveur renvoie le premier fichier correspondant à un nom indiqué dans la liste. Si vous n'avez pas encore créé un fichier welcome.html ou index.html dans le répertoire principal des documents, le serveur utilise la page d'accès Frntpage.html comme page d'accueil.

Par exemple, si vous utilisez la configuration par défaut et que le répertoire principal des documents ne contient pas le fichier `welcome.html`, mais qu'il contient les fichiers `index.html` et `FrntPage.html`, le fichier `index.html` est utilisé comme page d'accueil.

Si aucune page d'accueil n'est identifiée, le contenu du répertoire principal des documents s'affiche sous la forme d'un répertoire.

Directives associées

La directive suivante définit les pages de bienvenue :

- «Welcome — Spécifie le nom des fichiers de bienvenue», à la page 292

Pour plus d'informations, voir Chapitre 4, «Modification manuelle du fichier `ibmproxy.conf`», à la page 13.

Formulaires de configuration et d'administration

Le formulaire de configuration et d'administration suivant définit les pages de bienvenue :

- **Configuration du serveur -> Répertoires et page de bienvenue -> Page de bienvenue**

Pour plus d'informations, voir Chapitre 2, «Utilisation des formulaires de configuration et d'administration», à la page 7.

Chapitre 12. Gestion de connexions FTP

S'applique aux configurations avec proxy d'acheminement uniquement.

Caching Proxy achemine les demandes d'URL de sites FTP vers le serveur FTP approprié mais ne peut être utilisé pour acheminer les demandes provenant d'un client FTP. Il ne peut prendre en charge que les demandes FTP provenant d'un client HTTP (en utilisant le modèle de protocole ftp://).

Seules les méthodes GET, PUT et DELETE sont admises pour les demandes de fichiers FTP. Seule la méthode GET est acceptée pour les demandes de listes de répertoires FTP. Par défaut, les méthodes PUT et DELETE sont désactivées dans Caching Proxy. Pour plus d'informations, voir «Activation des méthodes HTTP/FTP», à la page 39.

Ce chapitre décrit les modalités de protection des fichiers FTP et de gestion de la connexion serveur FTP, des chemins d'accès aux répertoires, et le chaînage.

Protection de fichiers FTP

Si vous avez activé les méthodes PUT ou DELETE pour télécharger ou supprimer des fichiers via FTP, vous devez définir la protection du serveur proxy FTP au moins pour les demandes PUT et DELETE. Cette disposition permet d'éviter la mise à jour non autorisée des fichiers sur le serveur FTP.

Pour protéger le traitement des demandes FTP sur le serveur proxy à partir des formulaires de configuration et d'administration, sélectionnez **Configuration du serveur -> Protection de document**. Pour créer une configuration de protection adaptée aux demandes de fichiers FTP, indiquez ftp:// au début du modèle de demande. Par exemple, pour protéger les fichiers du répertoire exams, utilisez le modèle ftp://exams/*.

Pour plus d'informations sur la création de configurations de protection, voir Chapitre 25, «Configurations de protection du serveur», à la page 113.

Connexion au serveur via FTP

Si l'ID utilisateur et le mot de passe ne sont pas indiqués dans l'adresse URL de la demande, Caching Proxy tente de se connecter anonymement au serveur FTP demandé (en utilisant l'ID utilisateur ANONYMOUS). De nombreux serveurs FTP requièrent une adresse électronique comme mot de passe pour établir une connexion anonyme FTP. Si le serveur FTP demande un mot de passe pour une connexion anonyme, Caching Proxy envoie l'adresse e-mail indiquée par la directive WebmasterEmail dans le fichier de configuration.

Pour définir l'adresse de l'administrateur du Web à partir des formulaires de configuration et d'administration, sélectionnez **Configuration du serveur -> Gestion de système -> SNMP MIB**. Vous pouvez également utiliser la directive WebmasterEmail. Pour plus d'informations, voir la section de référence : «WebMasterEMail — Définit une adresse électronique pour la réception des rapports d'un serveur sélectionné», à la page 291.

Si le serveur FTP indiqué dans l'adresse URL requiert un ID utilisateur et un mot de passe spécifiques pour la connexion, vous pouvez entrer ces valeurs dans l'URL, par exemple :

`ftp://idutilisateur:motdepasse@hôteserveurftp/`

Si vous ne voulez pas indiquer le mot de passe associé à l'ID utilisateur FTP dans l'adresse URL de la demande, il est possible d'entrer uniquement l'ID utilisateur dans l'URL : `ftp://idutilisateur@hôteserveurftp`. Caching Proxy tente d'abord de se connecter au serveur FTP qui présente l'ID utilisateur indiqué mais pas de mot de passe. Si la connexion sans mot de passe échoue, le navigateur vous invite à indiquer le mot de passe à associer à l'ID utilisateur.

Si vous ne tentez pas de vous connecter en mode anonyme, vous devez au moins indiquer l'ID utilisateur dans l'adresse URL. Si l'ID utilisateur n'est pas indiqué, le système cherche à établir une connexion anonyme sans inviter le client à préciser l'ID.

Gestion de chemins d'accès aux répertoires FTP

Vous devez indiquer à Caching Proxy si vous souhaitez que les noms de chemin dans les URL de sites FTP soient interprétés comme étant relatifs au répertoire de travail de l'utilisateur ou relatifs au répertoire principal. Par exemple, si un utilisateur connecté à un serveur FTP possède le répertoire de travail par défaut `/export/home/user1`, et s'il souhaite récupérer un fichier nommé `test1.exe` dans un sous-répertoire appelé `test`, le proxy utilise les URL suivantes pour récupérer le fichier FTP, selon le mode d'interprétation utilisé :

- Si le chemin d'accès *absolu* est appliqué : `ftp://util1:util1pw@hôteFTP/export/home/util1/test/test1.exe`
- Si le chemin d'accès *relatif* est appliqué : `ftp://util1:util1pw@hôteFTP/test/test1.exe`

Si des chemins relatifs sont définis pour les adresses URL de sites FTP, les utilisateurs ont toujours la possibilité d'indiquer un nom de chemin absolu en remplaçant la valeur initiale `/` par `%2F` pour indiquer le répertoire principal. Par exemple, si l'utilisateur `user1`, dont le répertoire de travail est `/export/home/user1`, souhaite accéder à un fichier situé dans le répertoire de travail de `user2`, `/export/home/user2`, la demande `ftp://user1:user1pw@FTPhost/%2Fexport/home/user2/file` est interprétée correctement comme une URL relative au répertoire principal de fichiers `/` (c'est-à-dire en tant que nom de chemin absolu), même si des noms de chemins relatifs ont été choisis pour les URL de sites FTP.

Pour définir la manière dont les URL de sites FTP sont interprétées dans les formulaires de configuration et d'administration, sélectionnez **Configuration du proxy** -> **Performances du proxy**. Dans la partie inférieure du formulaire, sous **Chemins des URL FTP**, sélectionnez **chemins absolus** pour spécifier le répertoire racine du serveur ou **chemins relatifs** pour spécifier le répertoire de travail de l'utilisateur comme point de départ du chemin.

Ce paramètre peut également être défini dans le fichier de configuration du proxy ; pour plus d'informations, voir «`FTPUrlPath` — Indique comment interpréter les URL FTP», à la page 221.

Gestion de chaînage FTP

Si vous enchaînez plusieurs serveurs proxy Web, vous pouvez demander que les demandes contenant des URL FTP soient transmises à un serveur proxy Web chaîné et qu'elles ne soient pas envoyées directement au serveur FTP. Pour définir un serveur proxy chaîné pour les demandes FTP dans les formulaires de configuration et d'administration, sélectionnez **Configuration du proxy -> Chaînes de proxy et domaines de connexion directe**. Le modèle de protocole `http://` est utilisé pour indiquer l'URL du proxy chaîné, même s'il s'agit de demandes de chaînage pour un modèle de protocole `ftp://`.

Pour configurer le chaînage FTP en utilisant le fichier de configuration du proxy, voir la section de référence «`ftp_proxy` — Spécifie un autre serveur proxy pour les demandes FTP», à la page 221.

Chapitre 13. Personnalisation du traitement sur le serveur

Le présent chapitre explique comment utiliser les inclusions côté serveur pour insérer des informations dans des programmes CGI et des documents HTML qui sont livrés à un client. Elle évoque également la personnalisation des messages d'erreur du serveur et le mappage des ressources.

Inclusions côté serveur

Les inclusions côté serveur permettent d'ajouter des informations à des programmes CGI et à des documents HTML que le serveur envoie au client lorsqu'il assure la fonction de serveur d'origine (pas aux objets placés dans le proxy ou la mémoire cache). La date en cours, la taille du fichier et la date de la dernière modification sont des exemples d'informations qui peuvent être envoyées au client. La présente section indique le format de commande à respecter pour utiliser les inclusions côté serveur. Elle explique également comment exécuter les commandes pour intégrer correctement les inclusions côté serveur aux programmes CGI et aux documents HTML. Par ailleurs, vous pouvez utiliser les inclusions côté serveur pour personnaliser les pages d'erreur.

Considérations sur les inclusions côté serveur

Avant d'utiliser les inclusions sur le serveur, vous devez prendre en considération les questions de performances, de sécurité et de risques.

- Les performances peuvent être fortement limitées si le serveur traite et envoie simultanément des fichiers.
- La sécurité peut être compromise si vous laissez des utilisateurs standard exécuter des commandes sur le serveur. Choisissez soigneusement les répertoires où vous placerez les inclusions côté serveur et ceux où vous placerez la commande **exec**. Vous pouvez réduire les risques en n'activant pas la commande **exec**.
- L'utilisation d'inclusions côté serveur peut provoquer des incidents. Par exemple, il n'est pas possible de référencer les fichiers de manière récursive : si vous exécutez le fichier `sleepy.html` et que le programme trouve `<-- !#include file="sleepy.html" -->`, le serveur ne détecte pas l'erreur et peut se bloquer. (Si les fichiers sont référencés de manière non récursive au sein d'autres fichiers, ce problème n'apparaît pas.)

Configuration des inclusions côté serveur

Pour activer les inclusions côté serveur à partir des formulaires de configuration et d'administration, sélectionnez **Configuration du serveur -> Paramètres de base**. Ce formulaire permet d'indiquer si les types d'inclusion côté serveur suivants sont autorisés :

- Scripts CGI
- Fichiers
- Tous à l'exception des scripts CGI utilisant la commande **exec**
- Aucun

Ce formulaire permet également de sélectionner si les inclusions côté serveur doivent être effectuées pour des textes ou des documents HTML.

Vérifiez également que l'extension du fichier utilisé pour l'inclusion est reconnue. Dans les formulaires de configuration et d'administration, sélectionnez **Configuration du serveur → Types MIME et codage** et utilisez le formulaire **Types MIME**. Les extensions shtml et htmls sont reconnues par défaut.

Pour configurer votre serveur pour les inclusions côté serveur en modifiant les directives dans le fichier de configuration du proxy, voir les sections de référence des directives suivantes :

- «AddType — Spécifie le type de données des fichiers ayant une extension particulière», à la page 183
- «imbeds — Indique si le traitement côté serveur est utilisé», à la page 227

Format à utiliser pour les inclusions côté serveur

Les commandes d'inclusion doivent être incluses dans le document HTML ou le programme CGI en tant que commentaires. Les commandes s'affichent sous le format suivant :

```
<!--#balise directive=valeur ... -->
ou
<!--#balise directive="valeur" ... -->
```

Les guillemets placés autour des valeurs sont facultatifs. Toutefois, vous devez les indiquer si vous voulez insérer des espaces.

Directives pour les inclusions côté serveur

La présente section indique les directives acceptées par le système pour les inclusions côté serveur. (Ne confondez pas ces directives avec celles du fichier de configuration du serveur proxy, présentées dans l'Annexe B, «Directives du fichier de configuration», à la page 175.)

config—contrôle du traitement des fichiers

Utilisez cette directive pour contrôler certains aspects du traitement des fichiers. Les codes autorisés sont cmntmsg, errmsg, sizefmt et timefmt.

cmntmsg

Utilisez cette balise pour spécifier un message ajouté au début de commentaires ajoutés par d'autres directives. Un texte se trouvant entre une spécification de directive et les balise "-->" est traité comme du commentaire et est ajouté au fichier envoyé au client par le serveur.

Exemple :

```
<!--#config cmntmsg="[Commentaire]" -->
<!-- #echo var=" " texte supplémentaire -->
```

Résultat : <!--[Commentaire] texte supplémentaire -->

Par défaut : [les commentaires suivants étaient ajoutés dans la directive]

errmsg

Utilisez cette balise pour indiquer un message envoyé au client si une erreur survient au cours du traitement d'un fichier. Le message est consigné dans le journal des erreurs du serveur.

Exemple :

```
<!-- #config errmsg="[Une erreur s'est produite]" -->
```

Par défaut : "[Une erreur s'est produite lors du traitement de la directive]"

sizefmt

Utilisez cette balise pour indiquer le format d'affichage de la taille du fichier. Dans les exemples suivants, bytes est la valeur utilisée pour afficher le nombre d'octets, et abbrev est la valeur utilisée pour afficher le nombre de kilooctets ou de mégaoctets.

Exemple 1 :

```
<!--#config sizefmt=bytes -->
<!--#fsize file=foo.html -->
```

Résultat : 1024

Exemple 2 :

```
<!--#config sizefmt=abbrev -->
<!--#fsize file=foo.html -->
```

Résultat : 1K

Par défaut : "abbrev"

timefmt

Utilisez cette balise pour indiquer le format d'affichage des dates.

Exemple :

```
<!--#config timefmt="%D %T" -->
<!--#flastmod file=foo.html -->
```

Résultat : "10/18/95 12:05:33"

Par défaut : "%a, %d %b %Y %T %Z"

Les formats strftime() suivants sont acceptés avec le code timefmt :

Spécificateur	Signification
%%	Remplace la valeur par %
%a	Remplace la valeur par le nom du jour de la semaine (sous forme abrégée)
%A	Remplace la valeur par le nom complet du jour de la semaine
%b	Remplace la valeur par le nom du mois (sous forme abrégée)
%B	Remplace la valeur par le nom complet du mois
%c	Remplace la valeur par la date et l'heure
%C	Remplace la valeur par le siècle (année divisée par 100, sous forme tronquée)
%d	Remplace la valeur par le jour du mois (01-31)
%D	Insère la date sous la forme %m /%d /%y (mois, jour, année)
%e	Insère le mois de l'année sous la forme d'une valeur comprise entre 01 et 12. (Sous C POSIX uniquement, zone de deux caractères, justifiée à droite et vierge)
%E[cCxyY]	Si l'autre format date/heure n'est pas disponible, les descripteurs %E sont mappés à leurs équivalents non développés (par exemple, %EC est mappé à %C)

Spécificateur	Signification
%Ec	Remplace la valeur par l'autre représentation date et heure
%EC	Remplace la valeur par l'année de base (période) en utilisant l'autre représentation
%Ex	Remplace la valeur par l'autre représentation des dates
%EX	Remplace la valeur par l'autre représentation des heures
%Ey	Remplace la valeur par le décalage de %EC (année uniquement) en utilisant l'autre représentation
%EY	Remplace la valeur par l'année complète en utilisant l'autre représentation.
%h	Remplace la valeur par le nom du mois sous forme abrégée (identique à %b)
%H	Remplace la valeur par l'heure (horloge de 23 heures) sous la forme d'un nombre compris entre 00 et 23.
%I	Remplace la valeur par l'heure (horloge de 12 heures) sous la forme d'un nombre compris entre 00 et 12)
%j	Remplace la valeur par le jour de l'année (001-366)
%m	Remplace la valeur par le mois (01-12)
%M	Remplace la valeur par les minutes (00-59)
%n	Remplace la valeur par une nouvelle ligne
%O[deHlImMSUwWy]	Si l'autre format date/heure n'est pas disponible, les descripteurs %E sont mappés à leurs équivalents non développés (par exemple, %Od est mappé à %d)
%Od	Remplace la valeur par le jour du mois en utilisant les autres symboles numériques et en indiquant des zéros à gauche, s'il existe d'autres symboles pour zéro (sinon, des espaces apparaissent)
%Oe	Remplace la valeur par le jour du mois en utilisant les autres symboles numériques et en indiquant des espaces à gauche.
%OH	Remplace la valeur par l'heure (horloge de 24 heures) à l'aide des autres symboles numériques.
%OI	Remplace la valeur par l'heure (horloge de 12 heures) à l'aide des autres symboles numériques.
%Om	Remplace la valeur par le mois à l'aide des autres symboles numériques.
%OM	Remplace la valeur par les minutes en utilisant les autres symboles numériques
%OS	Remplace la valeur par des secondes en utilisant les autres symboles numériques
%OU	Remplace la valeur par le numéro de la semaine en utilisant les autres symboles numériques (le dimanche représente le premier jour de la semaine, avec des règles correspondant à %U)
%Ow	Remplace la valeur par le jour de la semaine (dimanche = 0) en utilisant les autres symboles numériques
%OW	Remplace la valeur par le numéro de la semaine en utilisant les autres symboles numériques (le lundi est le premier jour de la semaine)

Spécificateur	Signification
%Oy	Remplace la valeur par l'année (décalage de %C) en utilisant l'autre représentation et les autres symboles numériques.
%p	Remplace la valeur par l'équivalent local des abréviations AM ou PM
%r	Remplace la valeur par une chaîne équivalent à %I:%M:%S %p
%R	Remplace la valeur par l'heure en utilisant la notation de 24 heures(%H:%M)
%S	Remplace la valeur par des secondes (00-61)
%t	Remplace la valeur par une tabulation
%T	Remplace la valeur par une chaîne équivalent à %H:%M:%S
%u	Remplace la valeur par le jour de la semaine sous la forme d'un nombre (1-7 à 7), 1 représentant le lundi
%U	Remplace la valeur par le numéro de la semaine (00-53), le premier jour de la semaine étant le dimanche
%V	Remplace la valeur par le numéro de la semaine (01-53), le premier jour de la semaine étant le lundi
%w	Remplace la valeur par le jour de la semaine (0-6). Le dimanche correspond à 0
%W	Remplace la valeur par le numéro de la semaine (01-53), le premier jour de la semaine étant le lundi
%x	Remplace la valeur par la représentation de date appropriée
%X	Remplace la valeur par la représentation de l'heure appropriée
%y	Remplace la valeur par la représentation de l'année dans le siècle en 2 chiffres
%Y	Remplace la valeur par l'année complète en 4 chiffres
%Z	Remplace la valeur par le nom du fuseau horaire. Aucun caractère n'apparaît si le fuseau horaire est inconnu.

La configuration du système d'exploitation détermine si les mois et les années apparaissent sous forme abrégée ou complète.

echo — affiche les valeurs des variables

Utilisez cette directive pour afficher la valeur des variables d'environnement indiquées par la balise var. Si la variable est introuvable, la valeur (None) s'affiche. La commande **echo** peut également afficher une valeur définie par les directives **set** ou **global**. Les variables d'environnement suivantes peuvent s'afficher :

DATE_GMT

Date et heure en cours au format GMT (Greenwich Mean Time). Le formatage de cette variable est défini à l'aide de la directive **config timefmt**.

DATE_LOCAL

Date et heure locales en cours. Le formatage de cette variable est défini à l'aide de la directive **config timefmt**.

DOCUMENT_NAME

Nom du document supérieur. Si le document HTML a été généré par un script CGI, cette variable contient le nom du script CGI.

DOCUMENT_URI

Adresse URL complète demandée par le client, sans la chaîne de la demande.

LAST_MODIFIED

Date et heure de la dernière modification du document en cours. Le formatage de cette variable est défini à l'aide de la directive **config timefmt**.

QUERY_STRING_UNESCAPED

Demande de recherche envoyée par le client. Cette valeur n'est pas définie sauf si le document HTML a été généré par un script CGI.

SSI_DIR

Chemin d'accès au fichier en cours, par rapport à SSI_ROOT. Si le fichier en cours se trouve dans SSI_ROOT, cette valeur correspond à `"/"`.

SSI_FILE

Nom du fichier en cours.

SSI_INCLUDE

Valeur utilisée dans la commande d'inclusion qui a extrait le fichier en cours. Elle n'est pas définie pour le fichier initial.

SSI_PARENT

Nom et chemin du fichier contenant la commande d'inclusion qui a extrait le fichier en cours, par rapport à SSI_ROOT.

SSI_ROOT

Chemin d'accès au fichier initial. Toutes les demandes d'inclusion doivent se trouver dans ce répertoire ou dans l'un de ses enfants.

Exemple :

```
<!--#echo var=SSI_DIR -->
```

exec — définit les programmes CGI

Utilisez cette directive pour inclure les données générées en sortie par un programme CGI. La directive **exec** supprime les en-têtes HTTP générés en sortie par le programme CGI, *sauf* les suivants :

Content-type

Détermine si le corps du document en sortie doit être analysé pour d'autres inclusions

Content-encoding

Détermine si une traduction EBCDIC -> ASCII est requise

Last-modified

Remplace la valeur en cours de l'en-tête last-modified sauf si elle est postérieure à la valeur indiquée.

cgi — définit l'adresse URL d'un programme CGI

Utilisez cette directive pour indiquer l'URL d'un programme CGI.

Dans cet exemple, **program** correspond au programme CGI à exécuter ; **path_info** et **query_string** représentent un ou plusieurs paramètres transmis au programme en tant que variables d'environnement :

```
<!--#exec cgi="/cgi-bin/program/path_info?query_string" -->
```

Cet exemple illustre l'utilisation des variables :

```
<!--#exec cgi="&path;&cgiprogram;&pathinfo;&querystring;" -->
```

flastmod — affiche la date et l'heure de la dernière modification du document

Utilisez cette directive pour afficher la date et l'heure de la dernière modification du document. Le formatage de cette variable est défini par la directive **config timefmt**. Les balises **file** et **virtual** peuvent être utilisées avec cette directive. Leurs significations figurent ci-dessous.

Formats de la directive :

```
<!--#flastmod file="/chemin/fichier" -->
<!--#flastmod virtual="/chemin/fichier" -->
```

file Utilisez ce code pour indiquer le nom du fichier. Pour **flastmod**, **fsize** et **include**, on suppose que **file** se trouve dans le chemin **SSI_ROOT**, s'il est précédé du signe **'/'**. Sinon, il se trouve dans le chemin **SSI_DIR**. Le fichier doit exister dans **SSI_ROOT** ou dans l'un de ses descendants. Par exemple :

```
<!--#flastmod file="/chemin/fichier" -->
```

virtual

Utilisez ce code pour indiquer l'adresse URL d'un chemin d'accès virtuel à un document. Pour **flastmod**, **fsize** et **include**, le code **virtual** est toujours transmis via les directives de mappage du serveur. Par exemple :

```
<!--#flastmod virtual="/chemin/fichier" -->
```

Exemple :

```
<!--#flastmod file="foo.html" -->
```

Résultat : 12mai96

fsize — affiche la taille du fichier

Utilisez cette directive pour afficher la taille du fichier indiqué. Le formatage de cette variable est défini par la directive **config sizefmt**. Les balises **file** et **virtual** peuvent être utilisées avec cette directive. Leur signification est identique à celle définie précédemment pour la directive **flastmod**.

Exemple :

```
<!--#fsize file="/chemin/fichier" -->
<!--#fsize virtual="/chemin/fichier" -->
```

Résultat : 1K

global — définit les variables globales

Utilisez cette directive pour définir les variables globales qui peuvent être répercutées ultérieurement par ce fichier ou par d'autres fichiers inclus.

Exemple :

```
<!--#global var=VariableName value="SomeValue" -->
```

Par exemple, si vous voulez faire référence à un document parent au-delà de la frontière « virtual », vous devez définir une variable globale **DOCUMENT_URI**.

Vous devez également référencer la variable globale dans le document enfant. Cet exemple indique le code HTML à insérer dans le document parent.

```
<!--#global var="PARENT_URI" value=&DOCUMENT_URI; -->
```

Cet exemple indique le code HTML à insérer dans le document enfant.

```
<!--#flastmod virtual=&PARENT_URI; -->
```

include — inclut un document dans les données en sortie

Utilisez cette directive pour inclure le texte d'un document dans les données générées en sortie. Les balises **file** et **virtual** peuvent être utilisées avec cette directive. Leur signification est identique à celle qui a été définie ci-dessus pour la directive **flastmod**.

set — définit les variables à répercuter (écho)

Utilisez cette directive pour définir une variable qui pourra être répercutée ultérieurement, mais seulement dans ce fichier.

Exemple :

```
<!--#set var=valeur "Variable 2"="autre_valeur" -->
```

Lors de la définition de la directive, vous pouvez répercuter une chaîne située au milieu de valeur. Par exemple :

```
<!--#include file="&nom_fichier;" -->
```

Variables : Une directive définie côté serveur est généralement suivie d'une directive écho, de sorte qu'elle cherche la variable définie, répercute l'endroit où la variable est trouvée et poursuit l'exécution de la fonction. Elle peut contenir plusieurs références à des variables. La définition côté serveur permet également de répercuter une variable déjà définie. Si aucune variable définie n'est trouvée, aucune donnée ne s'affiche

Lorsqu'une définition côté serveur rencontre une référence de variable dans une directive d'inclusion côté serveur, elle tente de la résoudre du côté *serveur*. Dans l'exemple suivant, sur la deuxième ligne, la variable côté serveur `&index;`, est associée à la chaîne `var` pour générer le nom de la variable `var1`. On attribue ensuite une valeur à la variable `&var1`; en supprimant le `&` dans `ê` de sorte qu'elle n'est pas reconnue comme une variable. Elle est utilisée comme une chaîne pour générer la valeur `frê` ou *fred* avec accent circonflexe sur le "e". La variable `ê` est une variable côté client.

```
<!--#set var=valeur "index" ="1" -->
<!--#set var=valeur "var&index;"="fr&ecirc;d" -->
<!--#echo var="var1" -->
```

Les caractères qui peuvent être ignorés (appelés variables ignorées) sont précédés d'une barre oblique inversée (`\`) et comprennent :

Caractère	Signification
<code>\a</code>	Alerte (sonnerie)
<code>\b</code>	Retour arrière
<code>\f</code>	Nouveau formulaire (nouvelle page)
<code>\n</code>	Nouvelle ligne
<code>\r</code>	Retour chariot

Caractère	Signification
\t	Tabulation horizontale
\v	Tabulation verticale
\'	Apostrophe
\"	Guillemet
\?	Point d'interrogation
\\	Barre oblique inversée
\-	Tiret
\.	Point
\&	Perluète

Personnalisation des messages d'erreur

Vous pouvez personnaliser les messages d'erreur renvoyés par Caching Proxy et définir des messages spécifiques à utiliser dans des conditions d'erreur particulières. Dans les formulaires de configuration et d'administration, sélectionnez **Configuration du serveur** → **Personnalisation des messages d'erreur**. Ce formulaire permet de sélectionner une condition d'erreur et d'indiquer le fichier HTML associé.

Pour personnaliser des messages d'erreur en modifiant les directives dans le fichier de configuration du proxy, voir la section de référence de la directive «ErrorPage — Spécifie un message personnalisé pour une condition d'erreur particulière», à la page 214.

Réacheminement RTSP (Real Time Streaming Protocol)

S'applique aux configurations avec proxy inversé uniquement.

WebSphere Application Server, Version 6.1 intègre la prise en charge des données en continu au moyen de la fonction Redirector RTSP. RTSP permet ainsi à Caching Proxy d'agir comme le premier point de contact avec les lecteurs multimédia et de réacheminer les demandes qui leur sont adressées vers le serveur proxy ou le serveur de contenu capable de fournir le contenu demandé.

Le protocole RTSP (Real Time Streaming Protocol) est défini dans RFC 2326. Il s'agit d'un protocole Internet standard qui contrôle les flux de données. Bien qu'il n'ait pas la capacité technique de *distribuer* les flux de données, il est suffisamment flexible pour contrôler les flux de données non liés à la lecture de données audio et vidéo.

A propos du réacheminement RTSP

La fonction de réacheminement RTSP permet à Caching Proxy de réacheminer les requêtes concernant les sessions multimédia en continu contrôlées par RTSP. Les types de média concernés sont les suivants :

- Données audio enregistrées RealNetworks
- Données vidéo enregistrées RealNetworks
- Flux de données en direct RealNetworks (audio et vidéo)
- Fichiers Microsoft Media Player
- Fichiers multimédia Apple Quicktime

Tout lecteur capable de se connecter au port RTSP (numéro 554 en général) d'un serveur proxy peut utiliser cette structure dans Caching Proxy pour transmettre ses demandes à la fonction de réacheminement RTSP.

La fonction de réacheminement RTSP ne stocke pas en mémoire cache les présentations multimédia et ne les traite pas en tant que proxy. Pour remplir l'une de ces fonctions, ou les deux, la fonction de réacheminement RTSP doit être associée à un serveur tiers de mise en mémoire cache des données en continu. Caching Proxy, doté de la fonction de réacheminement RTSP, doit être connectée via le réseau à un ou plusieurs serveurs proxy RTSP.

Limites de la fonction RTSP

Cette fonction présente la limitation suivante :

Actuellement, seule la technologie RealNetworks est prise en charge. Cette technologie inclut le serveur proxy RealProxy, le serveur d'origine RealServer et le lecteur multimédia RealPlayer.

Amélioration de la fonction RTSP

Auparavant, toutes les demandes dirigées vers le même serveur d'origine et en quête de n'importe quelle URL étaient réacheminées de la même manière par la fonction RTSP. Il était impossible de procéder au réacheminement en fonction des noms de fichiers ou d'autres portions de l'URL demandée. Cette limitation ne s'applique plus. La fonction de réacheminement RTSP utilise désormais l'URL complète des demandes reçues ainsi que la valeur de seuil (`rtsp_proxy_threshold`) définie dans le fichier de configuration de Caching Proxy pour déterminer s'il faut réacheminer la demande du client vers le serveur d'origine ou vers un serveur proxy. Les demandes destinées au même serveur d'origine sont maintenant traitées individuellement.

Configuration du réacheminement RTSP

Les directives du fichier de configuration suivantes permettent de contrôler le réacheminement RTSP. Les paramètres de ces directives ne sont pas régénérés à la suite du redémarrage du serveur. Les modifications sont prises en compte uniquement après l'arrêt complet et le redémarrage du serveur.

- «RTSPEnable — Active le réacheminement RTSP», à la page 273
- «`rtsp_proxy_server` - Spécifie les serveurs de réacheminement», à la page 274
- «`rtsp_proxy_threshold` — Spécifie le nombre de demandes avant réacheminement vers une mémoire cache», à la page 274
- «`rtsp_url_list_size` — Spécifie le nombre d'URL en mémoire de proxy», à la page 274

Chapitre 14. Configuration des options d'en-tête

Lors d'une demande de documents, les clients Web envoient des en-têtes fournissant des informations complémentaires sur le navigateur ou la demande. Les en-têtes sont générés automatiquement lors de l'envoi d'une demande.

Caching Proxy offre plusieurs options permettant de personnaliser les informations d'en-tête afin de les masquer au serveur de destination. Le remplacement d'un en-tête réel par un en-tête générique renforce l'anonymat du client mais cette opération entraîne la désactivation des options de personnalisation des en-têtes pour certaines pages Web.

Les en-têtes utilisent ce formulaire :

```
User-Agent: Mozilla 2.02/OS2
Client-IP: 45.37.192.3
Referer: http://www.bigcompany.com/WebTrafficExpress/main.html
```

Cet en-tête comprend les zones suivantes :

- **User-Agent** : fournit des informations sur le navigateur et le système d'exploitation.
- **Client-IP** : indique l'adresse IP du client demandant l'adresse URL.
- **Referer** : indique le serveur de destination avec l'adresse URL du lien de référence à cette page.

Il existe des définitions de configuration du proxy qui permettent de bloquer la plupart des en-têtes. Toutefois, certaines zones d'en-tête sont requises par les serveurs d'origine. Si vous les bloquez, il est possible que les pages Web ne s'affichent pas correctement. (Par exemple, dans certains cas, le fait de bloquer la zone d'en-tête "host" peut afficher une autre page Web que celle demandée par les utilisateurs.) Pour plus d'informations sur les zones d'en-tête, consultez les spécifications de HTTP version 1.1.

Directives associées

Pour redéfinir les options d'en-tête en modifiant le fichier de configuration du proxy, voir les sections de référence des directives suivantes :

- «NoCacheOnRange — Indique la non mise en cache pour les demandes Range», à la page 246
- «NoProxyHeader — Indique les en-têtes de client à bloquer», à la page 247
- «ProxyFrom — Spécifie un client avec un en-tête "From:"», à la page 266
- «ProxyIgnoreNoCache — Ignore les demandes de rechargement», à la page 266
- «ProxySendClientAddress — Génère l'en-tête "Client IP Address:"», à la page 267
- «ProxyUserAgent — Modifie la chaîne de l'agent utilisateur», à la page 267
- «ProxyVia — Spécifie le format de l'en-tête HTTP», à la page 267

Pour plus d'informations, voir Chapitre 4, «Modification manuelle du fichier ibmproxy.conf», à la page 13.

Formulaires de configuration et d'administration

Vous pouvez utiliser deux formulaires de configuration et d'administration pour indiquer les options d'en-tête :

- Sélectionnez **Configuration du proxy** -> **Paramètres de confidentialité**. Dans le formulaire **Paramètres de confidentialité**, définissez les options suivantes :
 - **Transmettre l'adresse IP du client au serveur de destination**
Cochez cette case si vous voulez que l'adresse IP du client qui envoie la demande soit acheminée vers le serveur de destination (de contenu). Si vous ne cochez pas cette case, le serveur de destination reçoit l'adresse IP du serveur proxy. Si vous ne cochez pas cette case, l'anonymat du client est renforcé lorsque vous naviguez sur le Web.
 - **Chaîne agent utilisateur**
Entrez la chaîne d'en-tête à envoyer au serveur de destination pour remplacer le type de navigateur et de système d'exploitation utilisé par un client. Par exemple : si vous indiquez Caching Proxy 4.0, celui-ci remplace Mozilla 2.02/OS2 dans l'en-tête suivant :

```
Content-Type:MIME  
User-Agent: Mozilla 2.02/OS2  
Referer: http://www.ics.raleigh.ibm.com/WebTrafficExpress/main.html  
Pragma:no-cache
```
 - **Provenance :**
Entrez l'adresse électronique que lit le serveur de destination lorsqu'il analyse l'en-tête "From :". Vous pouvez indiquer l'adresse électronique de l'administrateur du proxy, car les rapports d'incidents sont généralement destinés à l'administrateur.
 - Cliquez sur **Validation** pour modifier le fichier de configuration.
- Sélectionnez **Configuration du proxy** -> **Filtrage d'en-tête de proxy**. Utilisez ce formulaire pour répertorier les en-têtes HTTP à bloquer :
 1. Cliquez sur **Ajouter** ou **Supprimer** et indiquez une position d'indice pour l'en-tête bloqué.
 2. Entrez l'en-tête HTTP du client à bloquer. (Pour connaître la liste complète des en-têtes et obtenir les explications associées, voir les spécifications du programme HTTP 1.1.)
 3. Cliquez sur **Validation** pour modifier le fichier de configuration.

Pour plus d'informations, voir Chapitre 2, «Utilisation des formulaires de configuration et d'administration», à la page 7.

Chapitre 15. A propos de l'interface de programmation d'application

L'interface de programmation d'application (API pour application programming interface) est étudiée en détail dans *Programming Guide for Edge Components*. Les directives API du fichier de configuration activent les routines de plug-ins appelées lors d'opérations spécifiques du traitement des demandes. Ces routines de plug-ins peuvent remplacer ou s'exécuter en plus de routines prédéfinies.

Directives associées

Les directives ci-dessous sont des directives API :

- «Authentication — Personnalise l'étape d'authentification», à la page 187
- «Authorization — Personnalise l'étape d'autorisation», à la page 188
- «Error — Personnalise l'étape d'erreur», à la page 213
- «Log — Personnalise l'étape de personnalisation», à la page 234
- «Midnight — Identifie le plug-in API permettant d'archiver les fichiers journaux», à la page 243
- «NameTrans — Personnalise l'étape de conversion de nom», à la page 244
- «ObjectType — Personnalise l'étape de type d'objet», à la page 248
- «PostAuth — Personnalise l'étape PostAuth», à la page 254
- «PostExit — Personnalise l'étape PostExit», à la page 255
- «PreExit — Personnalise l'étape PreExit», à la page 255
- «ServerInit — Personnalise l'étape d'initialisation du serveur», à la page 277
- «ServerTerm — Personnalise l'étape d'arrêt du serveur», à la page 278
- «Service — Personnalise l'étape Service», à la page 279
- «Transmogrifier — Personnalise l'étape de manipulation des données», à la page 287
- «TransmogrifiedWarning — Envoie un message d'avertissement au client», à la page 288

Pour plus d'informations, voir Chapitre 4, «Modification manuelle du fichier ibmproxy.conf», à la page 13.

Formulaires de configuration et d'administration

Le formulaire de configuration et d'administration suivant modifie les valeurs des directives associées :

- **Configuration du serveur -> Traitement des demandes -> Traitement des demandes API**

Pour plus d'informations, voir Chapitre 2, «Utilisation des formulaires de configuration et d'administration», à la page 7.

Partie 4. Configuration de fonction de mise en cache du serveur proxy

Cette section traite de la mémoire cache du proxy et de la façon de la configurer. La mémoire cache peut être configurée pour stocker les fichiers en mémoire (cache mémoire) ou sur une ou plusieurs unités de stockage (cache disque). Il est possible de configurer un agent de régénération de la mémoire cache pour charger préalablement les fichiers les plus demandés dans la cache. Plusieurs filtres d'URL peuvent être appliqués à la mise en mémoire cache. Cette section traite également du partage de cache qui passe par l'utilisation de l'accès du cache à distance ou du plug-in ICP (Internet caching protocol), par la suppression des fichiers obsolètes avec le nettoyage de la mémoire cache (garbage collection) et par la mise en cache de fichiers générés en dynamique.

Cette partie comporte les chapitres suivants :

- Chapitre 16, «Présentation de la mise en cache sur le serveur proxy», à la page 73
- Chapitre 17, «Configuration de la mise en mémoire cache de base», à la page 77
- Chapitre 18, «Contrôle du contenu de la mémoire cache», à la page 81
- Chapitre 19, «Maintenance des données de la mémoire cache», à la page 85
- Chapitre 20, «Configuration de l'agent de la mémoire cache pour la régénération et le préchargement automatiques», à la page 91
- Chapitre 21, «Utilisation d'une mémoire cache partagée», à la page 99
- Chapitre 22, «Stockage en mémoire cache d'un contenu généré dynamiquement», à la page 103
- Chapitre 23, «Personnalisation de la mémoire cache du serveur proxy», à la page 107

Chapitre 16. Présentation de la mise en cache sur le serveur proxy

La mise en mémoire cache consiste, pour le serveur proxy, à sauvegarder des copies locales des fichiers demandés par les clients afin de les récupérer rapidement dans la mémoire cache lors d'une nouvelle demande.

Caching Proxy est compatible avec le protocole HTTP 1.1, qu'il utilise pour mettre des données en mémoire cache et déterminer si les documents sont à jour.

Ce chapitre présente un certain nombre de fonctions de la mémoire cache du serveur proxy. Les procédures de valeurs adéquates pour ces fonctions seront décrites ultérieurement.

Stockage de la mémoire cache

Le serveur proxy peut stocker la mémoire cache sur une unité physique ou dans la mémoire système. Le type de mémoire cache le mieux adapté à vos besoins dépend des capacités de votre équipement et des performances souhaitées (rapidité ou taille de la mémoire cache). Un cache mémoire est plus rapide qu'un cache disque mais la taille de la mémoire cache est limitée par la quantité de mémoire vive installée sur le serveur proxy. La taille d'un cache disque est limitée par la taille de l'unité de stockage, qui est généralement supérieure à celle de la mémoire vive.

En cas d'utilisation d'un cache disque, Caching Proxy effectue la mise en cache sur un disque de données brutes, ce qui signifie que le serveur proxy écrit directement sur le périphérique indépendamment des protocoles de lecture et d'écriture du système d'exploitation. L'unité de stockage sur laquelle réside un cache disque doit être préparée à l'aide de la commande **htcformat**. Pour plus d'informations sur la commande **htcformat**, voir Chapitre 17, «Configuration de la mise en mémoire cache de base», à la page 77.

Index de la mémoire cache

Qu'il s'agisse d'une mémoire cache ou d'un cache disque, Caching Proxy utilise également de l'espace mémoire système pour stocker l'index de la mémoire cache, ce qui réduit la durée de la recherche de fichiers en mémoire cache.

La structure de répertoires de la mémoire cache de Caching Proxy et les méthodes de recherche employées diffèrent de celles des autres serveurs proxy. Caching Proxy gère dans la mémoire un index contenant des informations sur les fichiers mis en mémoire cache. Les recherches effectuées dans la mémoire vive permettent de localiser et d'extraire les fichiers plus rapidement que celles effectuées sur un disque ou sur tout autre support.

L'index comprend des informations sur les URL, les emplacements en mémoire cache et l'expiration des objets mis en mémoire cache. C'est pour cela que la quantité de mémoire nécessaire à l'index est proportionnelle au nombre d'objets mis en mémoire cache.

Lorsqu'il reçoit une demande d'un client, le proxy recherche l'URL demandée dans l'index de la mémoire cache.

- Si le fichier ne se trouve pas dans l'index, la demande est adressée au serveur de destination.
 - L'URL extraite est examinée pour déterminer si le fichier peut être mis en mémoire cache. Si l'opération est autorisée, le serveur proxy place en mémoire cache le fichier récupéré.
 - L'index de la mémoire cache est ensuite mis à jour avec les informations concernant l'URL, l'emplacement et l'expiration du nouvel objet mis en mémoire cache.
- Si le fichier se trouve dans l'index :
 - Les informations d'expiration sont examinées pour déterminer si le fichier en mémoire cache est valide.
 - Si l'objet a expiré, le serveur de destination est contacté et l'objet est remplacé par le nouveau document extrait. Les informations relatives à l'expiration sont mises à jour dans l'index de la mémoire cache.
 - Si l'objet n'a pas expiré, le document est extrait de la mémoire cache du proxy.

Mise en cache FTP

Lorsque le proxy est configuré pour mettre les demandes en mémoire cache, il peut placer en mémoire cache les demandes de fichiers FTP et HTTP. Toutefois, comme les en-têtes des fichiers FTP ne contiennent pas le même type d'information que les fichiers HTTP, le calcul des dates d'expiration des fichiers FTP est différent de celui des autres fichiers.

Lorsqu'une demande d'extraction de fichier est transmise au serveur FTP, le proxy adresse d'abord une demande LIST au serveur FTP afin d'obtenir des informations sur les répertoires FTP associés. Si le serveur FTP adresse une réponse positive à la demande LIST et indique les informations de répertoire demandées, le proxy crée un en-tête HTTP Last-Modified daté et analysé à partir des informations du répertoire FTP. La fonction de mise en mémoire cache du proxy utilise ensuite l'en-tête Last-Modified, associé au jeu de valeurs de la directive CacheLastModifiedFactor dans le fichier de configuration, afin de déterminer la durée de stockage du fichier FTP.

Pour plus d'informations sur les modalités d'utilisation de l'en-tête Last Modified et de la directive CacheLastModifiedFactor lors de la définition de la durée de stockage d'un fichier en mémoire cache, voir Chapitre 19, «Maintenance des données de la mémoire cache», à la page 85.

Les fichiers FTP extraits à l'aide d'un ID utilisateur spécifique (sans l'établissement d'une connexion anonyme) sont considérés comme des fichiers privés ; ils ne sont pas conservés en mémoire cache.

Mise en cache DNS

Outre la mise en mémoire cache du contenu Web, le serveur proxy effectue une mise en mémoire cache DNS en utilisant le serveur de noms de domaine. Par exemple, quand un client demande une adresse URL à partir de `www.myWebsite.com`, le proxy demande à son serveur DNS de convertir le nom d'hôte `www.myWebsite.com` en adresse IP. L'adresse IP est ensuite mise en

mémoire cache pour améliorer les temps de réponse lors des demandes ultérieures concernant ce nom hôte. La mise en mémoire cache DNS est automatique et ne peut pas être reconfigurée.

Exclusions de la mémoire cache

Certains fichiers et documents ne sont jamais mis en mémoire cache. Tel est le cas des fichiers suivants :

- Les fichiers renvoyés lors des demandes faisant appel à des méthodes HTTP autres que GET, telles que POST et PUT
- Tous les documents pour lesquels une authentification est nécessaire, sauf si la mise en mémoire cache de ces documents est spécifiquement demandée par le serveur d'origine.
- La sortie dynamique des scripts CGI (celle-ci étant unique lors de chaque demande). Les résultats générés en dynamique par des servlets et des JSP (JavaServer Pages) exécutés par IBM WebSphere Application Server peuvent être mis en cache à condition que la fonction de mise en cache dynamique soit activée. Pour plus de détails, voir Chapitre 22, «Stockage en mémoire cache d'un contenu généré dynamiquement», à la page 103.
- Les informations transmises via une connexion tunneling SSL (le proxy étant incapable de déchiffrer les données transmises par son intermédiaire).
- Tout fichier renvoyé par une adresse URL contenant un point d'interrogation (?), sauf si la mise en mémoire cache de la requête est expressément autorisée. (Pour plus d'informations sur la configuration de la mise en mémoire cache des résultats des requêtes, voir Chapitre 18, «Contrôle du contenu de la mémoire cache», à la page 81.)

La définition de filtres de mémoire cache permet de limiter davantage le nombre et la nature des données mises en cache. Par exemple, vous pouvez empêcher le serveur proxy de placer en mémoire cache les fichiers locaux. Pour plus de détails, voir Chapitre 18, «Contrôle du contenu de la mémoire cache», à la page 81.

Gestion de la mémoire cache

La gestion d'une mémoire cache englobe un grand nombre de facteurs. En tant qu'administrateur du serveur, vous pouvez spécifier :

- La nature des documents mis en cache (voir Chapitre 18, «Contrôle du contenu de la mémoire cache», à la page 81).
- Le nombre de documents pouvant être mis en mémoire cache (voir Chapitre 17, «Configuration de la mise en mémoire cache de base», à la page 77).
- La durée de validité des documents en mémoire cache (voir Chapitre 19, «Maintenance des données de la mémoire cache», à la page 85).
- La fréquence de nettoyage du cache et le type des fichiers à ne pas supprimer (voir Chapitre 19, «Maintenance des données de la mémoire cache», à la page 85).
- Les modalités d'indexation des documents en mémoire cache sont indexés (voir Chapitre 17, «Configuration de la mise en mémoire cache de base», à la page 77).
- Le moment où la mémoire cache est mise à jour (voir Chapitre 20, «Configuration de l'agent de la mémoire cache pour la régénération et le préchargement automatiques», à la page 91).
- Les accès à la mémoire cache (voir Chapitre 21, «Utilisation d'une mémoire cache partagée», à la page 99).

- Les modalités de stockage et d'archivage des journaux (voir Chapitre 17, «Configuration de la mise en mémoire cache de base», à la page 77).

Par ailleurs, il est possible d'apporter certaines modifications à la configuration de la mémoire cache afin d'améliorer les performances générales de Caching Proxy. Pour plus de détails, voir Chapitre 23, «Personnalisation de la mémoire cache du serveur proxy», à la page 107.

Chapitre 17. Configuration de la mise en mémoire cache de base

Si vous avez utilisé les paramètres par défaut du programme d'installation du logiciel composants Edge pour installer Caching Proxy, ce dernier est activé et les données sont mises en mémoire. Vous pouvez choisir de régler les paramètres de base ci-dessous pour répondre aux besoins de votre système.

Si vous n'avez pas utilisé le programme d'installation, configurez ces paramètres pour activer la mise en mémoire cache.

Les opérations ci-dessous constituent la procédure de configuration de base de la mise en mémoire cache :

1. Activation de la mise en mémoire cache
2. Configuration de l'espace mémoire cache

Vous pouvez ensuite choisir d'ajouter ou de modifier des paramètres pour les fonctions suivantes.

- Personnalisation de la mémoire cache.
- Sauvegarde ou chargement de la mémoire cache sur le disque.
- Définition des conditions de mise en cache à l'aide de filtres d'URL
- Ouverture de la mémoire cache aux résultats de requêtes et aux fichiers générés en dynamique
- Configuration du délai d'expiration des fichiers en mémoire cache et de la récupération de place
- Configuration de la régénération et du préchargement automatiques de la mémoire cache
- Configuration du partage de la mémoire à l'aide de RCA (Remote Cache Access) ou du protocole ICP (Internet caching protocol)
- Configuration de la journalisation

Ce chapitre fournit ou renvoie à des instructions de modification de ces paramètres.

1. Activation de la mémoire cache

Pour activer la mémoire cache, réglez la directive Caching sur on ou cochez la case **Activer la mise en cache du proxy** dans le formulaire de configuration **Configuration de la mémoire cache -> Paramètres de la mémoire cache**. Si vous ne spécifiez pas d'unité de cache, la mémoire cache est stockée en mémoire vive. Pour créer un cache disque, suivez la procédure décrite à la section «2. Configuration de l'espace de mémoire cache».

2. Configuration de l'espace de mémoire cache

Les opérations de configuration de la mémoire cache varient selon que vous utilisez la mémoire vive ou un cache disque.

Personnalisez le paramètre Mémoire cache de manière à ce que la taille de la mémoire soit suffisante. Pour obtenir des recommandations concernant la taille de la mémoire cache, voir «Définition de la mémoire cache», à la page 79.

Pour utiliser un cache disque, vous devez effectuer les opérations suivantes :

1. Préparez l'unité de stockage devant contenir la mémoire cache.

La mémoire cache requiert une unité spécialement formatée à cette fin. Il est recommandé de réserver une unité ou une partition de disque entière à cet usage. La taille minimale de la mémoire cache est de 16392 ko.

Pour formater l'unité de stockage, procédez comme suit :

- a. Choisissez une unité pour le stockage des données en mémoire cache. Assurez-vous qu'aucun autre programme n'utilise cet espace de stockage et que l'unité est accessible en mode brut (formatage par caractère).
- b. Formatez l'unité à l'aide de la commande **htcformat**. La syntaxe est la suivante :

```
htcformat  
chemin_unité_brute [-blocksize taille_bloc] [-blocks nombre_de_blocs]
```

Les arguments `-blocksize` et `-blocks` sont facultatifs. La taille de bloc par défaut est de 8192 octets. Si le nombre de blocs n'est pas indiqué, la partition du disque comportera autant de blocs qu'elle peut en contenir.

Lorsque vous indiquez le chemin de l'unité, indiquez celui de l'unité en mode brut.

- Sur les plateformes AIX, le chemin de l'unité en mode brut pour un volume logique défini en tant que `/dev/lv02` est `/dev/rlv02`.
- Sous Linux, vous devez exécuter la commande **raw** avant la commande **htcformat** pour associer le chemin d'accès de l'unité en mode brut à l'unité SCSI réelle `sdb1`.

```
raw /dev/raw/raw1 dev/sdb1
```
- Sur les plateformes HP-UX et Solaris, le chemin de l'unité en mode brut pour une partition définie en tant que `/dev/dsk/c0t0d0s0` est `/dev/rdisk/c0t0d0s0`.
- Sur les plateformes Windows, le chemin d'une unité en mode brut définie en tant que `e:` est `\\.\e:`.

Pour plus d'informations sur l'accès aux nouvelles unités, voir les documents de référence disponibles pour votre système de fichiers.

2. Indiquez l'unité de stockage de la mémoire cache en utilisant la directive `CacheDev` ou le formulaire de configuration **Paramètres de la mémoire cache**. Vous pouvez spécifier plusieurs unités.

ATTENTION :

Sur les systèmes Windows, la commande **htcformat** ne rend pas automatiquement la mémoire cache non inscriptible.

Si le système d'exploitation tente d'écrire des données sur cette unité, les données en mémoire cache risquent d'être perdues. Pour éviter cette situation, faites appel à l'utilitaire Windows Disk Manager pour préparer le disque avant d'utiliser la commande **htcformat**. Pour préparer le disque, exécutez l'utilitaire de disque pour supprimer l'unité ou la partition choisie et la recréer ensuite sans la formater. Cette unité ne sera plus considérée comme disponible par le système à des fins de stockage.

Personnalisations optionnelles

Définition de la mémoire cache

Définissez la valeur dans la directive `CacheMemory` ou dans la zone **Mémoire cache** du formulaire de configuration **Paramètres de la mémoire cache** conformément aux principes ci-après. La quantité de mémoire définie dans cette valeur est utilisée pour la prise en charge de l'infrastructure de la mémoire cache, y compris l'index de la mémoire cache et, si la mise en mémoire cache est configurée, pour le stockage du contenu de la mémoire cache.

Valeurs minimales

Pour optimiser les performances des mémoires cache sur disque, un minimum de 64 Mo de mémoire cache est recommandé pour la prise en charge de l'infrastructure de mise en cache, y compris l'index de la mémoire cache. L'index de la mémoire cache augmente à mesure que la taille de la mémoire cache augmente, de sorte que l'espace mémoire nécessaire pour stocker l'index s'accroît également. Une mémoire cache de 64 Mo suffit pour prendre en charge l'infrastructure de mise en cache et pour stocker un index de mémoire cache pour une mémoire cache sur disque d'environ 6,4 Go. Les mémoires cache sur disque plus volumineuses doivent avoir une fois et demie la taille de la mémoire cache.

La valeur des mémoires cache correspond à la quantité de mémoire réservée pour la prise en charge de l'infrastructure de mise en cache et la mémoire cache elle-même. Un minimum de 64 Mo de mémoire cache est recommandé.

Valeur maximale

Si vous allouez trop de mémoire physique à une mémoire cache, des opérations non souhaitées telles que des erreurs "mémoire insuffisante" ou des échecs du serveur proxy peuvent se produire. Les limites des valeurs possibles pour la mémoire cache proviennent des limites des applications 32 bits. Caching Proxy étant une application 32 bits, elle peut utiliser jusqu'à 2 Go de mémoire.

Caching Proxy alloue la mémoire définie par la directive `CacheMemory` et l'utilise comme mémoire cache pour stocker les objets. Vous devez allouer de la mémoire supplémentaire, qu'il s'agisse de mémoire cache ou d'un disque en mode brut, aux structures de données de la mémoire cache, des mémoires tampon des connexions et des E/S réseau, des mémoires tampon de session et de la mémoire pour le processus principal et toutes autres unités d'exécution. De plus, il est possible que les demandes de certains clients aient à allouer un bloc pool de mémoire plus important que la valeur par défaut. Par conséquent, si la valeur de la directive `CacheMemory` est trop proche de 2 Go, il est possible que Caching Proxy n'ait pas assez de mémoire pour fonctionner et tout particulièrement si la charge de demandes est élevée.

Il est recommandé de choisir pour la directive `CacheMemory` une valeur inférieure ou égale à 1600 Mo. Une valeur supérieure à 1600 Mo interfère avec la mémoire dont Caching Proxy a besoin pour fonctionner correctement et peut avoir des effets secondaires. Ces effets secondaires peuvent se traduire par une utilisation plus importante du processeur (jusqu'à 100% de l'utilisation), des erreurs de mémoire insuffisante et des performances médiocres. Si une taille de mémoire cache plus importante est requise, utilisez des unités de mémoire cache ou implémentez une configuration de mémoire cache partagée avec RCA ou ICP.

Sauvegarde ou chargement de la mémoire cache sur le disque

Vous pouvez importer et exporter le contenu de la mémoire cache vers ou à partir d'un fichier de vidage. Cette opération est utile lorsque la mémoire cache est perdue lors du redémarrage ou lors du déploiement de la même mémoire cache sur plusieurs proxys.

Définition de filtres de mise en mémoire cache

Les filtres permettent de limiter le stockage en mémoire cache à certaines données sous la forme d'une demande d'URL. Pour plus de détails, voir Chapitre 18, «Contrôle du contenu de la mémoire cache», à la page 81.

Configuration de la mise en mémoire cache pour les résultats de requête et les fichiers générés en dynamique

Le cas échéant, le serveur proxy peut être configuré pour mettre en cache des résultats de requêtes. Par défaut, les URL contenant un point d'interrogation (?) ne sont jamais mises en mémoire cache. Pour plus de détails, voir «Mise en cache de réponses de requêtes», à la page 82.

Une autre option consiste à placer en mémoire cache les résultats de servlets ou de JSP exécutés sur une machine IBM WebSphere Application Server. Pour plus de détails, voir Chapitre 22, «Stockage en mémoire cache d'un contenu généré dynamiquement», à la page 103.

Configuration du délai d'expiration des fichiers en mémoire cache et de la récupération de place

Pour plus d'informations sur l'expiration des fichiers et la suppression de fichiers périmés, voir Chapitre 19, «Maintenance des données de la mémoire cache», à la page 85.

Configuration du préchargement automatique

Il est possible de configurer la mémoire cache de sorte que les fichiers qu'elle contient soient mis à jour quotidiennement. Pour plus d'informations, voir Chapitre 20, «Configuration de l'agent de la mémoire cache pour la régénération et le préchargement automatiques», à la page 91.

Configuration du partage de la mémoire cache

Dans certains cas, l'utilisation d'une mémoire cache partagée augmente les chances d'y trouver un fichier demandé. Pour plus d'informations, voir Chapitre 21, «Utilisation d'une mémoire cache partagée», à la page 99.

Configuration de la journalisation

La maintenance de journaux précis et concis est essentielle à la gestion de Caching Proxy. La Partie 6, «Contrôle de Caching Proxy», à la page 147 contient des informations sur la configuration et l'utilisation de journaux du serveur proxy.

Chapitre 18. Contrôle du contenu de la mémoire cache

Caching Proxy offre plusieurs méthodes de filtrage permettant de contrôler quels fichiers, documents et autres objets sont placés en mémoire cache. Les méthodes de filtrage sont les suivantes :

- Filtrage de mémoire cache par URL
- Mise en cache des réponses de requêtes
- Mise en cache de fichiers locaux
- Mise en cache par URL partielle
- Mise en cache de fichiers en fonction d'une partie de l'URL de demande
- Mise en cache de fichiers générés en dynamique — voir Chapitre 22, «Stockage en mémoire cache d'un contenu généré dynamiquement», à la page 103

Remarque : Le formulaire de configuration et d'administration **Configuration de la mémoire cache** → **Comportement de la mémoire cache** contient également une option intitulée **Mémoire cache basée sur l'URL entrante**. (La directive du fichier de configuration correspondant s'appelle `CacheByIncomingURL`.) Cette directive fait référence au nom de fichier du fichier mis en cache. Cochez cette case pour que le nom de ce fichier soit basé sur l'URL entrante ; si cette case n'est pas cochée, le nom du fichier est basé sur l'URL sortante.

Configuration des filtres de mise en mémoire cache d'URL

Le serveur proxy peut être configuré pour comparer des demandes avec un modèle d'URL et déterminer de cette manière si un fichier est placé en mémoire cache. Pour cela, définissez des modèles pour des demandes dont les fichiers seront *toujours* placés en cache et des modèles distincts pour des demandes dont les fichiers ne seront *jamais* placés en cache. Il est possible d'utiliser plusieurs modèles.

Un système similaire permet d'activer la mise en cache des réponses de requêtes. Pour plus d'informations, voir «Mise en cache de réponses de requêtes», à la page 82.

Pour définir des filtres de mise en cache d'URL en éditant le fichier `ibmproxy.conf`, voir «CacheOnly — Met en mémoire cache uniquement les fichiers dont les URL correspondent à un modèle», à la page 197 et «NoCaching — Ne met pas en mémoire cache les fichiers dont l'URL correspond à un modèle», à la page 245.

Pour définir des filtres de mise en cache d'URL dans les formulaires de configuration et d'administration, utilisez la zone **Configuration de la mémoire cache** → **Comportement de la mémoire cache** : **Filtrage de la mémoire cache par URL**. Utilisez cette section pour indiquer les URL pour lesquelles les fichiers sont toujours mis en mémoire cache et celles pour lesquelles les fichiers ne le sont jamais. Pour indiquer deux listes, l'une contenant les fichiers à mettre en mémoire cache et l'autre les fichiers à ne pas mettre en mémoire cache, créez une liste puis cliquez sur le bouton **Validation** avant de créer l'autre liste.

Mise en cache de réponses de requêtes

Les réponses de requêtes (demandes d'URL contenant un point d'interrogation) peuvent être mises en mémoire cache à l'aide de filtres de mise en mémoire cache. Cette fonctionnalité est particulièrement utile dans le cas de proxys inversés (substituts) si de nombreux clients envoient la même requête.

La mise en mémoire cache des requêtes peut être ajustée en éditant directement la directive `CacheQueries` du fichier de configuration `ibmproxy.conf`. Les options ci-après peuvent être utilisées avec la directive `CacheQueries`.

- **Toujours** — Toutes les réponses aux requêtes des hôtes correspondant au modèle seront placées en mémoire cache, si cela est possible selon les normes HTTP 1.1.
- **Public** — Les réponses aux requêtes des hôtes correspondant au modèle seront placées en mémoire cache si elles contiennent l'en-tête "Cache-control: public" ou un en-tête de revalidation forcée et si elles peuvent être placées en mémoire cache selon les normes HTTP 1.1.

Vous trouverez plus d'informations sur ces options dans la section «`CacheQueries` — Met en mémoire cache les réponses aux URL contenant le caractère ?», à la page 197

Pour configurer la mise en cache des réponses de requêtes, dans les formulaires de configuration et d'administration, utilisez la zone **Configuration de la mémoire cache** → **Comportement de la mémoire cache : Filtrage des réponses aux demandes de la mémoire cache par URL**. Pour indiquer deux listes, créez une liste puis cliquez sur le bouton **Validation** avant de créer l'autre liste.

Conditions supplémentaires pour la mise en mémoire cache des réponses de requêtes

Vous devez configurer le paramètre de mise en mémoire cache des requêtes et vérifier que les paramètres ci-après sont correctement configurés pour que les réponses aux requêtes puissent être placées en mémoire cache. Pour plus d'informations sur le paramétrage de ces options à l'aide des formulaires de configuration et d'administration, voir «Configuration de la validité de la mémoire cache», à la page 88.

- **CacheTimeMargin** — Cette directive spécifie un délai d'expiration minimum ; les fichiers dont les délais d'expiration sont inférieurs à celui indiqué dans ce paramètre ne sont pas mis en mémoire cache. Les délais d'expiration de certaines réponses pouvant être très courts, le choix d'une valeur plus faible dans cette directive permet de placer davantage de réponses en mémoire cache. Voir «`CacheTimeMargin` — Indique la durée minimale de mise en mémoire cache d'un fichier», à la page 199 ou utilisez le formulaire **Paramètres d'expiration de la mémoire cache**, décrit à la section «Configuration de la validité de la mémoire cache», à la page 88.
- **CacheDefaultExpiry** — Cette directive indique le délai d'expiration des fichiers n'ayant pas de date d'expiration explicite ou de date de dernière mise à jour à partir de laquelle le délai d'expiration pourrait être calculé. Si vous choisissez une valeur supérieure à la valeur par défaut (0) pour le paramètre des demandes HTTP, un nombre plus important de réponses pourra être mis en mémoire cache. Cependant, si ce paramètre est modifié de la sorte, il se peut que le contenu de la mémoire cache soit périmé. Voir «`CacheDefaultExpiry` — Indique l'heure d'expiration par défaut des fichiers», à la page 191 ou utilisez le formulaire **Paramètres d'expiration de la mémoire cache**, décrit à la section «Configuration de la validité de la mémoire cache», à la page 88.

- **CacheLastModifiedFactor** — Cette directive est utilisée pour calculer la date d'expiration des fichiers ayant une date de dernière modification, mais aucune date d'expiration explicite. L'affectation d'une valeur plus élevée au facteur des fichiers HTTP augmente la durée pendant laquelle un fichier HTTP reste dans la mémoire cache sans être revalidé. Si ce paramètre est modifié de la sorte, il se peut que le contenu de la mémoire cache soit périmé. Voir «CacheLastModifiedFactor — Spécifie la valeur permettant de déterminer les dates d'expiration», à la page 193 ou utilisez le formulaire **Dernier facteur modifié**, décrit à la section «Configuration de la validité de la mémoire cache», à la page 88.
- Vous pouvez éventuellement définir les directives **SignificantUrlTerminator** et **AggressiveCaching**. Voir «SignificantURLTerminator — Spécifie un code d'arrêt pour les demandes d'URL», à la page 280 et «AggressiveCaching — Spécifie la mise en mémoire en cache des fichiers ne pouvant pas être mis en mémoire cache», à la page 186.

Mise en cache de fichiers locaux

Du fait que la mise en cache de fichiers fournis par le serveur proxy ne présente guère d'intérêt, les fichiers résidant dans le domaine local du serveur ne sont pas par défaut placés en mémoire cache. Pour mettre en mémoire cache des objets originaires du domaine local du serveur, cochez la case **Fichiers de domaine local de mémoire cache** dans le formulaire de configuration et d'administration **Configuration de la mémoire cache** → **Comportement de la mémoire cache**. Vous pouvez également choisir d'utiliser la directive **CacheLocalDomain** du fichier de configuration du proxy que, dans ce cas, vous définirez sur on.

Stockage des fichiers en mémoire cache par URL partielle

Vous pouvez désormais placer des objets en mémoire cache en fonction d'une seule partie (significative) de l'URL entrante, et non de l'URL complète. Cette fonction est utile pour les services Web avec modèles de transactions ou pour la mise en mémoire cache dynamique, dans la mesure où la même réponse est souvent envoyée à différentes demandes entrantes lorsque des éléments significatifs de leurs URL sont identiques.

Vous ne pouvez pas utiliser les formulaires de configuration et d'administration pour spécifier une mise en mémoire cache basée sur des URL partielles. Utilisez plutôt la directive **SignificantUrlTerminator** du fichier de configuration du proxy pour indiquer un code d'arrêt pour les demandes d'URL. Le module **Caching Proxy** ne tient alors compte que des caractères précédant le code d'arrêt lors du traitement de la demande, et détermine si le fichier demandé est placé en mémoire cache. Lorsque plusieurs codes d'arrêt sont utilisés, **Caching Proxy** compare les URL entrantes aux codes d'arrêt dans l'ordre dans lequel elles sont définies dans le fichier **ibmproxy.conf**. Pour plus d'informations, voir «SignificantURLTerminator — Spécifie un code d'arrêt pour les demandes d'URL», à la page 280.

Directives du fichier de configuration associées

Pour définir des filtres de mise en mémoire cache en éditant directement le fichier de configuration du proxy, voir les sections de référence des directives suivantes :

- «**NoCaching** — Ne met pas en mémoire cache les fichiers dont l'URL correspond à un modèle», à la page 245
- «**CacheOnly** — Met en mémoire cache uniquement les fichiers dont les URL correspondent à un modèle», à la page 197

- «CacheQueries — Met en mémoire cache les réponses aux URL contenant le caractère ?», à la page 197
- «CacheLocalDomain — Indique s'il est nécessaire de mettre le domaine local en mémoire cache», à la page 194
- «SignificantURLTerminator — Spécifie un code d'arrêt pour les demandes d'URL», à la page 280

Pour obtenir des informations sur les documents ne pouvant pas être mis en mémoire cache, voir Chapitre 16, «Présentation de la mise en cache sur le serveur proxy», à la page 73.

Chapitre 19. Maintenance des données de la mémoire cache

Du fait que la mise en cache implique la création et la sauvegarde d'une copie du fichier servi, certaines opérations sont nécessaires au fonctionnement de la mémoire cache. Le *rafraîchissement* de la mémoire cache permet de mettre à jour les données et d'invalider les fichiers qui ne sont pas synchronisés avec les fichiers du serveur origine. La procédure d'expiration des fichiers est décrite à la section «Expiration des fichiers». Les fichiers invalidés ou inutilisés doivent également être supprimés de la mémoire cache pour faire place à des nouveaux fichiers. La procédure de nettoyage de la mémoire cache est décrite à la section «Récupération de place», à la page 90.

Expiration des fichiers

Préserver la cohérence entre les objets en mémoire cache et les objets stockés sur le serveur de contenu consiste à s'assurer que les informations en mémoire cache sont à jour. Pour chaque document ou autre objet mis en mémoire cache, Caching Proxy calcule le délai d'expiration de l'objet.

Pour les pages HTTP, l'en-tête du document, généré par le serveur de contenu, contient les informations d'expiration.

Le protocole FTP ne fournissant pas d'informations équivalentes sur l'expiration, Caching Proxy génère lui-même un en-tête « Last-Modified: » pour les fichiers FTP, sur la base d'informations du répertoire FTP de chaque fichier et utilise ces informations pour calculer le délai d'expiration. Si le serveur proxy ne peut pas obtenir du serveur FTP les informations de répertoire concernant le fichier, la valeur par défaut correspondant à l'URL FTP est utilisée. Par ailleurs, dans la mesure où il n'existe pas de format standard de date pour les serveurs FTP, Caching Proxy peut ne pas comprendre la date et l'heure renvoyées par certains serveurs FTP. Dans ce cas, l'heure d'expiration par défaut du serveur proxy est utilisée. Cela permet au proxy de gérer la mise en mémoire cache de pages HTTP et de fichiers FTP d'une manière similaire.

L'expiration peut être indiquée par un serveur de contenu de l'une des manières suivantes (par ordre de préférence) :

1. Le serveur de contenu définit un en-tête Cache-control: s-maxage= *n*. Cet en-tête indique au proxy que l'objet, après réception, est valide pendant une durée de *n* secondes.
2. Le serveur de contenu définit un en-tête Cache-control: max-age=*n*. Cet en-tête indique au proxy que l'objet, après réception, est valide pendant une durée de *n* secondes.
3. Le serveur de contenu définit un en-tête Expires: *n*. Cet en-tête indique au proxy que l'objet est valide pendant la durée *n* indiquée.
4. Le serveur de contenu indique la date de dernière modification, à l'aide de l'en-tête Last-Modified: *n*. Le serveur proxy calcule le temps qui s'est écoulé depuis la dernière modification du document, multiplie cette valeur par le facteur de dernière modification de la mémoire cache défini dans le fichier de configuration, et considère que le document est valide pendant cette période. Par exemple si le serveur de contenu indique que le document a été modifié pour la dernière fois il y a une semaine (sept jours) et que le facteur de dernière modification de la mémoire cache est 0,14, le serveur proxy considère

que le document est valide pendant un jour environ. Pour obtenir des instructions sur la définition du facteur de dernière modification de la mémoire cache, voir «Configuration de la validité de la mémoire cache», à la page 88.

5. Si aucune des informations ci-dessus n'est indiquée par le serveur de données, Caching Proxy recherche le paramètre d'expiration par défaut de la mémoire cache correspondant à l'URL en cours et utilise celui-ci en tant que délai d'expiration. Pour obtenir des instructions sur la définition des valeurs d'expiration par défaut de la mémoire cache, voir «Configuration de la validité de la mémoire cache», à la page 88.

Après avoir calculé le délai d'expiration en utilisant la procédure décrite ci-dessus, Caching Proxy vérifie si une valeur de conservation minimale s'applique à cette URL. Si tel est le cas et que la valeur indiquée est supérieure au délai d'expiration calculé, la valeur de conservation minimale est utilisée en tant que délai d'expiration. Cela est vrai même si Caching Proxy calcule un délai d'expiration de 0 minute pour un document. En conséquence, pour éviter de fournir des données périmées, veillez à utiliser le paramètre Minimum Hold. Pour définir la valeur de ce paramètre, utilisez la directive CacheMinHold ou le paramètre **Configuration de la mémoire cache -> Paramètres d'expiration de la mémoire cache : Expiration d'URL**. Pour plus d'informations, voir «Configuration de la validité de la mémoire cache», à la page 88.

La valeur finale du délai d'expiration est comparée à celle indiquée dans le paramètre définissant la marge de la durée. Si la valeur d'expiration est supérieure à la marge de la durée, le document est mis en mémoire cache ; dans le cas contraire, il ne l'est pas. Pour définir la valeur de la durée de la mémoire cache, recourez à la directive CacheTimeMargin ou aux instructions de la section «Configuration de la validité de la mémoire cache», à la page 88.

Si le document est trouvé dans la mémoire cache et qu'il a expiré, Caching Proxy envoie au serveur de contenu une demande spéciale *if-modified-since*. A la suite de cette demande, le serveur de contenu envoie le document si celui-ci a été modifié depuis que le proxy l'a reçu pour la dernière fois. Si le document n'a pas été modifié, le serveur de contenu envoie un message contenant cette information et ne renvoie pas la page entière. Dans ce cas, le proxy fournit le document mis en mémoire cache. Dans le cas de fichiers FTP, le serveur proxy simule la demande « if-modified-since ». S'il détermine que le fichier n'a pas été modifié sur le serveur FTP, il extrait le fichier de la mémoire cache. Sinon, il récupère la version la plus récente sur le serveur FTP.

Informations complémentaires sur la validité de la mémoire cache

- Pratiquement tous les documents Web statiques (contrairement aux documents générés dynamiquement) comportent un en-tête « Last-Modified: ». C'est la méthode utilisée communément par les serveurs proxy pour calculer le délai d'expiration des documents et la première qu'utilise Caching Proxy pour les fichiers FTP. Si cette méthode échoue, le proxy se réfère aux valeurs d'expiration par défaut.
- Très peu de documents utilisent un en-tête « Cache-control: s-maxage », « Cache-control: max-age » ou « Expires: ».
- Les pages générées dynamiquement, qui ne peuvent généralement pas être mises en mémoire cache, peuvent comporter un en-tête Expires: 0 ou Cache-control: no-cache, indiquant que le document arrive à expiration immédiatement. Pour plus d'informations sur la mise en cache de fichiers IBM

WebSphere Application Server générés en dynamique, voir Chapitre 22, «Stockage en mémoire cache d'un contenu généré dynamiquement», à la page 103.

- Agissez avec précaution lorsque vous attribuez une valeur différente de 0 minute au paramètre d'expiration par défaut à l'aide de la syntaxe HTTP:. Un grand nombre de pages générées dynamiquement ne comporte aucun en-tête d'expiration ; dans ce cas, c'est la valeur d'expiration par défaut qui s'applique. L'attribution d'une valeur supérieure à 0 minutes à l'expiration par défaut autorise le proxy à mettre ces objets en mémoire cache mais les utilisateurs peuvent recevoir un contenu périmé (ou des résultats inattendus renvoyés par des programmes CGI ou des servlets).
- Dans les cas suivants, le serveur proxy revalide les documents sur le serveur pour chaque demande, que le document en mémoire cache soit arrivé à expiration ou non :
 - Le document inclut l'un des en-têtes suivants :
 - Cache-control: s-maxage
 - Cache-control: must-revalidate
 - Cache-control: proxy-revalidate
 - Il requiert des droits utilisateur, mais peut être placé en mémoire cache par le serveur.
 - Il contient un en-tête Cache-Control: no-cache, mais il est tout de même mis en mémoire cache (mise en mémoire cache forcée).

Définition des dates avec FTP

S'applique aux configurations avec proxy d'acheminement uniquement.

Dans la mesure où le protocole FTP n'utilise pas des définitions aussi strictes que le protocole HTTP en matière de date et d'heure, plusieurs facteurs peuvent entraîner une légère différence entre les données de l'en-tête Last-Modified générées par le proxy pour les fichiers FTP et la date réelle du fichier. Ces facteurs comprennent les éléments suivants :

- Contrairement au protocole HTTP, le protocole FTP n'indique pas que les valeurs renvoyées doivent correspondre à l'heure GMT (Greenwich Mean Time). Il est donc probable que la date renvoyée par le serveur FTP corresponde à l'heure locale du serveur FTP. Dans la mesure où le proxy ne dispose d'aucun moyen pour déterminer le fuseau horaire utilisé par le serveur FTP, il interprète l'heure comme étant dans son propre fuseau horaire. Le serveur FTP Windows, qui renvoie les heures GMT, fait figure d'exception. Si le proxy détecte que le serveur FTP s'exécute sur des systèmes Windows, il suppose que l'heure du répertoire indiquée correspond à l'heure GMT.
- Sur certains serveurs FTP, la date définie dans les informations de répertoire est renvoyée uniquement au format *Mois Jour Année* les heures et les minutes ne sont pas indiquées. Si le serveur FTP ne transmet pas les heures et les minutes pour le fichier demandé, le proxy suppose que la dernière modification du fichier remonte à la dernière heure et à la dernière minute de la date renvoyée par le serveur FTP. Par exemple, si le serveur FTP renvoie des informations de répertoire et indique que le fichier a été modifié pour la dernière fois le 13 octobre 1998 sans préciser les heures ni les minutes, le proxy suppose que le fichier a été modifié le 13 octobre 1998 à 23:59:59. Ensuite, si le serveur FTP n'est pas un serveur Windows FTP, la date est convertie du fuseau horaire local au fuseau horaire GMT correspondant.

Lorsqu'un fichier FTP arrive à expiration en mémoire cache, le proxy simule le processus de revalidation HTTP if-modified-since pour ce fichier. Au cours de cette opération, il exécute de nouveau la commande FTP LIST pour le fichier demandé, analyse la date du fichier à partir de la réponse renvoyée par le serveur FTP et compare cette date à celle générée par le serveur proxy pour l'en-tête Last-Modified, au moment où le fichier a été extrait. Si la date du fichier n'a pas changé, le serveur proxy indique que le fichier FTP mis en mémoire cache a été revalidé ; il définit une nouvelle date d'expiration et transmet le fichier conservé en mémoire cache plutôt que celui stocké sur le serveur FTP. Si les deux dates du fichier ne concordent pas, le proxy extrait de nouveau le fichier du serveur FTP et stocke cette nouvelle version en mémoire cache, avec la nouvelle date associée.

Il n'est pas toujours possible d'extraire les informations de répertoire pour le fichier sur le serveur FTP. Si le proxy ne parvient pas à déterminer la date du fichier FTP, il ne génère pas l'en-tête « Last-Modified » associé. A la place, il utilise la valeur indiquée pour la directive CacheDefaultExpiry associée à l'adresse URL afin de déterminer la durée de stockage du fichier en mémoire cache. A l'issue de cette période, le proxy extrait toujours une nouvelle version du fichier sur le serveur FTP de nouveau. Si des fichiers FTP mis en mémoire cache utilisent très souvent la directive CacheDefaultExpiry et qu'ils sont fréquemment consultés (trafic réseau élevé), envisagez d'indiquer une valeur CacheDefaultExpiry plus précise pour conserver plus longtemps ces fichiers en mémoire cache.

Pour spécifier les paramètres du délai d'expiration de la mémoire cache, dans les formulaires de configuration et d'administration, sélectionnez **Configuration de la mémoire cache -> Paramètres d'expiration de la mémoire cache -> Délai des fichiers mis en cache**. Pour plus d'informations sur la définition de la durée du stockage en mémoire cache, voir «Expiration des fichiers», à la page 85.

Configuration de la validité de la mémoire cache

Pour spécifier les délais d'expiration des fichiers en mémoire cache, dans les formulaires de configuration et d'administration, sélectionnez **Configuration de la mémoire cache -> Paramètres d'expiration de la mémoire cache**. Les formulaires suivants sont utiles.

Expiration basée sur l'URL

Utilisez ce formulaire pour définir le délai minimal pendant lequel les fichiers sont conservés en mémoire cache, en fonction de leur URL. Vous pouvez indiquer un comportement différent de mise en mémoire cache pour chaque modèle de demande d'URL.

Pour définir le délai d'expiration des fichiers basés sur l'URL en éditant le fichier de configuration du proxy, voir les sections de référence dans l'Annexe B, «Directives du fichier de configuration», à la page 175 pour les directives suivantes :

- «CacheMinHold — Indique la durée de disponibilité des fichiers», à la page 196

Paramètres d'expiration par défaut

Le formulaire **Paramètres d'expiration de la mémoire cache** permet de définir les paramètres d'expiration par défaut des fichiers utilisés ou inutilisés. Vous pouvez définir des valeurs différentes pour les fichiers HTTP, FTP et Gopher et des valeurs différentes pour les fichiers utilisés et inutilisés.

Ce formulaire contient également des options supplémentaires relatives au délai d'expiration des fichiers :

- **Activer le contrôle d'expiration des fichiers en mémoire cache.** Cette case est cochée par défaut. Il est généralement recommandé de sélectionner cette option pour que le serveur n'envoie pas de contenu périmé.
- **Désactiver la récupération des fichiers sur des serveurs éloignés.** Sélectionnez cette option si vous ne voulez pas que le serveur extrait des fichiers des serveurs éloignés.
- **Ne pas mettre en cache des fichiers qui arrivent à expiration dans.** Pour ne pas placer en mémoire cache des fichiers qui arrivent bientôt à expiration, indiquez un délai à l'aide de cette option. Par défaut, les fichiers arrivant à expiration dans moins de 10 minutes ne sont pas mis en mémoire cache.

Pour définir les paramètres d'expiration par défaut en modifiant le fichier de configuration du serveur proxy, reportez-vous aux pages de référence des directives suivantes :

- «CacheDefaultExpiry — Indique l'heure d'expiration par défaut des fichiers», à la page 191
- «CacheExpiryCheck — Indique si le serveur renvoie les fichiers expirés», à la page 192
- «CacheTimeMargin — Indique la durée minimale de mise en mémoire cache d'un fichier», à la page 199
- «CacheUnused — Indique la durée de conservation des fichiers en mémoire cache et non utilisés», à la page 199
- «CacheNoConnect — Spécifie le mode de mémoire cache autonome», à la page 197

Paramètres du facteur de dernière modification

Le formulaire **Facteur de dernière modification** permet de définir la valeur utilisée par le proxy pour calculer une date d'expiration pour les fichiers en mémoire cache dont les en-têtes ne comportent pas de date d'expiration. Vous pouvez définir des valeurs différentes pour les fichiers correspondant à des modèles de demandes différents. Le premier modèle correspondant est utilisé pour calculer la date d'expiration.

Pour définir le facteur de dernière modification en éditant directement le fichier de configuration du proxy, voir «CacheLastModifiedFactor — Spécifie la valeur permettant de déterminer les dates d'expiration», à la page 193.

Délai de conservation en mémoire cache

Le formulaire de configuration **Délai de conservation des fichiers en mémoire cache** permet de définir la durée maximale pendant laquelle un fichier peut rester en mémoire cache. Ces délais sont définis sur la base des modèles de demandes et vous pouvez spécifier quels fichiers éliminer ou revalider une fois ce délai écoulé. Ces paramètres permettent de gérer les fichiers dont la date d'expiration est non valide ou dont le délai d'expiration est très long.

Pour définir une limite maximale pour le délai d'expiration des fichiers en mémoire cache en éditant le fichier de configuration du proxy, consultez les éléments suivants :

- «CacheMaxExpiry — Spécifie la durée de vie maximale des fichiers en mémoire cache», à la page 195
- «CacheClean — Indique la durée de conservation des fichiers en mémoire cache», à la page 191

Récupération de place

Dans le but de conserver en mémoire cache les URL les plus utilisées et de réduire l'utilisation des ressources du système, Caching Proxy met en oeuvre le processus de nettoyage, appelé *récupération de place*, au cours duquel les fichiers anciens ou inutilisés sont supprimés de la mémoire cache afin de libérer de l'espace pour les fichiers plus récents.

Le processus de récupération de place examine les fichiers dans le répertoire de la mémoire cache et tente d'éliminer les fichiers arrivés à expiration pour réduire la taille de la mémoire et ménager de l'espace pour les nouveaux fichiers. La récupération de place s'effectue automatiquement mais certains paramètres peuvent être configurés pour personnaliser le processus en fonction des besoins.

Configuration de la récupération de place

Pour configurer la récupération de place dans les formulaires de configuration et d'administration, sélectionnez **Configuration de la mémoire cache** → **Paramètres de la récupération de place**. Ce formulaire permet de définir la *cote d'alerte supérieure* et la *cote d'alerte inférieure*, qui déterminent le moment du lancement ou de l'arrêt de la récupération de place. Lorsque la quantité d'espace utilisée dans la mémoire cache atteint ou dépasse le pourcentage défini pour la cote d'alerte supérieure, la récupération de place commence. Ce processus continue jusqu'à ce que le pourcentage d'espace utilisé en mémoire cache soit inférieur ou égal à la valeur définie pour la cote d'alerte inférieure.

Vous avez le choix entre deux algorithmes de récupération de place. L'algorithme **responsetime** optimise le temps requis pour répondre aux utilisateurs en supprimant les fichiers volumineux de la mémoire cache. L'algorithme **bandwidth** optimise l'utilisation de la largeur de bande du réseau en supprimant les petits fichiers de la mémoire cache. Choisissez l'un des deux ou une combinaison des deux.

Pour définir la récupération de place en modifiant le fichier de configuration du serveur proxy, voir les sections de référence des directives suivantes :

- «Gc — Spécifie la récupération de place en mémoire cache», à la page 221
- «GcHighWater — Indique le moment du lancement de la récupération de place», à la page 222
- «GcLowWater — Spécifie le moment d'arrêt de la récupération de place», à la page 222
- «CacheAlgorithm — Identifie l'algorithme de mémoire cache», à la page 190

Chapitre 20. Configuration de l'agent de la mémoire cache pour la régénération et le préchargement automatiques

Dans la plupart des cas, les serveurs proxy de mise en mémoire cache mettent un fichier en mémoire cache uniquement sur demande d'un utilisateur. Caching Proxy comporte un agent de mémoire cache qui assure une fonction de préchargement automatique en mémoire cache. Vous pouvez demander à ce que cet agent récupère automatiquement les URL spécifiées et les URL les plus utilisées et les place en mémoire cache avant qu'une demande soit émise.

Dans certains cas, vous devez définir le nom d'hôte du serveur proxy et indiquer le journal des accès à la mémoire cache pour permettre le chargement préalable dans cette dernière. Pour configurer l'agent de mémoire cache, dans les formulaires de configuration et d'administration, sélectionnez **Configuration de la mémoire cache** et utilisez les formulaires **Préchargement de la mémoire cache** et **Régénération de la mémoire cache**. Sachez que les fichiers correspondant aux résultats des requêtes (c'est-à-dire les fichiers dont l'URL comporte un point d'interrogation (?)) ne sont mis en mémoire cache que si la mise en mémoire cache des requêtes est activée.

Le préchargement et la régénération automatique de la mémoire cache offrent les avantages suivants :

- La mise en mémoire cache est appliquée aux URL indiquées avant qu'un utilisateur lance une demande concernant ces pages.
- La mémoire cache est alimentée avant que le serveur soit occupé à traiter les demandes des utilisateurs.
- Les fichiers en cours sont fournis aux utilisateurs plus rapidement en utilisant la mémoire cache plutôt qu'en les recherchant lors de la première demande.

Les inconvénients sont les suivants :

- Le serveur proxy qui met les pages en mémoire cache est actif même pendant les heures où l'activité des utilisateurs est faible.
- Vous devez exercer un certain contrôle sur les éléments chargés automatiquement. Le chargement de fichiers liés à partir de pages de haut niveau, telles que les index Web et les sites de recherche, peut générer des demandes portant sur un grand nombre de pages.

Pour être efficace, l'agent de la mémoire cache doit être lancé lorsque l'activité du serveur est faible et avant que ce dernier ne doive traiter les demandes des clients. Les fichiers sont alors disponibles en mémoire cache pour un traitement plus rapide des demandes les concernant. Par défaut l'agent de la mémoire cache est lancé toutes les nuits, à 3 heures, heure locale.

Remarques sur les configurations avec un serveur proxy inversé :

Pour des raisons de sécurité, lorsque vous utilisez une configuration avec un serveur proxy inversé, par défaut, désactivez la règle Proxy http:*. (Autrement dit, placez en commentaire cette règle dans le fichier ibmproxy.conf.) Cependant, si la règle est désactivée, l'agent de la mémoire cache ne réussit pas à envoyer des demandes et à rafraîchir le contenu du cache de Caching Proxy. Une erreur "403 Forbidden By Rule Error" apparaît dans le journal des erreurs et le rafraîchissement de la mémoire cache n'a pas lieu.

Pour contourner cet incident, utilisez `cacheAgentService`, qui est un service interne fourni par Caching Proxy. Pour activer le service, placez la directive `Service` suivante avant toute autre règle de mappage dans le fichier `ibmproxy.conf` :

```
Service /toute-chaîne-valide* INTERNAL:cacheAgentService
```

La variable `toute-chaîne-valide` correspond à une chaîne quelconque valide n'entrant pas en conflit avec les autres règles de mappage du fichier `ibmproxy.conf`.

Caching Proxy et l'agent de mémoire cache analysent tous les deux l'URI sur la base de cette directive `Service`. Au lieu d'envoyer directement l'URI à Caching Proxy, l'agent de la mémoire cache ajoute à l'URI le modèle `/toute-chaîne-valide` de la directive du service.

Par exemple, l'agent de la mémoire cache transforme l'URI suivante :

```
http://www.ibm.com/
```

en

```
/toute-chaîne-valide/http://www.ibm.com/
```

L'agent de la mémoire cache envoie l'URI et son préfixe à Caching Proxy. À sa réception de la demande, Caching Proxy supprime le préfixe `/toute-chaîne-valide/`. Si l'URI restante est une unité qualifiée complète, Caching Proxy répond directement à la demande sans mapper l'URI par rapport à d'autres règles.

En outre, l'agent de la mémoire cache peut envoyer une URI relative à Caching Proxy. Par exemple, si vous ajoutez `LoadURL /abc/` à l'aide de la directive `Service` précédemment mentionnée dans le fichier `ibmproxy.conf`, l'agent de la mémoire cache transforme cette chaîne en `/toute-chaîne-valide/abc/` et l'envoie à Caching Proxy. Caching Proxy reçoit l'URL, supprime le préfixe, mappe `/abc/` par rapport aux autres règles de mappage et gère la demande en cas de correspondance.

Pour plus d'informations sur la directive `Service`, voir «`Service` — Personnalise l'étape `Service`», à la page 279.

Définition du nom d'hôte du serveur

Sous UNIX et Linux, indiquez le nom d'hôte du serveur proxy dont la mémoire cache est préchargée ou régénérée. Sous Windows, ne précisez le nom d'hôte que si le serveur proxy en cours de régénération ne se trouve pas sur le serveur local. Notez que vous ne pouvez pas régénérer la mémoire cache sur un serveur éloigné pour charger les fichiers les plus fréquemment consultés car l'agent de mémoire cache local ne peut pas accéder au journal des accès de la mémoire cache sur le système éloigné.

Pour définir le nom d'hôte du serveur, dans les formulaires de configuration et d'administration, sélectionnez **Configuration de la mémoire cache → Régénération de la mémoire cache : Identification du serveur de destination de la mémoire cache**.

Préchargement de fichiers spécifiques dans la mémoire cache

Pour précharger la mémoire cache en y intégrant le contenu d'adresses URL spécifiques, dans les formulaires de configuration et d'administration, sélectionnez **Configuration de la mémoire cache** → **Préchargement de la mémoire cache**. Dans ce formulaire, vous pouvez spécifier les URL de l'agent de mémoire cache à charger. Lors du lancement de l'agent, le proxy récupère ces pages en mémoire cache, qu'elles aient été ou non mises en mémoire cache précédemment. (Ces URL sont spécifiées par la directive LoadURL dans le fichier de configuration du proxy). Ce formulaire permet également de définir les adresses URL dont le contenu ne doit jamais être mis en mémoire cache. Il n'est pas nécessaire de définir un journal des accès à la mémoire cache pour ce type de préchargement.

Le formulaire **Préchargement de la mémoire cache** permet de configurer les options suivantes :

- **Régénération quotidienne de la mémoire cache**—Cochez cette case pour que l'agent régénère la mémoire cache toutes les nuits. Si vous ne souhaitez pas lancer l'agent de mémoire cache, assurez-vous que cette case n'est pas cochée.
- **Heure de régénération de la mémoire cache**—Si vous voulez que l'agent de la mémoire cache ne soit pas exécuté à 3:00 du matin, heure locale, indiquez l'heure de lancement choisie.
- **Contenu de la mémoire cache**—Dans la zone **URL ou adresse IP**, spécifiez les URL à charger. Pour exclure des URL du préchargement, spécifiez-les, puis cliquez sur **Ignorer** dans la zone **Etat de la mémoire cache**.

Préchargement dans la mémoire cache des fichiers fréquemment consultés

Pour précharger automatiquement les pages les plus consultées, utilisez le formulaire **Configuration de la mémoire cache** → **Régénérer la mémoire cache**. Cette fonction nécessite un journal des accès à la mémoire cache pour le serveur proxy. Le nom et l'emplacement sont modifiables ; pour en savoir plus, voir Partie 6, «Contrôle de Caching Proxy», à la page 147. Il est possible de déterminer automatiquement les URL les plus utilisées à l'aide du journal des accès à la mémoire cache. L'administrateur peut également préciser le nombre de pages fréquemment consultées à précharger dans la mémoire cache. (Ce nombre est indiqué dans le fichier de configuration du proxy par la directive LoadTopCached).

Le formulaire **Régénération de la mémoire cache** permet de configurer les options suivantes :

- **Régénération quotidienne de la mémoire cache**—Cochez cette case pour que l'agent régénère la mémoire cache toutes les nuits. Si vous ne souhaitez pas lancer l'agent de mémoire cache, assurez-vous que cette case n'est pas cochée.
- **Heure de régénération de la mémoire cache**—Si vous voulez que l'agent de la mémoire cache ne soit pas exécuté à 3:00 du matin indiquez l'heure de lancement choisie.
- **Identifier le serveur de destination de la mémoire**—Utilisez cette option pour régénérer un autre serveur que celui installé sur la machine locale. (Vous ne pouvez pas régénérer un serveur éloigné en fonction de la fréquence d'accès à certains fichiers).
- **Mise en mémoire cache des URL les plus utilisées**—Indiquez le nombre d'URL à mettre en mémoire cache en fonction du journal des accès à la mémoire cache de la nuit précédente.

- **Chargement des pages liées**—Utilisez ce paramètre pour configurer la fonction de suivi logique des liens (pour plus de précisions à propos de cette fonction, ou mise en mémoire cache des chemins d'accès, voir la section suivante). Indiquez le nombre de niveaux auquel appliquer la fonction de suivi logique des liens et s'il convient d'appliquer celle-ci à toutes les pages (**toujours**), à aucune (**jamais**), aux pages indiquées par l'administrateur uniquement (**admin**) ou aux pages les plus utilisées uniquement (**topn**). Indiquez également si la fonction de suivi logique des liens peut être appliquée à plusieurs hôtes, si un délai doit être inséré entre les demandes et s'il convient de mettre en mémoire cache des images en ligne.
- **Nombre d'unités d'exécution pour les demandes**—Indiquez le nombre maximal d'unités d'exécution utilisables pour la régénération de la mémoire cache.
- **Longueur maximale de la file d'attente des travaux**—Indiquez une longueur maximale pour la file d'attente des URL à demander.
- **Nombre maximal d'URL à demander**—Indiquez le nombre maximal de pages à charger. Ce nombre est vérifié avant que la fonction de suivi logique des liens commence à récupérer les pages.
- **Durée maximale pour la demande d'URL**—Indiquez la durée maximale d'exécution de l'agent de la mémoire cache. Si cette durée est fixée à 0 heure 0 minute, l'exécution de l'agent se prolonge jusqu'à son terme.

Fonction de suivi logique des liens

La fonction de *suivi logique des liens* est une fonction facultative de la régénération automatique de la mémoire cache. La plupart des pages Web contiennent des liens vers d'autres pages contenant des informations associées et les utilisateurs suivent souvent ces liens qui les amènent d'une page à une autre et d'un site à un autre. La fonction de suivi logique des liens offre la possibilité de mettre en mémoire cache ces chemins d'informations logiques. Grâce à cette fonction, l'agent de mémoire cache suit un niveau de liens hypertexte HTML indiqué sur les pages en cours de chargement et place toutes ces pages liées en mémoire cache. Les pages liées peuvent être installées sur le même hôte que la page source ou sur des hôtes différents. Un schéma est présenté à la figure 1, à la page 95.

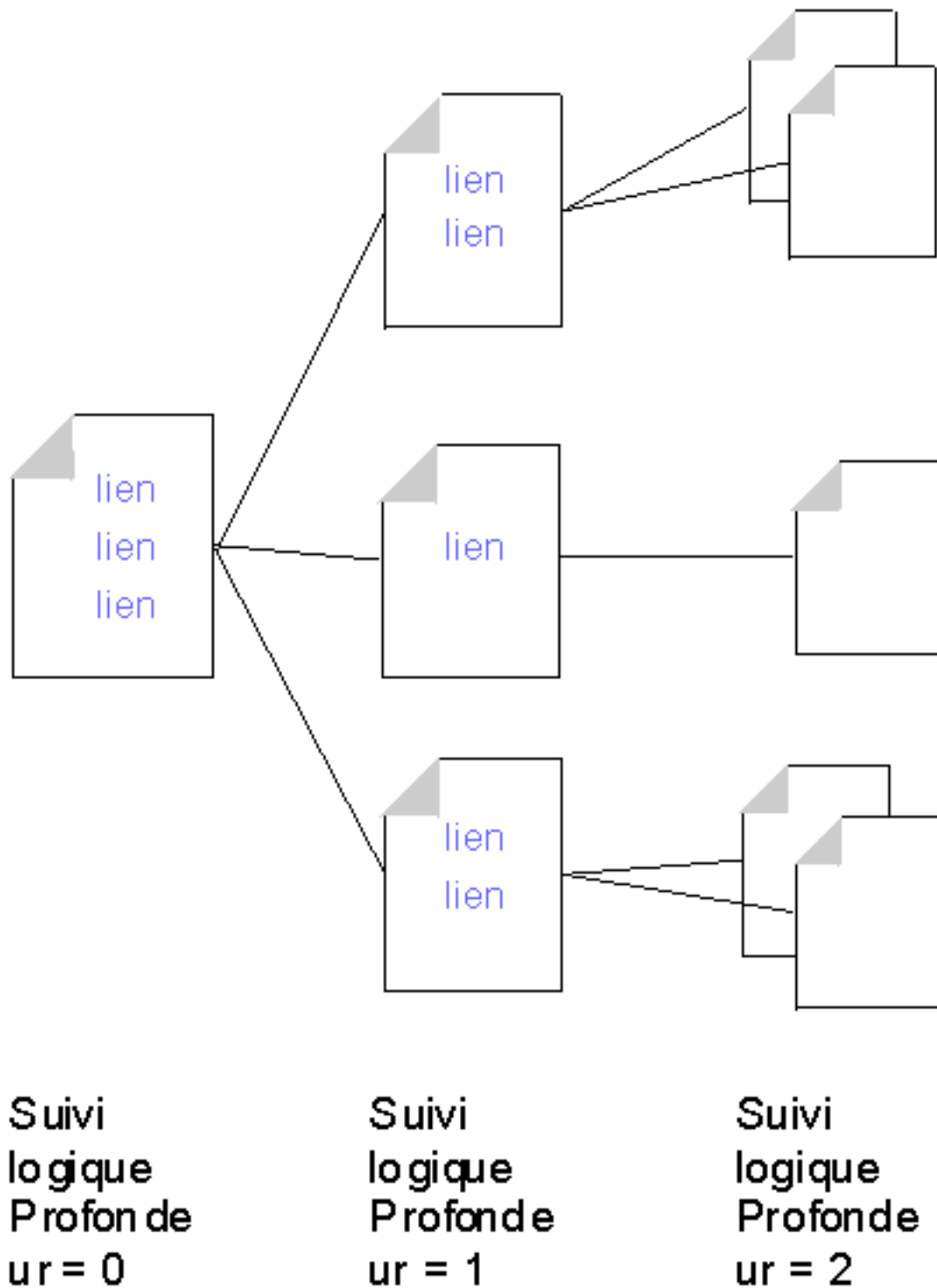


Figure 1. Fonction de suivi logique des liens

Pour contrôler le processus de suivi logique des liens, l'agent de la mémoire cache comporte un nombre maximal d'URL à charger (le paramètre par défaut est 2000), une durée maximale d'exécution (le paramètre par défaut est deux heures) et un nombre maximal d'unités d'exécution utilisables (le paramètre par défaut est

quatre). L'administrateur peut également configurer des contrôles supplémentaires. Par défaut, cette fonction est activée pour deux niveaux de hiérarchie mais son utilisation n'est pas autorisée sur plusieurs hôtes. De plus, un délai est inséré entre les demandes. Pour modifier ces paramètres, voir «Directives du fichier de configuration du proxy associées», à la page 97.

L'agent de la mémoire cache est chargé et régénère ensuite la mémoire cache dans l'ordre suivant :

1. Il charge certaines pages spécifiées par l'administrateur.
2. Il charge les pages les plus utilisées sur la base du journal des accès à la mémoire cache.
3. Si le nombre maximal de pages n'est pas atteint, d'autres pages sont récupérées par la fonction de suivi logique des liens.

Sachez que l'agent de la mémoire cache ne vérifie pas si le nombre maximal de pages a été atteint tant qu'il n'a pas lancé la fonction de suivi logique des liens. Si le nombre maximal de pages (valeur appelée MaxURLs dans le fichier de configuration du proxy) est inférieur au nombre de pages récupérées aux étapes 1 et 2, aucune page liée n'est récupérée.

Les exemples suivants indiquent comment l'agent de la mémoire cache traite les priorités de régénération de la mémoire cache et comment fonctionne le suivi logique des liens, en fonction du nombre maximal d'URL indiqué (en considérant que la fonction de suivi logique des liens est configurée pour tous ces exemples).

Paramètre du fichier de configuration	Résultat
LoadURL http://www.getthis.com/main.html LoadURL http://www.getmetoo.com/welcome.htm LoadTopCached 30 MaxURLs 50	Si le journal des accès à la mémoire cache contient plus de 30 URL uniques, l'agent de la mémoire cache récupère les fichiers main.html et welcome.htm, ainsi que les 30 URL les plus demandées en se basant sur le journal des accès à la mémoire cache. La valeur MaxURLs n'ayant pas été atteinte, l'agent récupère et charge jusqu'à 18 URL liées aux pages déjà mises en mémoire cache.
LoadURL http://www.joesmith.edu/favorites.html LoadURL http://www.janesmith.edu/dislikes.html LoadTopCached 30 MaxURLs 25	Si le journal des accès à la mémoire cache contient plus de 30 URL uniques, l'agent récupère les fichiers favorites.html et dislikes.html, ainsi que les 30 URL les plus demandées en se basant sur le journal des accès à la mémoire cache. Aucun autre fichier n'est récupéré en raison du dépassement de la valeur MaxURLs.
LoadURL http://www.hello.com/hi.htm LoadURL http://www.ballyhoo.com/index.html LoadTopCached 20 MaxURLs 25	Si le journal des accès à la mémoire cache contient plus de 20 URL uniques, l'agent de la mémoire cache récupère l'URL hi.htm et index.html, ainsi que les 20 URL les plus demandées en se basant sur le journal des accès à la mémoire cache, et jusqu'à 3 URL liées aux pages précédentes. Aucun autre fichier n'est récupéré, la valeur MaxURLs ayant été atteinte.

Directives du fichier de configuration du proxy associées

L'agent de mémoire cache peut également être configuré en modifiant directement les directives appropriées dans le fichier de configuration du proxy. Pour obtenir ces directives, reportez-vous aux pages de référence suivantes dans l'Annexe B, «Directives du fichier de configuration», à la page 175 :

- «AutoCacheRefresh — Spécifie si la régénération de la mémoire cache doit être utilisée», à la page 188
- «CacheAccessLog — Spécifie le chemin des fichiers journaux des accès à la mémoire cache», à la page 189
- «CacheRefreshTime — Indique à quel moment démarrer l'agent de la mémoire cache», à la page 198
- «DelayPeriod — Définit une pause entre les demandes», à la page 207
- «DelveAcrossHosts — Active la mise en mémoire cache dans les domaines», à la page 207
- «DelveDepth — Indique jusqu'à quel niveau suivre les liens lors de la mise en mémoire cache», à la page 207
- «DelveInto — Indique si l'agent de la mémoire cache doit suivre les liens», à la page 207
- «IgnoreURL — Spécifie les URL qui ne sont pas régénérées», à la page 226
- «LoadInlineImages — Contrôle la régénération des images intégrées», à la page 233
- «LoadTopCached — Indique le nombre de pages préférées à régénérer», à la page 233
- «LoadURL — Spécifie les URL à régénérer», à la page 234
- «MaxUrls — Indique le nombre maximal d'URL à régénérer», à la page 242

Lancement manuel de l'agent de la mémoire cache

Si la régénération automatique de la mémoire cache est activée, l'agent de la mémoire cache exécute automatiquement une régénération à l'heure indiquée. Vous pouvez cependant exécuter l'agent de la mémoire cache à tout moment à partir de la ligne de commande.

Le fichier exécutable est le suivant :

- Sous Linux et UNIX : `usr/sbin/cacheagt`
- Sous Windows : `serveur_racine\bin\cacheagt.exe`,
serveur_racine correspondant à l'unité et au répertoire d'installation de Caching Proxy (par exemple, `C:\Program Files\IBM\edge\cp`).

Sous Linux et UNIX, vous pouvez exécuter automatiquement l'agent de la mémoire cache à plusieurs reprises à l'aide du démon **cron**. Les travaux contrôlés par **cron** sont indiqués par l'ajout d'une ligne dans le fichier crontab du système. Exemple d'entrée de ce fichier de commandes sous Linux et UNIX :

```
45 16 * * * /usr/sbin/cacheagt
```

Cette commande lance l'agent de la mémoire cache tous les jours à 16 h 45, heure locale. Vous pouvez utiliser plusieurs entrées pour exécuter l'agent plusieurs fois. Pour plus d'informations, consultez la documentation du système d'exploitation traitant du démon **cron**.

Si vous utilisez un démon **cron** pour exécuter l'agent de la mémoire cache, n'oubliez pas de désactiver l'option de régénération automatique, soit en utilisant le formulaire de configuration **Configuration de la mémoire cache** -> **Régénération de la mémoire cache**, soit en modifiant le fichier de configuration du proxy. Dans le cas contraire, l'agent est exécuté plusieurs fois par jour.

Chapitre 21. Utilisation d'une mémoire cache partagée

Il n'est pas rare que le trafic sur un point de présence Web soit trop important pour être géré par un seul serveur. Une solution consiste à ajouter des serveurs. Lorsque plusieurs serveurs proxy avec mémoire cache sont utilisés, il arrive fréquemment que le contenu des différentes mémoires cache se chevauche. Outre que la redondance de données est anti-productive, la bande passante n'est pas totalement optimisée puisqu'un fichier en mémoire cache est extrait une nouvelle fois du serveur origine quand il ne réside pas dans la mémoire cache du serveur proxy duquel il émane. S'il est possible de réduire les mises en mémoire cache redondantes en utilisant une chaîne hiérarchique de serveurs proxy, ce scénario provoque toujours une augmentation du trafic sur un serveur donné et chaque maillon supplémentaire dans la chaîne accroît les temps d'attente.

Le partage de cache permet d'y remédier en permettant aux caches de partager leur contenu les uns avec les autres. La largeur de bande nécessaire est bien inférieure pour les raisons suivantes :

- Les objets ne font plus l'objet de recherches multiples.
- Une mémoire cache logique combinée et de plus grande taille augmente le taux de réussite des recherches.

Les deux méthodes permettant d'utiliser plusieurs caches comme s'il s'agissait d'un cache logique unique sont les suivantes :

- Remote Cache Access (RCA) est une fonction de Caching Proxy définissant un tableau de caches membres. Un fichier est stocké dans l'une de ces mémoires cache selon la logique applicative interne.
- Le plug-in Caching Proxy permet au serveur proxy d'utiliser le protocole ICP (Internet Caching Protocol). Il peut remplacer RCA si vous souhaitez partager des données entre des machines Caching Proxy et d'autres.

Cependant, RCA et ICP sont utilisables conjointement.

Remote cache access (RCA)

Lors de la planification de la fonction RCA, tenez compte des recommandations suivantes :

- Les serveurs proxy mis en oeuvre doivent être proches les uns des autres et connectés entre eux via des connexions à largeur de bande élevée (bus FDDI ou SP2, par exemple).
- L'inscription à la fonction RCA doit être à long terme pour que la configuration soit aussi stable que possible.
- Les serveurs proxy doivent posséder des capacités similaires (CPU, taille de la mémoire, taille de la mémoire cache).
- Les arrêts du réseau doivent être peu fréquents.
- Un tableau doit comporter moins de 100 membres.
- Tous les membres du tableau doivent utiliser la même version de Caching Proxy.

Remarque : Si les serveurs proxy utilisent plusieurs versions du système d'exploitation Linux (SUSE et Red Hat par exemple), assurez-vous que l'utilisateur « nobody » possède le même UID que ses homologues. Vérifiez les entrées du fichier des mots de passe et des

groupes dans le répertoire /etc/ de chaque ordinateur et affectez le même UID à l'utilisateur « nobody." »

L'accès à distance à la mémoire cache n'est pas approprié si l'une de ces conditions n'est pas respectée, ou si différentes organisations gèrent des serveurs différents, membres du même tableau.

Configuration de la fonction RCA (Remote Cache Access)

Pour configurer la fonction RCA, dans les formulaires de configuration et d'administration, sélectionnez **Configuration de la mémoire cache -> Remote Cache Access**. Ce formulaire contient des zones permettant de définir un tableau nommé qui partage une mémoire cache logique. Entrez les informations requises pour chaque membre du tableau.

Pour configurer la fonction RCA en modifiant le fichier de configuration du fichier, voir les sections de référence dans l'Annexe B, «Directives du fichier de configuration», à la page 175 pour les directives suivantes :

- «ArrayName — Attribue un nom au tableau de la mémoire cache à distance», à la page 187
- «Member — Spécifie un membre d'un tableau», à la page 242

Configuration du plug-in Internet Caching Protocol

Le plug-in ICP (Internet Caching Protocol) permet à Caching Proxy d'interroger d'autres mémoires cache compatibles ICP au cours de ses recherches de pages HTML et d'autres ressources à mettre en mémoire cache. Lorsqu'un serveur proxy reçoit une demande HTTP, il recherche la ressource en question dans sa propre mémoire cache. Si la ressource ne se trouve pas dans son cache local et que le plug-in ICP est actif, le serveur proxy lance une recherche en boucle de l'URL dans un paquet de requêtes ICP et place ce paquet dans toutes les mémoires cache homologues ICP identifiées. Si une mémoire cache homologue détecte la ressource, le serveur d'origine la récupère dans cette mémoire cache. Si plusieurs mémoires cache homologues répondent de façon positive, le traitement de la première réponse commence. Si aucune mémoire cache homologue ne la détecte, le serveur d'origine continue la recherche en fonction de son flux de travail. Par exemple, le serveur proxy peut appeler un autre plug-in, poursuivre le traitement avec la routine Remote Caching Access (si RCA est activé) ou récupérer la ressource demandée.

Configuration du plug-in ICP

Le plug-in ICP est activé et configuré en modifiant le fichier de configuration proxy, `ibmproxy.conf`. Pour pouvoir initialiser le plug-in ICP, vous devez ajouter une directive `ServerInit`, une directive `PreExit`, ou les deux, à la section directives API du fichier `configuration.conf`. Les directives utilisées dépendent du rôle que joue Caching Proxy dans le système ICP :

- Pour que Caching Proxy joue le rôle d'un serveur ICP, choisissez la directive `ServerInit` qui appellera le module `icpServer`.
- Pour que Caching Proxy joue le rôle d'un client ICP, choisissez la directive `PreExit` qui appellera le module `icpClient`.
- Pour que Caching Proxy soit à la fois client ICP et serveur ICP, utilisez les deux directives.
- A l'aide des directives `icpAddress`, `icpMaxThreads`, `icpPeer`, `icpPort` et `icpTimeout`, configurez les paramètres utilisés par le plug-in.

Pour créer cette directive, modifiez manuellement le fichier `ibmproxy.conf` ou, si le serveur proxy est en cours d'exécution, utilisez le formulaire de configuration et d'administration pour sélectionner **Configuration du serveur** → **Traitement des demandes** → **Traitement des demandes API**.

En effet, des directives données à titre de prototype ont été ajoutées (sous forme de commentaires) à la section API du fichier `ibmproxy.conf`. Ces directives API sont placées dans un ordre délibérément choisi. Lors de l'ajout de directives d'API pour permettre de nouvelles fonctionnalités et l'utilisation de plug-ins, respectez l'ordre dans lequel figurent les directives dans la section Prototypes du fichier de configuration. Vous pouvez également supprimer les marques de commentaires et modifier, si nécessaire, les directives API pour chacune des fonctionnalités ou chacun des plug-ins souhaités.

Les directives `ServerInit` et `PreExit` ont deux arguments chacune : (1) le chemin qualifié complet d'accès à la bibliothèque partagée et (2) l'appel à la fonction. Les deux derniers arguments doivent être délimités par deux points (:). Le premier argument est propre au système et dépend de l'endroit où sont installés les composants du plug-in. Le deuxième argument est défini dans le code de la bibliothèque partagée et doit être tapé exactement comme il apparaît dans cette dernière.

Chacune de ces directives doit figurer sur une seule ligne dans le fichier de configuration du proxy.

```
ServerInit chemin_de_bibliothèque_partagée:icpServer
```

Exemple Linux et UNIX :

```
ServerInit /opt/ibm/edge/cp/internet/lib/plugins/icp/libicp_plugin.so:icpServer
```

Exemple Windows :

```
ServerInit C:\Program Files\IBM\edge\cp\Bin\plugins\icp\icpplugin.dll:icpServer
```

```
PreExit chemin_de_bibliothèque_partagée:icpClient
```

Exemple Linux et UNIX :

```
PreExit /opt/ibm/edge/cp/internet/lib/plugins/icp/libicp_plugin.so:icpClient
```

Exemple Windows :

```
PreExit C:\Program Files\IBM\edge\cp\Bin\plugins\icp\icpplugin.dll:icpClient
```

Pour configurer les paramètres du plug-in, ajoutez ou modifiez les directives ICP* disponibles dans le fichier de configuration du proxy. Pour plus d'informations, reportez-vous aux descriptions des directives suivantes.

- «ICP_Address — Spécifie l'adresse IP des requêtes ICP», à la page 225
- «ICP_MaxThreads — Spécifie le nombre maximal d'unités d'exécution pour requêtes ICP», à la page 225
- «Occupier — Spécifie un membre de cluster ICP», à la page 225
- «ICP_Port — Spécifie le numéro de port des requêtes ICP», à la page 226
- «ICP_Timeout — Spécifie le délai d'attente maximal des requêtes ICP», à la page 226
- «PreExit — Personnalise l'étape PreExit», à la page 255
- «ServerInit — Personnalise l'étape d'initialisation du serveur», à la page 277

Chapitre 22. Stockage en mémoire cache d'un contenu généré dynamiquement

S'applique aux configurations avec proxy inversé uniquement.

La fonction de mise en mémoire cache dynamique permet au Caching Proxy de placer en mémoire cache un contenu généré dynamiquement sous forme de réponses JavaServer Pages (JSP) et de servlets générés par un serveur IBM WebSphere Application Server. Un module d'adaptateur Caching Proxy est utilisé sur le serveur d'applications pour modifier les réponses afin qu'elles puissent être stockées dans la mémoire cache dynamique du serveur d'applications ainsi que sur le serveur proxy. À l'aide de cette fonctionnalité, le contenu généré dynamiquement peut être stocké en mémoire cache à la périphérie du réseau, évitant ainsi à l'hôte du contenu d'envoyer des demandes répétées au serveur d'applications lorsque plusieurs clients demandent le même contenu.

Remarque : La fonction de mise en mémoire cache dynamique ne permet pas au serveur proxy de placer en mémoire cache des résultats issus de demandes d'URL. Pour mettre en mémoire cache des résultats de requêtes, configurez des filtres de mise en mémoire cache (décrits dans Chapitre 18, «Contrôle du contenu de la mémoire cache», à la page 81 et dans la documentation de référence des directives dans «CacheQueries — Met en mémoire cache les réponses aux URL contenant le caractère ?», à la page 197). Il est possible de mettre en mémoire cache les résultats de demandes émanant de systèmes autres que IBM WebSphere Application Server.

Dans certains cas (vos servlets utilisent des URL sous la forme de demandes, par exemple), il est nécessaire d'activer la mise en mémoire cache des demandes pour que la fonction de mise en cache dynamique puisse fonctionner. Le serveur proxy assimile à une demande toute URL comportant un point d'interrogation (?).

La mise en cache de contenu généré dynamiquement offre les avantages suivants :

- réduction de la charge des hôtes de contenu,
- réduction de la charge des serveurs d'applications,
- livraison plus rapide des ressources demandées aux utilisateurs finaux,
- utilisation moins importante de la largeur de bande entre les serveurs et
- amélioration de l'évolutivité des sites Web qui créent ou traitent un contenu généré dynamiquement.

Le serveur d'applications n'exporte que les pages publiques intégralement composées pour la mise en mémoire cache du proxy. Les pages privées ne sont pas mises en cache par le proxy. Par exemple, une page générée de façon dynamique sur un site public et répertoriant les prévisions météorologiques peut être exportée par IBM WebSphere Application Server et mise en mémoire cache par Caching Proxy. Cependant, une page générée de façon dynamique répertoriant le contenu du panier électronique d'un utilisateur ne peut pas être mise en cache par le serveur proxy. En outre, pour qu'une page générée dynamiquement soit stockée en mémoire cache, tous ses sous-composants doivent également pouvoir être stockés en mémoire cache.

Les fichiers mis en mémoire cache dynamique n'expirent pas de la même manière que les fichiers normaux ; ils peuvent être invalidés par le serveur d'applications qui les a générés.

Les entrées de la mémoire cache dynamique sont invalidées dans les cas suivants :

- le processus de récupération de place de la mémoire cache dynamique supprime une entrée en raison de la surcharge de la mémoire cache ;
- le délai d'expiration défini dans l'entrée correspondant au servlet (servletcache.xml) ou dans la directive ExternalCacheManager du proxy arrive à expiration ;
- un agent ou une application externe demandent aux API de la mémoire cache dynamique d'invalidiser ses entrées.

L'invalidation d'entrées de la mémoire cache dynamique s'effectue en générant un message de type Invalidate à l'intention de l'instance spécifique du module de mise en mémoire cache dynamique de Caching Proxy. Caching Proxy reçoit les messages d'invalidation sous forme de méthodes post envoyées au pointeur de ressources /WES_External_Adapter. Caching Proxy efface ensuite les entrées non valides de sa mémoire cache.

La mise en mémoire cache dynamique requiert les étapes de configuration suivantes :

- Configuration de IBM WebSphere Application Server :
 - Configurez chaque serveur d'applications pour la mise en mémoire cache dynamique locale.
 - Configurez chaque serveur d'applications pour qu'il utilise l'adaptateur de mémoire cache externe.
 - Spécifiez les mémoires cache externes pouvant être utilisées pour chaque JSP et servlet pouvant être placé en mémoire cache.
- Configuration de Caching Proxy
 - Activez Caching Proxy pour utiliser le plug-in de mise en mémoire cache dynamique.
 - Spécifiez les sources à partir desquelles le contenu dynamique sera mis en mémoire cache.

Configuration de IBM WebSphere Application Server pour la mise en mémoire cache du proxy

Configuration de la mise en mémoire cache dynamique sur le serveur d'applications

Suivez les instructions de la documentation IBM WebSphere Application Server pour configurer votre serveur d'applications afin qu'il utilise sa mémoire cache dynamique locale (également appelée mémoire cache dynamique à fragments). La mémoire cache dynamique à fragments interagit avec la mémoire cache externe du Caching Proxy de Application Server.

Configuration de l'adaptateur du serveur d'applications

IBM WebSphere Application Server communique avec Caching Proxy à l'aide du module External Cache Adapter, installé avec Application Server.

Remarque : Pour plus d'informations sur la configuration de la fonction de mise en cache dynamique, reportez-vous à la note technique fournie sur le site Web d'assistance de IBM WebSphere Application Server.

Configuration des serveurs Caching Proxy pour la mise en mémoire cache dynamique

Pour activer le serveur proxy afin qu'il place le contenu dynamique en mémoire cache (résultats des servlets et des JSP), vous devez effectuer deux modifications dans le fichier de configuration du proxy, `ibmproxy.conf`. La première modification active le plug-in de la mise en mémoire cache dynamique et la seconde le configure pour qu'il reconnaisse les sources du contenu dynamique stockable en mémoire cache.

Configuration de la directive Service pour l'activation du plug-in de la mise en mémoire cache dynamique

Une directive API de l'étape Service est utilisée pour activer le plug-in de la mise en mémoire cache dynamique. Pour créer cette directive, modifiez manuellement le fichier `ibmproxy.conf` ou, si le serveur proxy est en cours d'exécution, utilisez les formulaires de configuration et d'administration pour sélectionner **Configuration du serveur** -> **Traitement des demandes** -> **Traitement des demandes API**. Le contenu de la directive est illustré dans des exemples qui apparaissent plus loin dans cette section.

Une directive Service pour l'activation de la mise en mémoire cache dynamique est donnée en exemple sous forme de commentaire dans la section API du fichier `ibmproxy.conf`. Elle comporte l'en-tête plug-in JSP. Notez que ces directives API sont placées dans un ordre délibérément choisi. Lors de l'ajout de directives d'API pour permettre de nouvelles fonctionnalités et l'utilisation de plug-ins, respectez l'ordre dans lequel figurent les directives dans la section Prototypes du fichier de configuration. Vous pouvez également supprimer les caractères de commentaires des exemples de directives API et les modifier si nécessaire afin de prendre en charge le support de chaque fonction ou plug-in souhaité.

Définissez la directive Service comme indiqué dans les exemples suivants. (Chacune de ces directives doit figurer dans le fichier de configuration sur une seule ligne ; ces exemples contiennent parfois des sauts de ligne pour plus de clarté).

- Sous AIX :

```
Service /WES_External_Adapter /opt/ibm/edge/cp/lib/plugins/  
dynacache/libdyna_plugin.o:exec_dynacmd
```

- Sous Solaris :

```
Service /WES_External_Adapter /opt/ibm/edge/cp/lib/plugins/  
dynacache/libdyna_plugin.so:exec_dynacmd
```

- Sous Linux :

```
Service /WES_External_Adapter /usr/lib/libdyna_plugin.so:exec_dynacmd
```

- Sous Windows :

```
Service /WES_External_Adapter C:\Program Files\IBM\edge\cp\bin\plugins\  
dynacache\dyna_plugin.dll:exec_dynacmd
```

Si le logiciel Caching Proxy est installé dans un répertoire autre que le répertoire par défaut, substituez le chemin spécifié dans l'exemple par le chemin de votre installation.

Configuration de la directive ExternalCacheManager pour la spécification des sources des fichiers

Il est également nécessaire de configurer chaque composant Caching Proxy pour qu'il reconnaisse la source des fichiers générés dynamiquement. Ajoutez une directive ExternalCacheManager au fichier ibmproxy.conf pour chaque serveur d'applications qui placera en mémoire cache un contenu généré dynamiquement sur serveur proxy. Cette directive spécifie un serveur WebSphere Application Server qui placera les résultats en mémoire cache sur le proxy et définit un délai d'expiration maximal pour le contenu de ce serveur. Vous trouverez plus de détails dans le document «ExternalCacheManager — Configure Caching Proxy pour la mise en mémoire cache dynamique à partir de IBM WebSphere Application Server», à la page 218.

L'ID serveur utilisé dans la directive ExternalCacheManager doit correspondre à l'ID de groupe utilisé dans la stance du groupe de mémoire cache externe du fichier dynacache.xml du serveur d'applications.

Dans le cas des exemples précédents, ajoutez l'entrée ci-après dans le fichier ibmproxy.conf de chaque proxy.

```
ExternalCacheManager IBM-edge-cp-XYZ-1 20 seconds
```

Le composant Caching Proxy ne met en mémoire cache que le contenu d'un serveur IBM WebSphere Application Server dont l'ID de groupe correspond à une entrée ExternalCacheManager du fichier ibmproxy.conf.

Chapitre 23. Personnalisation de la mémoire cache du serveur proxy

La vitesse des unités de mise en mémoire cache est déterminante pour les performances de Caching Proxy lorsque la mise en mémoire cache est activée. Cette section propose des suggestions sur le type d'unité de mise en mémoire cache à choisir et sur la façon de la configurer pour optimiser les performances.

Choix du support de stockage de la mémoire cache

Caching Proxy peut utiliser deux types de support pour la mise en mémoire cache :

- Mémoire
- Partitions de disque en mode brut

Le stockage des données en mémoire cache optimise la vitesse de récupération des fichiers mais la taille de la mémoire est limitée par la quantité de mémoire disponible sur le serveur. Un disque cache, composé d'une ou plusieurs partitions de disque en mode brut, est moins performant mais il offre généralement une plus grande capacité de stockage.

Optimisation des performances du cache disque

Les partitions de disque utilisées pour la mise en mémoire cache doivent être consacrées exclusivement à cet usage ; ces unités de disque physiques ne doivent contenir aucun autre système de fichiers et ne doivent pas être utilisées à d'autres fins qu'à la mise en mémoire cache du proxy. De plus, ne compressez pas les données sur une unité utilisée pour la mise en mémoire cache du proxy car cela réduit les performances.

Chaque support de mise en mémoire cache (disque ou fichier) peut être affecté par une surcharge de la mémoire du serveur proxy. En général, l'utilisation de la totalité d'une unité de disque physique en tant que support unique pour la mise en mémoire cache est la solution la plus performante. L'utilisation de RAID ou de tout autre mécanisme permettant de combiner plusieurs unités de disque physiques en une seule unité logique offre des résultats décevants. Si vous voulez utiliser plusieurs unités de disque, définissez-les comme telles dans le formulaire de configuration **Paramètres de la mémoire cache** ou au niveau de la directive CacheDev du fichier de configuration du proxy. Cette méthode permet au serveur proxy de contrôler le parallélisme de la lecture et de l'écriture sur plusieurs disques et le processus ne dépend pas des performances du système d'exploitation ou d'un sous-système de disque.

Récupération de place en mémoire cache

La récupération de place en mémoire cache pour le serveur proxy élimine de la mémoire cache les fichiers arrivés à expiration, libérant ainsi de l'espace pour le stockage des fichiers liés aux nouvelles demandes. Ce processus est lancé automatiquement lorsque la quantité d'espace utilisé dans la mémoire cache atteint un seuil défini, appelé *cote d'alerte supérieure*, et son exécution continue jusqu'à ce que le seuil *cote d'alerte inférieure* soit atteint.

Etant donné que la routine de récupération de place utilise un minimum de ressources CPU et n'a pas d'incidence sur la disponibilité des éléments non expirés en mémoire cache, il n'est pas nécessaire de configurer l'exécution de ce processus à un moment précis.

Pour améliorer les performances de la récupération de place, vous pouvez définir la cote d'alerte supérieure et la cote d'alerte inférieure. Vous pouvez également configurer le type d'algorithme utilisé pour la récupération de place. Pour plus d'informations sur la modification de la récupération de place, voir «Récupération de place», à la page 90.

Optimisations pour chaque plateforme

Les suggestions complémentaires suivantes permettent d'optimiser les performances de la mémoire cache sur chaque plateforme.

AIX

Créez un seul volume logique sur un disque, en utilisant de préférence toutes les partitions physiques (PP) disponibles. Par exemple, pour un disque de 9 Go, créez un volume logique de 9 Go appelé `cpcache1`. Formatez ce disque et définissez-le en tant qu'unité de mise en mémoire cache en utilisant son volume logique en mode brut, `/dev/rcpcache1`.

HP-UX et Solaris

Sur l'unité de mémoire cache, créez une partition unique (ou segment) occupant l'intégralité du disque. Par exemple, pour un disque de 9 Go, créez une partition de 9 Go appelée `clt3d0s0`. Formatez ce disque et définissez-le en tant qu'unité de mise en mémoire cache du proxy en utilisant son unité en mode brut, `/dev/rdisk/clt3d0s0`.

Windows

Créez une partition unique occupant l'intégralité du disque. Par exemple, pour un disque de 9 Go, créez une partition de 9 Go appelée `i:`. Formatez ce disque et définissez-le en tant qu'unité de mise en mémoire cache du proxy en utilisant son unité en mode brut, `\\.\i:`.

Des informations sur la configuration de la mémoire cache du serveur proxy et sur la définition des unités de mise en mémoire cache sont présentées Partie 4, «Configuration de fonction de mise en cache du serveur proxy», à la page 71.

Partie 5. Configuration de la sécurité de Caching Proxy

Cette partie traite de la sécurité de base qui utilise SSL avec Caching Proxy, active le matériel cryptographique et utilise le plug-in IBM Tivoli Access Manager (anciennement Tivoli Policy Director) et le module d'autorisation PAC-LDAP.

Cette partie comporte les chapitres suivants :

Chapitre 24, «A propos de la sécurité du serveur proxy», à la page 111

Chapitre 25, «Configurations de protection du serveur», à la page 113

Chapitre 26, «Secure Sockets Layer (SSL)», à la page 117

Chapitre 27, «Support du matériel cryptographique», à la page 133

Chapitre 28, «Utilisation du plug-in Tivoli Access Manager», à la page 135

Chapitre 29, «Utilisation de l'outil module d'autorisation PAC-LDAP», à la page 137

Chapitre 24. A propos de la sécurité du serveur proxy

Tout serveur accessible à partir du réseau Internet peut attirer l'attention de personnes non autorisées, désireuses de connaître le système d'exécution associé. Ces personnes peuvent tenter de découvrir des mots de passe, de mettre à jour des fichiers, d'exécuter des fichiers ou de lire des données confidentielles. La structure ouverte d'Internet constitue l'un des attraits du réseau World Wide Web. Toutefois, Internet peut donner lieu à des utilisations positives comme à des manipulations frauduleuses.

Les sections ci-après décrivent comment contrôler les utilisateurs autorisés à accéder aux fichiers stockés sur le serveur Caching Proxy.

Caching Proxy prend en charge les connexions Secure Sockets Layer (SSL). Il s'agit de connexions sécurisées qui utilisent les fonctions de chiffrement et de déchiffrement et sont établies entre le navigateur du client et le serveur de destination (serveur de données ou serveur de substitution).

Lorsque le composant Caching Proxy est configuré comme un serveur de substitution, il peut établir des connexions sécurisées avec des clients et/ou des serveurs de données. Pour configurer les paramètres des connexions SSL dans les formulaires de configuration et d'administration, sélectionnez **Configuration du proxy** → **Paramètres SSL**. Dans ce formulaire, cochez la case **Activation de SSL** et indiquez la base de données de clés et le fichier de mots de passe associé.

Lorsque le composant Caching Proxy est configuré comme un serveur proxy d'acheminement, il utilise un protocole de transmission appelé *SSL tunneling* pour acheminer les demandes chiffrées entre le client et le serveur de contenu. Les informations chiffrées ne sont pas mises en mémoire cache car le serveur proxy ne déchiffre pas ce type de demande. Si vous installez un serveur proxy d'acheminement, la fonction d'établissement des tunnels SSL est activée par défaut. Pour désactiver cette fonction à partir des formulaires de configuration et d'administration, sélectionnez **Configuration du proxy** → **Paramètres du proxy** et désactivez la case à cocher **SSL Tunneling** dans ce formulaire.

Plusieurs précautions élémentaires vous sont proposées pour protéger le système :

- Installez le serveur destiné à un accès public dans un réseau séparé du réseau local ou interne.
- Désactivez les outils permettant aux utilisateurs distants d'accéder aux processus internes du serveur. Envisagez notamment de désactiver les clients **telnet**, **TN3270**, **rlogin** et **finger** sur le système exécutant le serveur.
- Utilisez la fonction de filtrage de paquets et les pare-feu.

Le filtrage des paquets permet de définir les points d'origine et de destination des données. Vous pouvez configurer le système pour que certaines combinaisons point d'origine/point de destination soient rejetées.

Un pare-feu sépare un réseau interne d'un réseau auquel des utilisateurs ont accès, comme Internet. Le pare-feu peut se composer d'un groupe d'ordinateurs ou d'un ordinateur unique chargé d'assurer une fonction de passerelle dans les deux sens, et de réguler et de vérifier le trafic. IBM Firewall est un exemple de logiciel pare-feu.

- Contrôlez les scripts CGI. L'utilisation de scripts CGI sur un serveur Web peut présenter certains risques ; en effet, ces scripts peuvent afficher des variables d'environnement comportant des données confidentielles, telles que les ID utilisateur et les mots de passe. Avant d'exécuter un programme CGI sur le serveur, vous devez savoir exactement comment il fonctionne et contrôler les utilisateurs autorisés à y accéder.

Remarque : Si vous utilisez l'assistant de configuration pour configurer le serveur proxy, une règle de mappage doit être créée pour les demandes du proxy reçues sur le port 443 pour que SSL puisse être activé. Pour plus d'informations, voir «Définition de règles de mappage», à la page 42.

Exemples :

Proxy /* http://serveur de données :443

ou

Proxy /* https://serveur de données :443

Chapitre 25. Configurations de protection du serveur

Le présent chapitre indique comment protéger les données et les fichiers stockés sur le serveur à l'aide de configurations de protection. Les configurations de protection sont appliquées en fonction de la demande reçue par le serveur, et plus particulièrement en fonction du répertoire, du fichier ou du type de fichier indiqué dans cette demande. Dans une configuration de protection, les sous-directives contrôlent l'octroi ou le refus des droits d'accès en fonction des caractéristiques des répertoires ou des fichiers protégés.

Utilisation des formulaires de configuration et d'administration pour définir les informations de protection

Pour définir une configuration de protection et ses modalités d'application, sélectionnez dans les formulaires de configuration et d'administration **Configuration du serveur -> Protection des documents**. Utilisez ce formulaire pour les opérations suivantes :

1. Définissez l'ordre de la règle de protection.

Les règles de protection sont appliquées en fonction de leur ordre d'apparition dans le tableau du formulaire de configuration. Habituellement, le programme répertorie les règles de la plus spécifique à la plus générale.

Utilisez le menu déroulant et les boutons pour spécifier l'emplacement d'une règle de protection.

2. Définissez un modèle de demande.

La protection est activée en fonction des modèles de demandes qui sont comparés aux demandes envoyées au serveur proxy par les clients.

Une *demande* est un élément d'une adresse URL complète, indiqué après le nom d'hôte du serveur. Par exemple, si le serveur s'appelle *fine.feathers.com* et que l'utilisateur d'un navigateur entre l'adresse *http://fine.feathers.com/waterfowl/schedule.html*, la demande reçue par le serveur est */waterfowl/schedule.html*. Les modèles de demandes indiquent les noms de répertoires et/ou de fichiers protégés. Par exemple, les demandes qui activent la protection sur la base du modèle de demande qui vient d'être décrit (*/waterfowl/schedule.html*) comprennent les répertoires */waterfowl/** et */*schedule.html*.

Saisissez le modèle de demande dans la zone **Modèle de demande d'URL**.

3. Définissez une configuration de protection.

Une configuration de protection renseigne Caching Proxy sur le mode de traitement d'une demande correspondant à un modèle. Le formulaire **Protection des documents** permet d'utiliser une configuration de protection existante (nommée) ou d'en définir une nouvelle.

Pour utiliser une configuration existante, cliquez sur le bouton d'option **Protection nommée** et entrez le nom de la configuration dans la zone. Pour définir une nouvelle configuration, cliquez sur le bouton d'option **En ligne** et suivez les instructions indiquées à l'étape 6.

4. Sélectionnez l'adresse d'un demandeur (facultatif).

Vous pouvez appliquer différentes règles aux demandes provenant de différentes adresses de serveur. Par exemple, vous pouvez être amené à appliquer une configuration de protection différente pour traiter les demandes

concernant les fichiers journaux, lorsque celles-ci sont émises par des adresses IP appartenant à votre entreprise.

Remarque : Pour filtrer les adresses des demandes, vous devez activer la fonction de recherche DNS. Voir «DNS-Lookup — Indique si le serveur recherche les noms d’hôte client», à la page 212.

Si vous voulez inclure l’adresse d’un demandeur dans la règle, saisissez-la dans la zone **Adresse IP du serveur ou nom d’hôte**.

5. Cliquez sur **Validation**.

Si vous avez utilisé une configuration de protection existante, il est inutile d’entrer d’autres informations. Si vous avez sélectionné une configuration de protection en ligne ou indiqué une configuration qui n’existe pas, le système ouvre d’autres formulaires.

6. Définissez les informations de protection.

Si vous n’avez pas indiqué de configuration de protection existante, un formulaire complémentaire s’affiche pour vous permettre de définir les utilisateurs autorisés à accéder aux documents ou aux répertoires correspondant au modèle de demande, ainsi que les actions autorisées.

- **Paramètres d’authentification du mot de passe**—Indiquez le fichier de mots de passe et/ou le fichier de groupes à utiliser pour la procédure d’authentification des utilisateurs. Indiquez aussi le nom utilisé pour identifier le serveur lorsqu’il invite à entrer le nom et le mot de passe du demandeur.

Remarque : Certains navigateurs placent les ID utilisateur et les mots de passe en mémoire cache et les associent à l’ID du serveur. Pour les utilisateurs, il est peut-être plus simple de définir toujours le même ID de serveur avec le même fichier de mots de passe.

- **Droits** — Indiquez les utilisateurs ou les groupes autorisés à lire et à supprimer des fichiers protégés ou à y entrer des données.

7. Cliquez sur **Validation**.

8. Redémarrez le serveur.

Utilisation des directives du fichier de configuration pour définir les informations de protection

Pour définir la protection en modifiant directement le fichier de configuration de Caching Proxy, vous devez prendre en compte les éléments suivants :

- Les différences entre les directives Protect, defProt et Protection
 - La directive Protect définit la protection en associant un modèle de demande à une configuration de protection. Pour plus d’informations, voir «Protect — Active une configuration de protection pour les demandes correspondant à un modèle», à la page 255.
 - La directive defProt définit une configuration de protection par défaut pour un modèle de demande spécifique. Pour plus d’informations, voir «DefProt — Spécifie la configuration de protection par défaut pour les demandes correspondant à un modèle», à la page 204.
 - La directive Protection permet de définir une configuration de protection nommée (existante). Pour plus d’informations, voir «Protection — Définit une configuration de protection nommée dans le fichier de configuration», à la page 260.

- Le mode d'interaction existant entre la protection et l'acheminement des demandes

Les directives d'acheminement des demandes, telles que **Map**, **Exec**, **Pass** et **Proxy** permettent de contrôler les demandes acceptées par le serveur, ainsi que leur mode de réacheminement vers les emplacements de fichiers réels. Les directives d'acheminement utilisent le même type de modèles de demandes que les directives de protection. Etant donné que les directives associées au premier modèle concordant sont exécutées pour chaque demande, vous devez répertorier les directives de protection avant les directives d'acheminement dans le fichier de configuration pour permettre le bon fonctionnement des mesures de protection. Pour plus d'informations, voir «Protect — Active une configuration de protection pour les demandes correspondant à un modèle», à la page 255.

- La différence entre la configuration de protection en ligne et la configuration de protection nommée

La directive Protect permet de définir une configuration de protection en ligne ou de se référer à une configuration existante (nommée). La syntaxe utilisée pour chaque type d'instruction est légèrement différente. Pour plus d'informations, voir «Protect — Active une configuration de protection pour les demandes correspondant à un modèle», à la page 255.

- Comment créer une configuration de protection

Une configuration de protection est une série d'instructions utilisant les sous-directives de protection. La syntaxe et les informations de référence sur la définition d'une configuration de protection se trouvent dans l'Annexe B, «Directives du fichier de configuration», à la page 175 ; voir les sections suivantes :

- «Protect — Active une configuration de protection pour les demandes correspondant à un modèle», à la page 255
- «Protection — Définit une configuration de protection nommée dans le fichier de configuration», à la page 260
- «Sous-directives de protection — Spécifie le mode de protection d'un ensemble de ressources», à la page 261

Paramètres de protection par défaut

Le fichier de configuration par défaut du serveur proxy comprend une configuration de protection requérant un ID et un mot de passe administrateur pour autoriser l'accès aux fichiers stockés dans le répertoire /admin-bin/. Ce paramètre limite l'accès aux formulaires de configuration et d'administration.

Chapitre 26. Secure Sockets Layer (SSL)

Le protocole SSL (Secure Sockets Layer) est un système permettant de chiffrer automatiquement les informations transmises sur Internet, puis de les déchiffrer avant de les utiliser. Cela permet de protéger les données confidentielles telles que les numéros de cartes de crédit lors de leur transmission via Internet.

Caching Proxy utilise le protocole SSL pour sécuriser les serveurs de remplacement et l'administration à distance, comme le décrivent les sections qui suivent. SSL peut être utilisé pour protéger les connexions aux serveurs dorsaux (par exemple, les serveurs de contenu ou d'applications) et pour sécuriser les communications entre le serveur proxy et les clients.

Pour les serveurs proxy d'acheminement, Caching Proxy prend en charge l'établissement de tunnels SSL qui contournent le protocole SSL et transmettent les données déjà chiffrées sans les modifier à nouveau.

Etablissement d'une liaison SSL

La protection SSL est appliquée lorsqu'un système envoie une demande de connexion sécurisée à un autre système ; par exemple, un navigateur envoie une demande à un serveur proxy de remplacement. La syntaxe de la demande `https://` au lieu de `http://` indique au navigateur que la demande doit être envoyée sur le port 443, utilisé par le serveur pour identifier les demandes de connexion sécurisées (à la place du port 80 pour les demandes de routine). Pour mettre en place une session sécurisée entre les deux systèmes, les deux machines établissent un échange, appelé *liaison SSL*, afin de convenir d'une spécification de chiffrement, puis choisissent une clé pour chiffrer et déchiffrer les informations. Les clés sont automatiquement générées. Elles arrivent à expiration en même temps que la session. Le scénario classique (avec SSL version 3) se déroule de la manière suivante :

1. Contact du client

Le client établit une session SSL avec Caching Proxy en envoyant un message Client Hello décrivant ses capacités de chiffrement.

2. Contact du serveur

Le serveur envoie son certificat au client et sélectionne un algorithme de cryptographie pour effectuer le chiffrement des données.

3. Fin du client

Le client envoie des informations permettant de créer des clés de chiffrement symétriques pour les données chiffrées. Ces informations sont appelées *secret maître* et sont chiffrées à l'aide de la clé publique du serveur (obtenue à partir du certificat du serveur). Voir «Gestion des clés et des certificats», à la page 121. Le serveur et le client peuvent définir les clés de chiffrement symétriques pour la lecture et l'écriture à partir du "secret maître".

4. Fin du serveur

Le serveur envoie la confirmation finale et un code d'authentification du message (MAC) pour l'ensemble du protocole de liaison.

5. Validation du client

Le client envoie un message de validation du message de fin du serveur.

6. Flux de données sécurisées

Si le client valide le message de fin du serveur, la transmission des données chiffrées peut commencer.

Lors de connexions sécurisées, l'utilisation de Caching Proxy sous la forme d'un noeud final permet de réduire la charge de traitement des serveurs de contenu ou d'applications. Quand Caching Proxy gère une connexion sécurisée, il effectue des opérations de traitement particulièrement lourdes (chiffrement, déchiffrement, création de clés). Il permet également de configurer les délais d'expiration de la session SSL pour optimiser l'utilisation de chaque clé.

Limites du protocole SSL

Le protocole SSL présente les limites suivantes dans Caching Proxy de WebSphere Application Server :

- Caching Proxy ne peut pas être utilisé comme autorité de certification (voir «Gestion des clés et des certificats», à la page 121).
- Il est possible que certains navigateurs ne prennent pas en charge toutes les technologies de chiffrement utilisées par Caching Proxy.

Réglage des performances SSL

En présence de volumes de trafic HTTPS élevés, le serveur Caching Proxy peut entraîner une utilisation intensive de la CPU. Vous pouvez aider le serveur proxy à gérer la charge et réduire l'utilisation de la CPU en modifiant la variable d'environnement (`GSK_V3_SIDCACHE_SIZE`).

L'ID de session SSL identifie les sessions SSL réutilisables, y compris les clés de chiffrement et de déchiffrement utilisées par les navigateurs et les serveurs, et permet d'éviter les établissements de liaison SSL inutiles sur les nouvelles connexions, qui sont de gros consommateurs de temps CPU du serveur. La bibliothèque GSKit du serveur Caching Proxy prend en charge l'ID de session SSL et contient un cache d'ID de session SSL. Par défaut, le cache de l'ID de session SSL contient 512 entrées. A la saturation de limite des entrées, l'entrée de session la plus ancienne est supprimée et la nouvelle entrée est ajoutée dans le cache.

Servez-vous de la variable d'environnement `GSK_V3_SIDCACHE_SIZE` pour modifier la taille par défaut du cache d'ID de session SSL. Les valeurs correctes pour la variable sont comprises entre 1 et 4096. Augmenter la taille augmente le temps de consultation requis pour localiser une session SSL mise en cache. Toutefois, cette augmentation de temps est insignifiante par rapport au temps système requis pour établir une connexion SSL. Augmenter la taille du cache permet au serveur proxy de gérer un plus grand nombre de sessions SSL simultanées tout en réduisant l'utilisation de la CPU lorsque le serveur proxy est soumis à des charges HTTPS élevées.

Caching Proxy dispose également d'une directive ajustable `SSLV3Timeout`. (Voir «`SSLV3Timeout` — Indique le délai d'inactivité au-delà duquel une session `SSLV3` expire», à la page 285.) La valeur par défaut de la directive est 1000 secondes. Cette directive définit la durée de vie d'une session SSL dans le cache des sessions. Si aucune connexion SSL entrante n'utilise de session SSL existante et que la durée de vie de la session dépasse la valeur, cette session est supprimée du cache. Il est recommandé de choisir comme valeur `SSLV3Timeout` la longueur d'une session client sécurisée classique. Si le délai d'attente défini est trop court, les performances du proxy risquent d'être ralenties car plusieurs sessions

d'établissement de liaison SSL sont nécessaires pour une seule session sécurisée. En revanche, si la valeur définie est trop longue, la sécurité d'une session sécurisée peut s'en trouver compromise.

Etablissement de tunnels SSL

S'applique aux configurations avec proxy d'acheminement uniquement.

Lorsque Caching Proxy est configuré comme serveur proxy d'acheminement, il utilise la fonction de création de tunnels SSL pour prendre en charge les connexions sécurisées entre les clients et les serveurs de données. Lors de l'établissement des tunnels SSL, les données chiffrées sont transmises telles quelles via le serveur proxy. Comme le serveur proxy ne déchiffre pas les données, les fonctions demandant au serveur proxy de lire les demandes ou les en-têtes de documents ne sont pas prises en charge. Les demandes traitées via les tunnels SSL ne sont pas mises en mémoire cache.

La figure 2 décrit le mode d'établissement d'une connexion via des tunnels SSL.

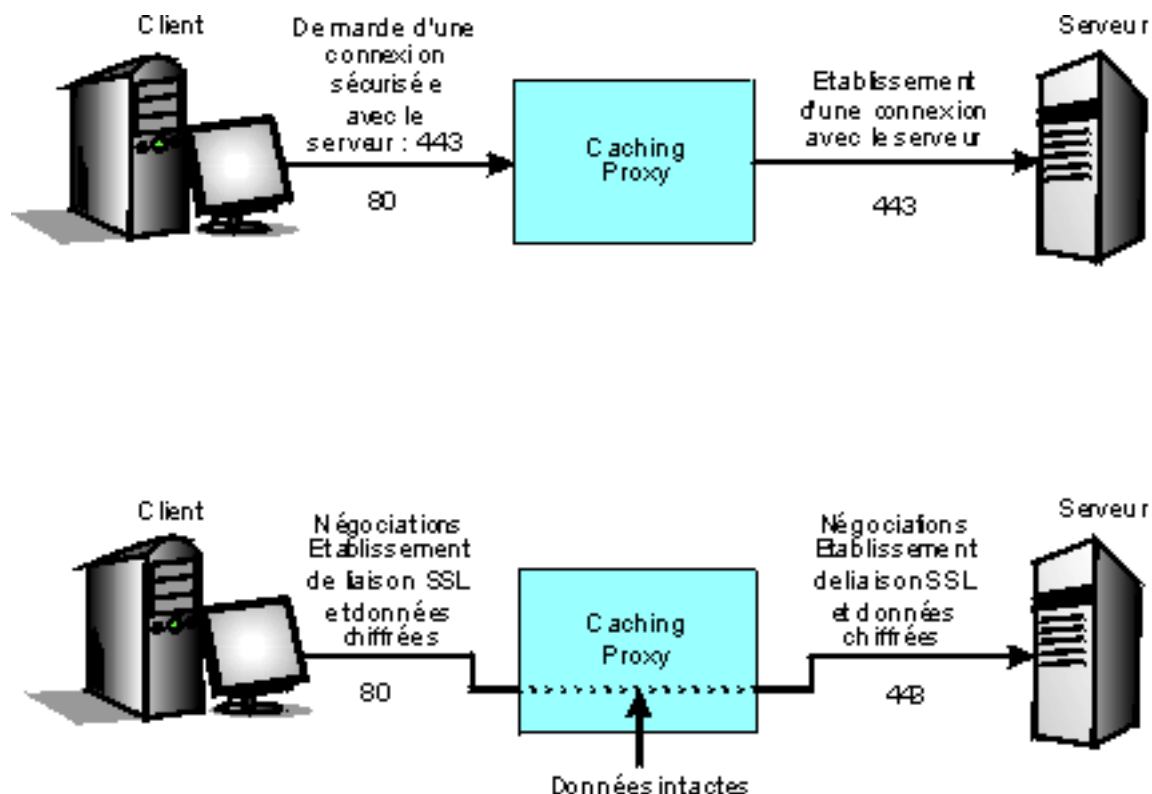


Figure 2. Etablissement de tunnels SSL

Le processus d'établissement de tunnels SSL se déroule de la manière suivante :

1. Le client fait une demande d'établissement de tunnel : `CONNECT nom_hôte-serveur:port HTTP/1.1` (ou `HTTP/1.0`). Le numéro de port est facultatif. En règle générale, il s'agit du port 443. Le navigateur client envoie automatiquement la demande `CONNECT` d'abord au serveur proxy pour chaque demande `HTTPS` si le serveur proxy d'acheminement est configuré dans le navigateur.

2. Le serveur proxy accepte la connexion sur le port 80, reçoit la demande et se connecte au serveur de destination sur le port demandé par le client.
3. Le serveur proxy indique au client que la connexion est établie.
4. Le proxy sert de relais aux messages d'établissement de liaison SSL dans les deux directions : du client vers le serveur de destination, et de ce dernier vers le client.
5. Une fois la liaison sécurisée établie, le proxy envoie et reçoit les données chiffrées qui seront déchiffrées sur le client ou sur le serveur de destination.
6. Si le client ou le serveur de destination demande la fermeture de la session sur l'un des ports, le serveur proxy arrête les deux connexions (sur les ports 443 et 80) et reprend ses activités habituelles.

Configuration de l'établissement des tunnels SSL

Lors de la configuration d'un serveur proxy d'acheminement, seule la fonction d'établissement des tunnels SSL est disponible. Pour configurer les paramètres des tunnels dans les formulaires de configuration et d'administration, sélectionnez **Configuration du proxy** → **Paramètres du proxy**. Cochez la case **Etablissement de tunnels**.

La méthode CONNECT (désactivée par défaut) doit également être activée pour les connexions utilisant les tunnels SSL. Pour l'activer avec les formulaires de configuration, sélectionnez **Configuration du serveur** → **Traitement des demandes** et utilisez le formulaire **Méthodes HTTP**.

Trois options (OutgoingPorts, OutgoingIPs, IncomingIPs) sont fournies pour la directive Enable CONNECT pour une meilleure sécurité lors de l'établissement de tunnels SSL. Vous devez indiquer une valeur pour OutgoingPorts au moins, sinon, la méthode CONNECT n'est pas activée.

- OutgoingPorts (pour limiter l'accès à l'établissement de tunnels SSL par les ports du serveur distant). Le format de la directive est
Enable CONNECT OutgoingPorts [all | [port1|port1-port2|port1-*],...]

Pour permettre aux clients de se connecter uniquement au port 443 des serveurs distants pour l'établissement de tunnels SSL, définissez les directives suivantes. (Le port 443 est normalement réservé aux demandes HTTPS sur le serveur distant.)

```
Enable CONNECT OutgoingPorts 443
SSLTunneling on
```

Pour permettre aux clients de se connecter à n'importe quel port sur les serveurs distants pour l'établissement de tunnels SSL, définissez les directives suivantes:

```
Enable CONNECT OutgoingPorts all
SSLTunneling on
```

Pour permettre aux clients de se connecter aux ports 80, 8080-8088, 9000 et suivants sur les serveurs distants pour l'établissement de tunnels SSL, définissez les directives suivantes:

```
Enable CONNECT OutgoingPorts 80,8080-8088,9000-*
SSLTunneling on
```

Séparez les numéros de ports et séries de ports par une virgule, sans ménager d'espace.

IMPORTANT : Pour les configurations avec serveur proxy d'acheminement, spécifiez au moins 443 ou all avec l'option OutgoingPorts pour activer l'établissements de tunnels SSL normal.

- OutgoingIPs (pour limiter l'accès à l'établissement de tunnels SSL via l'adresse IP de serveur distant). Le format de la directive est
Enable CONNECT OutgoingIPs [[!]modèle_IP,...]

Par exemple, pour permettre aux clients de se connecter à n'importe quel port sur les serveurs distants correspondant à l'adresse IP/au nom d'hôte *.ibm.com et ne devant pas correspondre à 192.168.*.*, définissez les directives suivantes :

```
Enable CONNECT OutgoingPorts all OutgoingIPs *.ibm.com,!192.168.*.*
SSLTunneling on
```

Remarque : Séparez les modèles IP par une virgule, sans ménager d'espace.

- IncomingIPs (pour limiter l'accès à l'établissement de tunnels SSL via l'adresse IP du client). Le format de la directive est
Enable CONNECT IncomingIPs [[!]modèle_IP,...]

Par exemple, pour permettre aux clients provenant de l'adresse IP 192.168.*.* de se connecter à n'importe quel port sur les serveurs distants pour l'établissement de tunnels SSL, définissez les directives suivantes :

```
Enable CONNECT OutgoingPorts all IncomingIPs 192.168.*.*
SSLTunneling on
```

Remarques :

1. Si l'on considère que 192.168.*.* est le masque d'IP réseau LAN interne, l'option ci-dessus autorise uniquement les utilisateurs internes à utiliser la méthode de connexion et la fonction d'établissement de tunnels SSL.
2. Séparez les modèles IP par une virgule, sans ménager d'espace.

Pour plus d'informations sur l'activation de la fonction d'établissement des tunnels SSL et les directives CONNECT en modifiant le fichier de configuration du proxy, voir les sections de référence dans l'Annexe B, «Directives du fichier de configuration», à la page 175 pour les directives suivantes :

- «Enable — Active les méthodes HTTP», à la page 212
- «SSLTunneling — Active l'établissement de tunnels SSL», à la page 284

Configuration de l'administration à distance sécurisée

Vous pouvez administrer à distance Caching Proxy en utilisant les fonctions de sécurité proposées par le protocole SSL (Secure Sockets Layer) et l'authentification du mot de passe. Cette fonction permet de réduire fortement le risque d'accès au serveur proxy par des personnes non autorisées.

Pour utiliser le protocole SSL lors de l'administration à distance du serveur, lancez une demande https:// et non une demande http:// pour ouvrir les formulaires de configuration et d'administration. Par exemple :

```
https://nom.serveur/pagedegarde.html
```

Gestion des clés et des certificats

Comme indiqué précédemment, avant de configurer le protocole SSL, vous devez définir une base de données de clés et vous procurer un certificat. Les certificats permettent d'authentifier l'identité du serveur. Vous devez lancer l'utilitaire IBM Key Management (appelé parfois iKeyman) pour définir les fichiers de

configuration. Cet utilitaire fait partie du logiciel GSKit, compris dans Application Server. GSKit est également doté d'une interface graphique Java qui permet d'ouvrir les fichiers de certificats.

Vous trouverez ci-après les instructions à suivre pour configurer des clés et des certificats SSL.

1. Vérifiez que GSKit est installé. Sur la plupart des plateformes, ce programme est installé automatiquement avec le composant Caching Proxy. Le nom du package est gsk7ikm (gsk7ikm_gcc295 sur les systèmes Linux pour i386). Le GSKit est généralement installé dans le répertoire `ibm/gsk7/` (`ibm/gskit/` sur les systèmes AIX). Sur les plateformes Windows, il est aussi accessible à partir du menu **Démarrer**.

Remarque : Sous Windows, si l'installation de GSKit échoue lorsque vous utilisez InstallShield, vérifiez que le chemin du répertoire sur le support d'installation comporte un espace.

2. Utilisez le gestionnaire de clés pour créer une clé permettant d'établir des communications réseau sécurisées et pour recevoir un certificat de l'autorité de certification. Vous pouvez décider de créer un certificat d'auto-signature en attendant de recevoir le certificat de l'autorité.
3. Créez une base de données de clés et définissez le mot de passe associé.

Remarque : Les fichiers key et keystack sont désinstallés chaque fois que Caching Proxy est désinstallé. Pour éviter d'avoir à demander un nouveau certificat à l'autorité de certification, faites des copies de sauvegarde de ces deux fichiers dans un autre répertoire avant de désinstaller le logiciel proxy.

Pour tous les systèmes d'exploitation à l'exception de Linux, si le certificat a expiré, Caching Proxy ne démarre pas correctement et un message d'erreur s'affiche pour indiquer que la base de données de clés a expiré. Sous Linux, le proxy semble avoir démarré mais le processus disparaît rapidement et aucun message d'erreur n'est généré.

Pour éviter cet incident sur les systèmes Red Hat Enterprise Linux 3.0, assurez-vous que les packages GCC ont au moins le niveau suivant :

- libstdc++-3.2.3-52
- libgcc-3.2.3-52

Autorités de certification

La clé publique doit être associée à un certificat doté d'une signature numérique et émis par une autorité de certification (CA) reconnue sur le serveur. Vous pouvez vous procurer un certificat signé en soumettant une demande à une autorité de certification (CA). Caching Proxy accepte les autorités de certification externes suivantes :

- VeriSign
- Thawte

Par défaut, les autorités de certification suivantes sont considérées comme sécurisées :

- Verisign Class 1 Individual Subscriber CA - Persona Not Validated
- Verisign Class 2 Individual Subscriber CA - Persona Not Validated

- Verisign Class 3 Individual Subscriber CA - Persona Not Validated
- Verisign Class 3 International Server CA
- Verisign Class 2 OnSite Individual CA
- Verisign Class 1 Public Primary CA
- Verisign Class 2 Public Primary CA
- Verisign Class 3 Public Primary CA
- Verisign Class 1 Public Primary CA - G2
- Verisign Class 2 Public Primary CA - G2
- RSA Secure Server CA (Verisign)
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA

Utilitaire IBM Key Manager

Cette section constitue un guide de référence d'utilisation de l'utilitaire IBM Key Manager (iKeyman). Utilisez le gestionnaire de clés pour créer une base de données de clés SSL, des paires de clés publiques et privées et une demande de certificat. Une fois que vous avez reçu le certificat signé par l'autorité de certification, vous pouvez utiliser le gestionnaire de clés pour placer le certificat dans la base de données de clés où la demande de certificat initiale a été créée.

Une documentation détaillée sur les programmes IBM Key Manager et GSKit est fournie avec le logiciel GSKit.

Configuration du système pour exécuter le gestionnaire de clés

Avant de lancer l'interface graphique utilisateur IKeyman, procédez aux opérations ci-dessous.

1. Installez IBM Java 2 Technology, version 1.4.2 32 bits ou une technologie Java 2 équivalente.
2. Définissez JAVA_HOME en indiquant l'emplacement du répertoire Java. Par exemple :
 - Windows : set JAVA_HOME=C:\Program Files\IBM\Java142
 - Linux et UNIX : export JAVA_HOME=/usr/opt/IBMJava2-142
3. Supprimez les fichiers ibmjsse.jar, gskikm.jar (le cas échéant) et ibmjcaprovider.jar du répertoire JAVA_HOME/jre/lib/ext.

Remarques :

- a. Pour Solaris, remplacez le répertoire JAVA_HOME/jre/lib/ext par JAVA_HOME/lib/ext/.
 - b. Ne déplacez ni supprimez les fichiers JAR d'un JDK dont dépend un autre produit (par exemple, WebSphere Application Server). En effet, ce type d'opération risque d'empêcher le bon fonctionnement du produit dépendant. Si vous ne savez pas si le JDK est en cours d'utilisation, installez-en un autre pour l'utilitaire IBM Key Management.
4. Tous les fichiers JAR ci-dessous se trouvent dans le répertoire *chemin_installation_GSKit/classes/jre/lib/ext/*.
 - Copiez les fichiers JAR indiqués dans le répertoire JAVA_HOME/jre/lib/

- ```
ibmjcefw.jar
ibmpkcs11.jar
```
- Copiez les fichiers JAR indiqués dans JAVA\_HOME/jre/lib/ext
 

```
ibmjceprovider.jar
ibmpkcs.jar
```
  - Copiez les fichiers JAR indiqués dans le répertoire JAVA\_HOME/jre/lib/security
 

```
local_policy.jar
US_export_policy.jar
```
5. Enregistrez les fournisseurs de services IBM JCE, IBM CMS, et/ou IBMJCEFIPS :
- Mettez à jour le fichier JAVA\_HOME/jre/lib/security/java.security en ajoutant les fournisseurs IBM CMS et IBM JCE après le fournisseur Sun. Par exemple :
- ```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.spi.IBMCMSProvider
security.provider.3=com.ibm.crypto.provider.IBMJCE
```
- Un exemple de fichier java.security se trouve dans *chemin_installation_GSKit/classes/gsk_java.security*.
- Pour activer la fonction FIPS, mettez à jour le fichier JAVA_HOME/jre/lib/security/java.security pour ajouter IBMJCEFIPS après le fournisseur Sun. Vérifiez que le fournisseur IBMJCEFIPS a été enregistré avec une priorité plus élevée que le fournisseur IBMJCE. Par exemple :
- ```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.spi.IBMCMSProvider
security.provider.3=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.4=com.ibm.crypto.provider.IBMJCE
```
6. (Facultatif) Si vous êtes un utilisateur JSSE et que vous utilisez JSSE pour accéder au matériel cryptographique, installez le fichier ibmpkcs11.jar dans le répertoire JAVA\_HOME/jre/lib et suivez les instructions figurant dans le fichier *chemin\_installation\_GSKit/classes/native/native-support.zip* pour configurer les bibliothèques partagées du matériel cryptographique.

**Remarque :** Le fichier ibmpkcs11.jar se trouve également dans le package JSSE livré après le 5 août 2002. Voici un exemple de mise à jour du fichier JAVA\_HOME/jre/lib/security/java.security, pour l'enregistrement d'un fournisseur de services IBMPKCS11 :

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.crypto.pkcs11.provider.IBMPKCS11
```

### Lancement du gestionnaire de clés

Lancez l'interface graphique du gestionnaire de clés en procédant comme suit :

- Sous Linux et UNIX, entrez `gsk7ikm` à partir de l'invite de commande.
- Sur les plateformes Windows, sélectionnez **Démarrer -> Programmes -> IBM WebSphere -> Edge Components -> Caching Proxy -> Démarrer l'utilitaire de gestion des clés**.

Si vous créez un fichier de la base de données de clés au cours de cette session, le fichier est stocké dans le répertoire à partir duquel le gestionnaire de clés a été lancé.

## Création d'un fichier de stockage, de mots de passe et d'une base de données de clés

La base de données de clés est un fichier utilisé par le serveur pour stocker des certificats et une ou plusieurs paires de clés. Vous pouvez utiliser une base de données de clés pour toutes les paires de clés et les certificats, ou créer plusieurs bases de données. L'utilitaire de gestion des clés permet de créer des bases de données et de définir leurs mots de passe et leurs fichiers de stockage.

Pour créer une base de données de clés et un fichier de stockage, procédez comme suit :

1. Lancez l'utilitaire de gestion des clés.
2. Dans le menu principal, sélectionnez **Fichier de base de données de clés -> Nouveau**.
3. Dans la boîte de dialogue **Nouveau**, vérifiez que le type de fichier **Fichier de base de données de clés CMS** est sélectionné. Saisissez le nom de la base de données de clés, ainsi que son chemin d'accès. Vous pouvez également accepter la valeur par défaut **key.kdb**. Cliquez sur **OK**.
4. Dans la boîte de dialogue **Invite du mot de passe**, saisissez le mot de passe de la base de données, puis confirmez-le. Cliquez sur **OK**.
5. Cochez la case permettant de stocker le fichier de mots de passe. A l'invite du programme, saisissez et confirmez le mot de passe pour vérification. Le message suivant s'affiche : DB-Type: CMS key database file  
*nom\_base\_fichierclés*

**Remarque :** Si vous ne stockez pas le fichier de mots de passe, le serveur démarre mais il n'écoute pas le port 443.

Le mot de passe défini lors de la création de la base de données permet de protéger la clé privée. La clé privée est la seule clé disponible pour signer des documents ou déchiffrer des messages chiffrés à l'aide de la clé publique.

Lors de la définition du mot de passe, respectez les instructions suivantes :

- Vous devez utiliser le jeu de caractères anglais (Etats-Unis).
- Le mot de passe doit comporter au moins 6 caractères, ainsi que deux chiffres qui ne se suivent pas. Assurez-vous que le mot de passe ne correspond pas à des données personnelles que l'on peut facilement se procurer, comme votre nom, le nom des membres de votre famille, vos initiales ou votre date de naissance.
- Stockez le mot de passe.

Il est bon de redéfinir fréquemment le mot de passe de la base de données de clés. Toutefois, si vous définissez une date d'expiration du mot de passe, n'oubliez pas de noter la date à laquelle il doit être changé. Si le mot de passe arrive à expiration avant que vous ne le redéfinissiez, un message est consigné dans le journal ; le serveur démarre mais il ne peut pas établir de connexions réseau sécurisées.

Pour changer le mot de passe de la base de données de clés, effectuez les opérations suivantes :

1. Dans le menu principal, cliquez sur **Fichier de base de données de clés -> Ouverture**.
2. Dans la boîte de dialogue **Ouverture**, saisissez le nom de la base de données de clés ou acceptez la valeur par défaut, **key.kdb**. Cliquez sur **OK**.

3. Dans la boîte de dialogue **Invite du mot de passe**, saisissez votre mot de passe défini et cliquez sur **OK**.
4. Dans le menu principal, cliquez sur **Fichier de base de données de clés -> Modification du mot de passe**.
5. Dans la boîte de dialogue **Modification du mot de passe**, saisissez un nouveau mot de passe puis confirmez-le. Cliquez sur **OK**.

Pour établir une connexion SSL entre un serveur proxy et un serveur LDAP, placez le mot de passe de la base de données de clés dans le fichier `pac_keyring.pwd`. (Le fichier `pac_keyring.pwd` n'est pas un fichier de dissimulation généré par IKeyMan.)

### Création d'une paire de clés et d'une demande de certificat

La base de données stocke des paires de clés et des demandes de certificats. Pour créer une paire de clés publique-privée, procédez comme suit :

1. Si vous n'avez pas encore créé de base de données de clés, suivez les instructions indiquées à la section «Création d'un fichier de stockage, de mots de passe et d'une base de données de clés», à la page 125.
2. Dans le menu principal de l'utilitaire de gestion des clés, cliquez sur **Base de données de clés -> Fichier -> Ouverture**.
3. Dans la boîte de dialogue **Ouverture**, saisissez le nom de la base de données de clés (ou cliquez sur **key.kdb** si vous utilisez la valeur par défaut). Cliquez sur **OK**.
4. Dans la boîte de dialogue **Invite du mot de passe**, saisissez votre mot de passe et cliquez sur **OK**.
5. Dans le menu principal, cliquez sur **Création -> Nouvelle demande de certificat**.
6. Dans la boîte de dialogue **Création d'une clé et d'une demande de certificat**, indiquez les éléments suivants :
  - **Label de la clé** : Entrez un nom (libellé) utilisé pour identifier la clé et le certificat dans la base de données : par exemple, `mon certificat d'auto-signature` ou `www.companyA.com`.
  - **Taille de la clé** : Taille de la clé, par exemple, 1024. (Pour bénéficier des avantages du chiffrement 128 bits, une taille de clé de 1024 est conseillée.)
  - **Nom de l'organisation** : Nom de l'organisation à associer à la clé, par exemple Société A.
  - **Service de la société** (facultatif)
  - **Localité** (facultatif)
  - **Département** (facultatif)
  - **Code postal** (facultatif)
  - **Pays** : Code du pays. Vous devez indiquer au moins deux caractères, par exemple US.
  - **Nom du fichier de demande** : Entrez le nom du fichier destiné à stocker la demande de certificat. Vous pouvez éventuellement spécifier un nom par défaut.
7. Cliquez sur **OK**. Un message de confirmation s'affiche :
 

```
Une
demande de certificat a été créée
dans le fichier nom_base_fichier_clés.
```

8. Cliquez sur **OK**. Attendez que le libellé s'affiche sous le titre **Demandes de certificats personnels**.
9. Dans la boîte de dialogue **Informations**, cliquez sur **OK**. Le programme vous rappellera que vous devez envoyer le fichier à une autorité de certification.
10. Si vous n'avez pas créé de certificat d'auto-signature (voir la section "Création d'un certificat d'auto-signature"), envoyez la demande de certificat à une autorité de certification :
  - Laissez le gestionnaire de clés ouvert.
  - Lancez un navigateur Web et entrez l'adresse URL de l'autorité de certification qui doit vous délivrer le certificat.
  - Suivez les instructions fournies par l'autorité de certification pour envoyer la demande de certificat.

Il faut parfois attendre deux à trois mois avant que la demande de certificat ne soit satisfaite. En attendant que l'autorité de certification traite votre demande, vous pouvez jouer le rôle de votre propre autorité de certification et utiliser iKeyman pour créer un certificat d'auto-signature et activer des sessions SSL entre les clients et Caching Proxy.

### Création d'un certificat d'auto-signature

En attendant, vous pouvez lancer l'utilitaire de gestion des clés pour créer un certificat d'auto-signature et activer des sessions SSL entre les clients et le serveur proxy. Vous pouvez également utiliser des certificats d'auto-signature à des fins de test.

Pour créer un certificat d'auto-signature, procédez comme suit :

1. Si vous n'avez pas encore créé de base de données de clés, suivez les instructions indiquées à la section «Création d'un fichier de stockage, de mots de passe et d'une base de données de clés», à la page 125.
2. Dans le menu principal de l'utilitaire de gestion des clés, cliquez sur **Base de données de clés → Fichier → Ouverture**.
3. Dans la boîte de dialogue **Ouverture**, entrez le nom de la base de données de clés (ou acceptez la valeur par défaut, **key.kdb**). Cliquez sur **OK**.
4. Dans la boîte de dialogue **Invite du mot de passe**, saisissez votre mot de passe et cliquez sur **OK**.
5. Dans le cadre **Contenu de la base de données de clés**, sélectionnez **Certificats personnels** et cliquez sur le bouton **Nouveau certificat auto-signé**.
6. Dans la fenêtre **Création d'un certificat auto-signé**, indiquez les éléments suivants :
  - **Label de la clé** : Entrez un nom (libellé) utilisé pour identifier la clé et le certificat dans la base de données ; par exemple, mon certificat d'auto-signature
  - **Taille de la clé** : Taille de la clé, par exemple 512.
  - **Nom courant** : Nom d'hôte complet du serveur, par exemple, `www.monserveur.com`
  - **Société** : Nom de l'organisation à associer à la clé, par exemple Société A
  - **Service de la société** (facultatif)
  - **Localité** (facultatif)
  - **Département** (facultatif)
  - **Code postal** (facultatif)



- **Pays** : Code du pays. Vous devez indiquer au moins deux caractères, par exemple US.
  - **Période de validité** : Période de validité du certificat.
7. Cliquez sur **OK**.
  8. Enregistrez la base de données de clés sur le serveur en ajoutant les fichiers de clés et de stockage aux paramètres de configuration (voir «Création d'un fichier de stockage, de mots de passe et d'une base de données de clés», à la page 125).

### Exportation des clés

Pour exporter des clés dans une autre base de données, procédez comme suit :

1. Lancez l'utilitaire de gestion des clés.
2. Dans le menu principal, cliquez sur **Fichier de base de données de clés -> Ouverture**.
3. Dans la boîte de dialogue **Ouverture**, entrez le nom de la base de données de clés (ou acceptez la valeur par défaut, **key.kdb**). Cliquez sur **OK**.
4. Dans la boîte de dialogue **Invite du mot de passe**, saisissez votre mot de passe et cliquez sur **OK**.
5. Dans le cadre **Contenu de la base de données de clés**, sélectionnez **Certificats personnels**, puis cliquez sur le bouton **Exportation/Importation** sur le libellé.
6. Dans la fenêtre **Exportation/Importation de clés** :
  - Sélectionnez **Exportation de clés**.
  - Sélectionnez le type de la base de données cible (par exemple, **PKCS12**).
  - Saisissez le nom du fichier ou cliquez sur **Parcourir** pour le sélectionner.
  - Saisissez l'emplacement.
7. Cliquez sur **OK**.
8. Dans la boîte de dialogue **Invite du mot de passe**, saisissez le mot de passe approprié, indiquez-le une nouvelle fois pour confirmation, puis cliquez sur **OK** pour exporter la clé sélectionnée dans une autre base de données.

### Importation des clés

Pour importer des clés à partir d'une autre base de données, procédez comme suit :

1. Lancez l'utilitaire de gestion des clés.
2. Dans le menu principal, sélectionnez **Fichier de base de données de clés -> Ouverture**.
3. Dans la boîte de dialogue **Ouverture**, entrez le nom de la base de données de clés (ou acceptez la valeur par défaut, **key.kdb**). Cliquez sur **OK**.
4. Dans la boîte de dialogue **Invite du mot de passe**, saisissez votre mot de passe et cliquez sur **OK**.
5. Dans le cadre **Contenu de la base de données de clés**, sélectionnez **Certificats personnels**, puis cliquez sur le bouton **Exportation/Importation** sur le libellé.
6. Dans la fenêtre **Exportation/Importation de clés** :
  - Sélectionnez **Importation de clés**.
  - Sélectionnez le type de la base de données (par ex., **PKCS12**)
  - Saisissez le nom du fichier ou cliquez sur **Parcourir** pour le sélectionner.
  - Sélectionnez l'emplacement.



7. Cliquez sur **OK**.
8. Dans la boîte de dialogue **Invite du mot de passe**, saisissez votre mot de passe et cliquez sur **OK**.
9. Dans la liste **Sélection dans la liste de labels de clés du fichier**, sélectionnez le libellé approprié et cliquez sur **OK**.

### Affichage des autorités de certification

Pour afficher la liste des autorités de certification reconnues (CA) dans la base de données de clés :

1. Lancez l'utilitaire de gestion des clés.
2. Dans le menu principal, cliquez sur **Fichier de base de données de clés -> Ouverture**.
3. Dans la boîte de dialogue **Ouverture**, entrez le nom de la base de données de clés (ou acceptez la valeur par défaut, **key.kdb**). Cliquez sur **OK**.
4. Dans la boîte de dialogue **Invite du mot de passe**, saisissez votre mot de passe et cliquez sur **OK**.
5. Dans le cadre **Contenu de la base de données de clés**, sélectionnez **Certificats signataires**.
6. Cliquez sur **Certificats signataires**, **Certificats personnels** ou **Demandes de certificats** pour afficher la liste des autorités d'accréditation dans la fenêtre **Données de clé**.

## Réception d'un certificat signé par une autorité de certification

Suivez la procédure ci-après pour recevoir un certificat adressé par courrier électronique par une autorité de certification (AC) considérée comme sécurisée par défaut (voir la liste de la section «Autorités de certification», à la page 122). Si l'autorité émettrice du certificat signé n'est pas considérée comme une autorité sécurisée dans la base de données, vous devez d'abord stocker le certificat et définir l'autorité comme une entité sécurisée. Vous pouvez ensuite recevoir le certificat signé par l'autorité dans la base de données. Vous ne pouvez pas recevoir le certificat signé d'une autorité qui n'est pas considérée comme sécurisée (voir la section «Stockage d'un certificat signé par une autorité de certification», à la page 130).

Pour recevoir un certificat signé dans la base de données, procédez comme suit :

1. Lancez l'utilitaire de gestion des clés.
2. Dans le menu principal, sélectionnez **Fichier de base de données de clés -> Ouverture**.
3. Dans la boîte de dialogue **Ouverture**, entrez le nom de la base de données de clés (ou acceptez la valeur par défaut, **key.kdb**). Cliquez sur **OK**.
4. Dans la boîte de dialogue **Invite du mot de passe**, saisissez votre mot de passe et cliquez sur **OK**.
5. Vérifiez que le nom du fichier est correct dans la liste des types de fichiers de base de données.
6. Dans le cadre **Contenu de la base de données de clés**, sélectionnez **Certificats personnels** puis cliquez sur le bouton **Réception**.
7. Dans la boîte de dialogue **Réception d'un certificat provenant d'un fichier**, saisissez le nom d'un fichier valide codé à 64 bits dans la zone **Nom du fichier de certificat**. Cliquez sur **OK**.

8. Pour fermer l'utilitaire de gestion des clés, cliquez, dans le menu principal, sur **Base de données de clés -> Quitter**.

## Stockage d'un certificat signé par une autorité de certification

Seuls les certificats signés par des autorités agréées sont acceptés pour l'établissement de connexions sécurisées. Pour ajouter une autorité de certification à la liste des autorités agréées (sécurisées), vous devez vous procurer son certificat et le stocker en indiquant qu'il s'agit d'un certificat sécurisé. Pour stocker un certificat émis par une nouvelle autorité, procédez comme suit avant de l'enregistrer dans la base de données :

1. Lancez l'utilitaire de gestion des clés.
2. Dans le menu principal, cliquez sur **Fichier de base de données de clés -> Ouverture**.
3. Dans la boîte de dialogue **Ouverture**, entrez le nom de la base de données de clés (ou acceptez la valeur par défaut, **key.kdb**). Cliquez sur **OK**.
4. Dans la boîte de dialogue **Invite du mot de passe**, saisissez votre mot de passe et cliquez sur **OK**.
5. Dans le cadre **Contenu de la base de données de clés**, sélectionnez **Certificats signataires** puis cliquez sur le bouton **Ajout**.
6. Dans la boîte de dialogue **Ajout d'un certificat d'AC provenant d'un fichier**, sélectionnez le nom du fichier ASCII codé à 64 bits ou utilisez l'option **Survol**. Cliquez sur **OK**.
7. Dans la boîte de dialogue **Saisie d'un label**, entrez un nom de libellé puis cliquez sur **OK**.
8. Cochez la case appropriée pour indiquer que le certificat est sécurisé (par défaut).

**Remarque :** Visualisez la case à cocher *après* la création du certificat en cliquant sur le bouton d'affichage et d'édition. La case à cocher est répertoriée dans le panneau mais ne s'affiche pas lors de l'ajout du certificat.

## Affichage de la clé par défaut dans la base de données

Affichez l'entrée de clé par défaut comme suit :

1. Lancez l'utilitaire de gestion des clés.
2. Dans le menu principal, cliquez sur **Fichier de base de données de clés -> Ouverture**.
3. Dans la boîte de dialogue **Ouverture**, entrez le nom de la base de données de clés (ou acceptez la valeur par défaut, **key.kdb**). Cliquez sur **OK**.
4. Dans la boîte de dialogue **Invite du mot de passe**, saisissez votre mot de passe et cliquez sur **OK**.
5. Dans le cadre **Contenu de la base de données de clés**, sélectionnez **Certificats personnels** et le libellé du certificat d'AC.
6. Dans la fenêtre **Données de clé**, cliquez sur **Affichage/Édition** pour afficher les informations de la clé par défaut du certificat.

---

## Spécifications de chiffrement autorisées

Les algorithmes de chiffrement et les modules de hachage utilisés par SSL versions 2 et 3 sont répertoriés dans les tableaux ci-après :

Génération de paires de clés : Tailles des clés privées RSA 512–1024

### SSL version 2

| Version utilisée aux Etats-Unis | Version utilisée dans les autres pays |
|---------------------------------|---------------------------------------|
| RC4 US                          | RC4 Export                            |
| RC2 US                          | RC2 Export                            |
| DES 56 bits                     | <i>non applicable</i>                 |
| Triple DES US                   | <i>non applicable</i>                 |
| RC4 Export                      | <i>non applicable</i>                 |
| RC2 Export                      | <i>non applicable</i>                 |

### SSL version 3

| Version utilisée aux Etats-Unis | Version utilisée dans les autres pays |
|---------------------------------|---------------------------------------|
| Triple DES SHA US               | DES SHA Export                        |
| DES SHA Export                  | RC2 MD5 Export                        |
| RC2 MD5 Export                  | RC4 MD5 Export                        |
| RC4 SHA US                      | NULL SHA                              |
| RC4 MD5 US                      | NULL MD5                              |
| RC4 MD5 Export                  | NULL NULL                             |
| RC4 SHA 56 bits                 | <i>non applicable</i>                 |
| DES CBC SHA                     | <i>non applicable</i>                 |
| NULL SHA                        | <i>non applicable</i>                 |
| NULL MD5                        | <i>non applicable</i>                 |
| NULL NULL                       | <i>non applicable</i>                 |

Ces spécifications SSL peuvent également être configurées en modifiant directement le fichier de configuration du proxy. Pour plus d'informations, voir les sections de référence dans le Annexe B, «Directives du fichier de configuration», à la page 175 pour les directives suivantes :

- «V2CipherSpecs — Indique les spécifications de chiffrement prises en charge par SSL version 2», à la page 290
- «V3CipherSpecs — Indique les spécifications de chiffrement prises en charge par SSL version 3», à la page 290
- «FIPSEnable — Codes de chiffrement conformes à la norme FIPS (Enable Federal Information Processing Standard) pour SSLV3 et TLS», à la page 220

### Chiffrement sur 128 bits pour Caching Proxy

Seule une version de chiffrement sur 128 bits est fournie avec Caching Proxy. La version de chiffrement sur 56 bits n'est plus disponible. Si vous mettez à jour une version précédente, vous pouvez installer Caching Proxy directement sur la version

de chiffrement 128 ou 56 bits déjà installée. Si vous utilisiez un navigateur (pour l'export) 56 bits, vous devez le mettre à niveau pour obtenir un navigateur 128 bits afin de profiter du chiffrement sur 128 bits du proxy.

Après la mise à niveau de la version de chiffrement sur 56 bits de Caching Proxy vers une version de chiffrement sur 128 bits, vérifiez la valeur de la taille de la clé utilisée pour le chiffrement des certificats. Si cette valeur est égale à 1024, il n'est pas nécessaire de modifier la configuration. Cependant, si la taille de la clé a une valeur égale à 512, vous devez créer de nouveaux certificats dotés d'une clé dont la taille est égale à 1024 pour pouvoir bénéficier du chiffrement sur 128 bits du proxy. Créez des clés avec l'utilitaire IBM Key Manager (iKeyman).

1. Lancez le gestionnaire de clés.
  - Sous Linux et UNIX, entrez `gsk7ikm` à partir de l'invite de commande.
  - Sur les systèmes Windows, sélectionnez **Démarrer -> Programmes -> IBM WebSphere -> Edge Components -> Démarrer l'utilitaire de gestion de clés**.
2. Dans le menu principal, cliquez sur **Fichier de base de données de clés -> Ouverture**.
3. Dans la boîte de dialogue **Ouverture**, entrez le nom de la base de données de clés (ou cliquez sur **key.kdb** si vous utilisez le nom par défaut) puis cliquez sur **OK**.
4. Si la boîte de dialogue **Invite du mot de passe** s'ouvre, saisissez votre mot de passe et cliquez sur **OK**.
5. Dans le menu principal, cliquez sur **Création -> Nouvelle demande de certificat**.
6. Dans la fenêtre **Création d'une clé et d'une demande de certificat**, indiquez les éléments suivants :
  - **Label de la clé** : Saisissez un nom permettant d'identifier la clé et le certificat dans la base de données.
  - **Keysize** : sélectionnez **1024**.
  - **Nom de l'organisation** : Saisissez le nom de la société à associer à la clé.
  - **Pays** : Saisissez le code de votre pays. Vous devez indiquer au moins deux caractères, par exemple US.
  - **Nom du fichier de demande** : Saisissez le nom du fichier destiné à stocker la demande de certificat. Vous pouvez utiliser un nom par défaut.
7. Cliquez sur **OK**.

Pour plus d'informations sur l'utilitaire IBM Key Manager, voir «Gestion des clés et des certificats», à la page 121.

Cette version ne prend pas en charge le chiffrement dans l'environnement Linux SUSE.

---

## Chapitre 27. Support du matériel cryptographique

S'applique aux configurations avec proxy inversé uniquement.

Pour activer le déchargement de la routine d'établissement de liaison SSL sur une carte matérielle de cryptographie :

1. Conformez-vous aux instructions du fabricant pour l'installation de la carte matérielle de cryptographie.
2. Activez SSL pour Caching Proxy. Pour plus d'informations, voir Chapitre 26, «Secure Sockets Layer (SSL)», à la page 117.
3. Editez manuellement la directive SSLCryptoCard dans le fichier de configuration ibmproxy.conf. Aucune entrée correspondant à cette directive ne figure dans les formulaires de configuration et d'administration. Pour plus d'informations, voir la section de référence sur la directive SSLCryptoCard, «SSLCryptoCard — Spécifie la carte de chiffrement installée», à la page 282.

Sous AIX, pour prendre en charge la carte IBM 4960 PCI Cryptographic Accelerator Card, voir «PKCS11DefaultCert, PKCS11DriverPath, PKCS11TokenPassword — Prend en charge la carte IBM 4960 PCI Cryptographic Accelerator Card (AIX uniquement)», à la page 252.



---

## Chapitre 28. Utilisation du plug-in Tivoli Access Manager

Un plug-in Caching Proxy est fourni avec Tivoli Access Manager (anciennement appelé Tivoli Policy Director) pour permettre à Caching Proxy d'utiliser Access Manager pour l'authentification et l'autorisation. Ce module permet à une entreprise, utilisant Access Manager pour contrôler l'accès au Web, d'ajouter la technologie Edge sans avoir à configurer en plus des schémas d'autorisation distincts pour le serveur proxy.

Pour plus d'informations sur Tivoli Access Manager, consultez le site Web du produit à l'adresse <http://www.ibm.com/software/tivoli/products/>. Pour plus d'informations sur les logiciels et matériels requis, ainsi que sur l'installation du plug-in Access Manager, reportez-vous à la documentation fournie avec Tivoli Access Manager.

**Remarque :** Il se peut que le plug-in Tivoli Access Manager ne fonctionne pas sous Red Hat Linux. Contactez Tivoli pour obtenir des informations relatives au support sur les plateformes Linux.

---

### Configuration

Un script de configuration pour Caching Proxy est fourni avec le plug-in Access Manager.

#### Etapes préalables à l'utilisation du script de configuration

Avant d'exécuter le script, vous devez :

- installer tous les logiciels nécessaires,
- vérifier que le serveur proxy est configuré pour utiliser le port 80 (il s'agit de la valeur par défaut),
- configurer les composants LDAP et Access Manager et vous assurer qu'ils sont en cours d'exécution lors de la configuration du plug-in Access Manager,
- vérifier que vous possédez l'ID administrateur d'Access Manager et que le nom de l'administrateur LDAP est disponible. Ces valeurs sont nécessaires à la configuration du serveur proxy.

#### Utilisation du script de configuration

Le script de configuration s'appelle **wslconfig.sh** et se trouve dans le répertoire `/opt/pdweb-lite/bin/`. Entrez l'ID administrateur d'Access Manager et le nom de l'administrateur LDAP lorsque vous y êtes invité.

Le script de configuration effectue automatiquement les étapes suivantes :

- attribution de la valeur `root` à l'ID utilisateur de Caching Proxy, et de la valeur `other` à l'ID groupe ;
- attribution de la valeur `*` à la directive `noLog`, ce qui empêche l'écriture d'élément dans le Journal des accès de Caching Proxy ;
- création d'une directive `ServerInit` à l'aide des informations suivantes :  
`ServerInit /opt/pdweb-lite/lib/wesauth.so:WTESeal_Init /opt/pdweb-lite/etc/ibmwesas.conf`
- création d'une directive `PreExit` à l'aide des informations suivantes :  
`PreExit /opt/pdweb-lite/lib/wesauth.so:WTESeal_PreExit`

- création d'une directive Authorization à l'aide des informations suivantes :  
Authorization \* /opt/pdweb-lite/lib/wesauth.so:WTESeal\_Authorize
  - création d'une directive ServerTerm à l'aide des informations suivantes :  
ServerTerm /opt/pdweb-lite/lib/wesauth.so:WTESeal\_Term
- création et configuration d'une instruction Protect qui transmet toutes les demandes au processus d'authentification de Access Manager de la manière suivante :
- ```
Protection PROXY-PROT {
    ServerId WebSEAL-Lite
    Mask      All@(*)
    AuthType  Basic
}
Protect * PROXY-PROT
```

Démarrage de Caching Proxy et du plug-in Access Manager

Après avoir configuré le serveur proxy et le plug-in Access Manager, utilisez la commande **wslstartwte**, et non plus **ibmproxy start**, pour lancer le serveur proxy. La commande **wslstartwte** charge automatiquement les variables d'environnement requises pour l'initialisation du plug-in Access Manager. Si vous n'utilisez pas cette commande **wslstartwte** lors du démarrage du serveur proxy, des messages d'erreur concernant le plug-in Access Manager s'affichent à l'écran. La commande d'arrêt correspondante, **ibmproxy stop**, reste valide lorsque le plug-in est utilisé.

Chapitre 29. Utilisation de l'outil module d'autorisation PAC-LDAP

Présentation

L'outil module d'autorisation PAC-LDAP permet au Caching Proxy d'accéder à un serveur LDAP (Lightweight Directory Access Protocol) quand il exécute des routines d'autorisation ou d'authentification. Le module est constitué de deux jeux de composants : d'une part, deux bibliothèques partagées qui dotent l'API Caching Proxy des fonctionnalités LDAP, et, d'autre part, un démon PAC (Policy Authentication Control). Le fichier `ibmproxy.conf` contient la directive `ServerInit` qui donne l'instruction à la bibliothèque partagée d'initialiser un ou plusieurs démons PAC lors du démarrage de Caching Proxy. Les bibliothèques partagées lisent le fichier `paccp.conf` pour déterminer le nombre et les caractéristiques des démons PAC. Lors de l'initialisation, le démon recherche les directives de configuration dans le fichier `pac.conf` et les informations de stratégie de sécurité dans le fichier `pacpolicy.conf`. Ensuite, soit la directive `Authentication` du fichier `ibmproxy.conf` donne instruction au serveur proxy d'appeler la bibliothèque partagée lorsque une authentification est nécessaire, soit une directive `Authorization` prend le contrôle du flux des travaux de Caching Proxy lors du traitement des demandes HTTP standard.

Authentification

Le processus d'authentification détermine si l'ensemble de justificatifs fourni – nom utilisateur et mot de passe – est valide. Ce processus vérifie entre autre qu'un utilisateur se trouve dans le registre et que le mot de passe indiqué correspond au mot de passe stocké dans le registre. Les opérations effectuées avec le module PAC-LDAP lors de l'étape d'authentification sont répertoriées ci-après.

Lorsque l'authentification est possible sur le module d'autorisation PAC-LDAP, ce dernier devient le référentiel d'où sont extraits par défaut les identificateurs utilisateurs, les mots de passe et les groupes. A chaque fois qu'une demande HTTP traverse le flux des travaux de Caching Proxy, chaque directive `Protect` compare l'URL demandée à son modèle de demandes. En cas de correspondance, la directive `Protect` invoque un schéma de protection, lequel inclut l'identificateur du serveur, le type d'authentification à utiliser, les règles de masquage à appliquer au client demandeur et l'emplacement des fichiers de mots de passe et de groupes. Si le fichier de mots de passe n'est pas défini, l'identificateur de l'utilisateur et le mot de passe sont extraits par l'intermédiaire du module d'autorisation PAC-LDAP. Des stratégies de type 0, 1, 2 et 3 définissent les méthodes d'authentification. Si l'authentification aboutit, la demande est servie ; dans le cas contraire, Caching Proxy retourne au client une erreur 401.

Autorisation

Le processus d'autorisation détermine si un utilisateur possède les droits d'accès requis à une ressource protégée. Lorsque le module PAC-LDAP est utilisé, des règles d'autorisation spécifiées dans le fichier `pacpolicy.conf` pour la demande HTTP sont appliquées.

Quand le module d'autorisation PAC-LDAP est configuré pour l'autorisation, les règles d'autorisation contenues dans le fichier `pacpolicy.conf` s'appliquent à la demande HTTP. A chaque fois que la demande HTTP traverse le flux des travaux

de Caching Proxy, chaque directive Protect compare l'URL demandée à son modèle de demandes. En cas de correspondance, la directive Protect invoque un schéma de protection. En l'occurrence, le schéma de protection est la routine d'autorisation usurpée par le module d'autorisation PAC-LDAP. La directive Authorization compare l'URL demandée à son modèle de demandes, et, en cas de correspondance, il fait appel au module d'autorisation PAC-LDAP. Des stratégies de type 4 définies dans le fichier `pacpolicy.conf` affineront par la suite l'authentification nécessaire aux diverses demandes d'URL.

LDAP (Lightweight Directory Access Protocol)

LDAP permet un accès interactif à des annuaires X.500 avec une consommation minimale des ressources système. L'IANA a attribué à LDAP un port TCP 389 et un port UDP 389. Pour plus d'informations, consultez la RFC 1777, qui définit LDAP.

Exemples de clients LDAP pris en charge : client LDAP IBM Tivoli et client LDAP IBM SecureWay.

Installation

Tous les composants du module d'autorisation PAC-LDAP sont automatiquement installés lors de l'installation du système de Caching Proxy de WebSphere Application Server, Version 6.1. Sur les systèmes Linux et UNIX, des répertoires pour la bibliothèque Caching Proxy (`./lib/`), pour la bibliothèque module d'autorisation PAC-LDAP (`./lib/plugins/pac/`), pour les fichiers binaires (`./bin/`) et pour les fichiers de configuration (`./etc/`) sont créés dans le répertoire `/opt/ibm/edge/cp/`. Des liens symboliques sont ensuite créés vers les répertoires spécifiques du produit à partir des répertoires `/usr/lib/`, `/usr/sbin/` et `/etc/`.

Structure des répertoires

Répertoire Linux et UNIX	Répertoire Windows	Contenu
<code>/opt/ibm/edge/cp/</code>	<code>\Program Files\IBM\edge\cp\</code>	Répertoire principal Caching Proxy (<i>cp_root</i>)
<i>cp_root</i> /sbin/	<code>\Program Files\IBM\edge\cp\Bin\</code>	fichiers binaires et scripts Caching Proxy
<code>/usr/sbin/</code>		liens symboliques vers <i>cp_root</i> /sbin/
<i>cp_root</i> /etc/	<code>\Program Files\IBM\edge\cp\etc\</code>	fichiers de configuration Caching Proxy
<code>/etc/</code>		liens symboliques vers <i>cp_root</i> /etc/
<i>cp_root</i> /lib/	<code>\Program Files\IBM\edge\cp\lib\plugins\</code>	bibliothèques Caching Proxy
<i>cp_root</i> /lib/ plugins/pac/	<code>\Program Files\IBM\edge\cp\lib\plugins\pac\</code>	bibliothèques module d'autorisation PAC-LDAP

Répertoire Linux et UNIX	Répertoire Windows	Contenu
/usr/lib/		liens symboliques vers <i>cp_root/lib/</i> et <i>cp_root/lib/plugins/pac/</i>
<i>cp_root/server_root/pac/data/</i>	\Program Files\IBM\edge\cp\server_root\pac\data\	stockage des données module d'autorisation PAC-LDAP
<i>cp_root/server_root/pac/creds/</i>	\Program Files\IBM\edge\cp\server_root\pac\creds\	données d'identification module d'autorisation PAC-LDAP

Fichiers du plug-in LDAP

Nom de fichier Linux et UNIX	Nom du fichier Windows	Description
libpacwte.so	pacwte.dll	bibliothèque partagée
libpacman.so	pacman.dll	bibliothèque partagée
pacd_restart.sh	pacd_restart.bat	script de redémarrage du démon PAC
paccp.conf, pac.conf, pacpolicy.conf	paccp.conf, pac.conf, pacpolicy.conf	fichiers de configuration et de stratégies

Restrictions et configuration supplémentaire requise pour les connexions du serveur sécurisé PACD-LDAP

Utilisation obligatoire de GSKit avec le client LDAP

Pour établir des connexions SSL (Secure Sockets Layer) entre le démon PACD et le serveur LDAP, vous devez installer le module GSKit requis par le module client LDAP. GSKit 7 est requis et installé par défaut sur le système Caching Proxy mais il est possible que cette version ne corresponde pas à celle demandée par le client LDAP sur le système. Il est possible d'utiliser différentes versions de GSKit sur le même système pour des processus différents.

Placez le fichier de clés de GSKit dans `$pacd_creds_dir/pac_keyring.kdb` et le mot de passe dans `$pacd_creds_dir/pac_keyring.pwd`.

Remarque : Pour connaître les paramètres requis pour GSKit sur le serveur LDAP, consultez la documentation IBM Tivoli Directory Server sur le site Web suivant : <http://www.ibm.com/software/tivoli/products/directory-server/>

Définition requise de la variable d'environnement LD_PRELOAD pour les systèmes Linux

Sous Linux, vous devez configurer la variable d'environnement LD_PRELOAD comme indiqué ci-après pour permettre les connexions SSL entre le démon PACD et le serveur LDAP. Associez la variable à la valeur suivante :

```
LD_PRELOAD=/usr/lib/libstdc++-libc6.1-1.so.2
```

Les paramètres requis pour GSKit indiqués plus haut sont également valables pour les systèmes Linux.

Sur les systèmes Linux, le démarrage du processus PACD échoue lors de l'utilisation du client LDAP IBM Tivoli Directory Server (ITDS) 6.0

Sur les systèmes Red Hat Enterprise Linux 4.0, le processus PACD ne démarre pas lorsque Caching Proxy est configuré pour utiliser le plug-in LDAP ITDS 6.0 pour authentification. Le message d'erreur suivant apparaît :

```
"error while loading shared libraries:
/usr/lib/libldapconv.so: R_PPC_REL24 relocation at 0x0fb58ad0
for symbol 'strpbrk' out of range"
```

Une restriction actuelle empêche ITDS 6.0 de prendre en charge les systèmes RHEL 4.0.

Sur les systèmes AIX, il est impossible de charger le module PAC-LDAP en utilisant le client LDAP ITDS (IBM Tivoli Directory Server)

Le processus PACD ne démarre pas sur les systèmes AIX à cause de liens non résolus lorsque vous utilisez le client LDAP ITDS. Au démarrage du processus PACD, l'erreur suivante risque de se produire :

```
exec(): 0509-036 Cannot load program /usr/sbin/pacd because of the following errors:
0509-022 Cannot load module /usr/lib/libpacman.a.
0509-150 Dependent module libldap.a could not be loaded.
0509-022 Cannot load module libldap.a.
```

Pour contourner cet incident pour la version 5 d'ITDS pour le client LDAP, créez le lien symbolique suivant :

```
ln -s /usr/lib/libibmlldap.a /usr/lib/libldap.a
```

Pour contourner cet incident pour la version 6 d'ITDS pour le client LDAP, créez le lien symbolique suivant :

```
ln -s /opt/IBM/ldap/V6.0/lib/libibmlldap.a /usr/lib/libldap.a
```

Modification du fichier ibmproxy.conf pour activer le module d'autorisation PAC-LDAP

Pour pouvoir initialiser le module d'autorisation PAC-LDAP, il est nécessaire d'ajouter à la section API Directives du fichier ibmproxy.conf les directives suivantes : ServerInit, Authorization ou Authentication, et ServerTerm. Pour créer ces directives, vous pouvez modifier manuellement le fichier ibmproxy.conf, ou, si le serveur proxy est en cours d'exécution, vous connecter avec un navigateur Web aux formulaires de configuration et d'administration et ouvrir le formulaire de traitement des demandes API (cliquez sur **Configuration du serveur** → **Traitement des demandes** → **Traitement des demandes API**). Chacune de ces directives doit figurer dans le fichier de configuration sur une seule ligne, même si les exemples contiennent, pour plus de clarté, des sauts de ligne.

En effet, des directives données à titre de prototype ont été ajoutées (sous forme de commentaires) à la section API du fichier ibmproxy.conf. Ces directives API sont

placées dans un ordre délibérément choisi. Lors de l'ajout de directives d'API pour permettre de nouvelles fonctionnalités et l'utilisation de plug-ins, respectez l'ordre dans lequel figurent les directives dans la section Prototypes du fichier de configuration. Vous pouvez également supprimer les marques de commentaires et modifier, si nécessaire, les directives API pour chacune des fonctionnalités ou chacun des plug-ins souhaités.

La directive `ServerInit` comporte trois arguments : (1) le chemin qualifié complet d'accès à la bibliothèque partagée, (2) l'appel à la fonction et (3) le chemin qualifié complet d'accès à `pacpp.conf`. Le premier et le deuxième arguments doivent être délimités par deux points (:). Un espace doit séparer le deuxième et le troisième arguments. Le premier et le troisième arguments sont propres au système et dépendent de l'endroit où sont installés les composants du plug-in. Le deuxième argument est défini dans le code de la bibliothèque partagée et doit être tapé exactement comme il apparaît dans cette dernière. Lors de la création d'une directive `ServerInit` à l'aide du formulaire Traitement des demandes API, le deuxième et le troisième arguments doivent tous deux être entrés dans la zone **Nom de la fonction**. Le troisième argument s'affiche dans la colonne **Modèle d'IP**.

La directive `Authorization` comporte trois arguments : (1) un modèle de demande, (2) le chemin d'accès complet à la bibliothèque partagée et (3) le nom de la fonction. Les demandes HTTP sont comparées au modèle de demandes pour permettre de déterminer si la fonction de l'application est appelée. Le modèle de demande peut inclure le protocole, le domaine et l'hôte ; il peut être précédé d'une barre oblique (/) et utiliser un astérisque (*) en tant que caractère générique. Par exemple, `/front_page.html`, `http://www.ics.raleigh.ibm.com/`, `/pub*`, `/*` et `*` sont tous valides. La fonction porte le nom qui est donné au nom de l'application au sein du programme. Ce nom est figé dans le code et doit être entré exactement tel qu'il apparaît. Un espace doit séparer les deux premiers arguments. Les deux derniers arguments doivent être délimités par deux points (:).

La directive `Authentication` comporte deux arguments : (1) le chemin qualifié complet d'accès à la bibliothèque partagée et (2) le nom de la fonction. Les deux derniers arguments doivent être délimités par deux points (:). Le premier argument est propre au système et dépend de l'endroit où est installée la bibliothèque partagée. Lorsque vous utilisez `Caching Proxy` comme proxy inversé, le modèle d'URL du premier argument doit commencer par la racine du document (/). Le deuxième argument est défini dans le code de la bibliothèque partagée et doit être tapé exactement comme il apparaît dans cette dernière.

La directive `ServerTerm` comporte deux arguments : (1) le chemin qualifié complet d'accès à la bibliothèque partagée et (2) le nom de la fonction. Les deux derniers arguments doivent être délimités par deux points (:). Le premier argument est propre au système et dépend de l'endroit où est installée la bibliothèque partagée. Le deuxième argument est défini dans le code de la bibliothèque partagée et doit être tapé exactement comme il apparaît dans cette dernière. Cette directive met fin à l'activité du démon PAC lors de l'arrêt du serveur proxy. Si le démon et le serveur proxy appartiennent à des propriétaires différents, le serveur proxy risque d'être incapable d'arrêter le démon, auquel cas seul un administrateur peut l'arrêter manuellement.

```
ServerInit chemin_accès_bibliothèque_partagée:pacwte_auth_init  
chemin_accès_fichier_stratégie
```

Exemple Linux et UNIX :

```
ServerInit /usr/lib/libpacwte.so:pacwte_auth_init /etc/pac.conf
```

Exemple Windows :

```
ServerInit C:\Progra ~1\IBM\edge\cp\lib\plugins\  
pac\pacwte.dll:pacwte_auth_init C:\Progra ~1\IBM\edge\cp  
Modèle de demande d'autorisation chemin_bibliothèque_partagée:pacwte_auth_policy
```

Exemple Linux et UNIX :

```
Authorization http://* /usr/lib/libpacwte.so:pacwte_auth_policy
```

Exemple Windows :

```
Authorization http://* C:\Program Files\IBM\edge\cp\lib\plugins\  
pac\pacwte.dll:pacwte_auth_policy  
Authentication BASIC chemin_bibliothèque_partagée:pacwte_auth_policy
```

Exemple Linux et UNIX :

```
Authentification BASIC  
/usr/lib/plugins/pac/libpacwte.so:pacwte_auth_policy
```

Exemple Windows :

```
Authentication BASIC C:\Program Files\IBM\edge\cp\lib\plugins\  
pac\pacwte.dll:pacwte_auth_policy  
ServerTerm chemin_librairie_partagée:pacwte_shutdown
```

Exemple Linux et UNIX :

```
ServerTerm /usr/lib/libpacwte.so:pacwte_shutdown
```

Exemple Windows :

```
ServerTerm BASIC C:\Program Files\IBM\edge\cp\lib\plugins\  
pac\bin\pacwte.dll:pacwte_shutdown
```

Modification des fichiers de configuration du module d'autorisation PAC-LDAP

Vous devez modifier manuellement les fichiers de configuration et de stratégie du module d'autorisation PAC-LDAP en utilisant un éditeur de texte. Le nom d'une directive doit être séparé de son premier argument par le signe deux-points (:). Les arguments sont séparés les uns des autres par des virgules (,). Des commentaires sont inclus dans les fichiers de configuration et de stratégies comme une aide à la modification. Les principales directives de stratégie sont indiquées ci-dessous.

paccp.conf

Le fichier paccp.conf est lu par les bibliothèques partagées lors de l'initialisation de Caching Proxy et contient les définitions (section [PAC_MAN_SERVER]) de chacun des démons PAC qui seront lancés. Chacun de ces démons doit avoir sa propre section [PAC_MAN_SERVER].

```
[PAC_MAN_SERVER]  
hostname:                # nom du démon PAC  
port:                    # port ausculté par pacd  
  
[PACWTE_PLUGIN]  
hostname_check:[true|false] # active la recherche DNS. La recherche DNS  
                             # doit avoir été activée pour qu'ibmproxy  
                             # puisse fonctionner.
```

pac.conf

Le fichier pac.conf définit le serveur LDAP auquel le démon PAC tente de se connecter.

```
[PAC_MAN_SERVER]
hostname:                # nom du démon PAC
port:                    # port ausculté par pacd
conn_type:ssl             # mettez en commentaire si vous n'utilisez pas SSL
authentication_sequence:[primary|secondary|none]
authorization_sequence:[primary|secondary|none]

[LDAP_SERVER]
hostname:                # nom d'hôte du serveur LDAP
port:389                 # port ausculté par LDAP
ssl_port:636             # port SSL utilisé par le serveur LDAP
admin_dn:                # utilisateur disposant de droits d'accès au
                        # serveur LDAPindiquez admin_dn=NULL pour activer
                        # les connexions anonymes portion de l'arborescence
search_base:             # LDAP dans laquelle rechercher les informations de
                        # stratégies Si non requis, indiquez
search_key:              # search_base=NULL champ ID dans lequel
                        # effectuer la recherche

[CACHE]
cred_cache_enabled [TRUE|FALSE] # active la mémoire cache des données
                                # d'identification
cred_cache_min_size:100      # nombre minimal dans pacd de données
                                # d'identification à mettre en mémoire cache
cred_cache_max_size:64000    # nombre maximal dans pacd de données
                                # d'identification à mettre en mémoire cache
cred_cache_expiration:86400  # expiration des données d'identification
policy_cache_enabled:[TRUE|FALSE] # activation/désactivation de la mémoire
                                # cache des stratégies
policy_cache_min_size:100    # nombre minimal d'éléments liés aux stratégies
                                # à mettre en cache
policy_cache_max_size:64000  # max. nombre maximal d'éléments liés aux
                                # stratégies à mettre en cache
policy_cache_expiration:86400 # expiration des éléments liés aux stratégies
```

pacpolicy.conf

Toutes les stratégies LDAP utilisent le modèle suivant dans les fichiers de configuration et de stratégies. Chacune de ces stratégies doit commencer par le mot POLICY en majuscules entre crochets.

```
[POLICY]
default_policy:[grant|deny] # indique la stratégie par défaut des
utilisateurs
                                # qui ne figurent pas dans la section POLICY
pac_client_hostname:         # les instances du Caching Proxy qui ont le droit
                                # d'utiliser une liste de stratégies
id:                          # l'ID de l'entrée LDAP ou ip/nom hôte
                                # (caractères génériques acceptés,
                                # par exemple, *.ibm.com)
grant:[true|false]          # true autorise l'accès, false
                                # interdit l'accès
type:[0|1|2|3|4]            # 0 entrée LDAP correspondant à un groupe,
                                # 1 entrée LDAP ne correspondant pas à un groupe,
                                # 2 adresse IP
                                # 3 nom hôte
                                # 4 URL
propagate:[true|false]      # true indique que les droits d'accès (grant
                                # ou deny) se propageront à tous les
                                # descendants ou membres
stop_entry:[entry|NULL]     # La propagation des droits d'accès s'arrête
                                # à cette entrée. Si l'ID est un groupe,
                                # stop_entry doit recevoir la valeur NULL.
```



```

# stop_entry peut s'appliquer à une adresse IP
# ou à un nom d'hôte. Chaque stop_entry
# doit figurer sur une ligne différente
exception_entry:[entry|NULL] # L'affectation des droits d'accès saute
# ces entrées, mais se poursuit dans leurs
# sous-arborescences. Il peut s'agir d'une
# liste d'entrées.
# exception_entry peut s'appliquer à un groupe,
# une adresse IP ou un nom d'hôte. Chaque
# exception_entry doit figurer sur une ligne
# différente.

Exception_type:
Exception:

```

Le caractère générique (*) n'est possible dans les directives ID et stop_entry que pour la dernière position des adresses IP ou la première position d'un nom d'hôte. Les caractères génériques ne sont pas acceptés dans l'exception_entry. Ils ne sont pris en charge dans aucun champ des entrées LDAP.

Plusieurs stratégies sont prises en charge et la valeur false a toujours la priorité en cas de conflit entre des stratégies. En d'autres termes, un simple refus dans n'importe quelle stratégie bloque tout accès. L'ordre dans lequel sont énumérées les stratégies dans les fichiers de configuration et de stratégies n'a aucune importance et ne crée aucune priorité.

Vous trouverez un jeu d'exemples de stratégies dans le fichier pacpolicy.conf qui se trouve dans le répertoire des fichiers de configuration.

Remarque : Les groupes imbriqués n'héritent pas des stratégies des groupes parents. Les seules stratégies mises en action sont celles auxquelles appartient explicitement le groupe.

Création de pac_ldap.cred

Créez un fichier texte appelé pac_ldap.cred dans */cp_root>/server_root/pac/creds*. Ce fichier contient le mot de passe associé au nom d'utilisateur de la directive admin_dn, définie dans le fichier pac.conf.

Remarque : Pour activer une connexion anonyme, remplacez la directive admin_dn par admin_dn:NULL dans le fichier pac.conf et placez une chaîne fictive dans le fichier pac_ldap.cred.

Le démon PAC chiffrera le mot de passe lors de sa première lecture du fichier.

Pour créer le fichier pac_ldap.cred sous Linux et UNIX, entrez les commandes suivantes :

```

cd cp_root/server_root/pac/creds
echo "password" > pac_ldap.cred
chown nobody pac_ldap.cred
chgrp nobody pac_ldap.cred
(sur Linux SUSE, utilisez chgrp nogroup pac_ldap.cred.)

```

Pour créer le fichier sur une plateforme Windows, tapez le mot de passe dans un fichier texte et stockez ce fichier dans le répertoire server_root\pac\creds\.

Démarrage et arrêt de pacd

Le démon d'autorisation LDAP s'exécute en même temps que pacd. Vous pouvez redémarrer le démon d'autorisation LDAP sans interrompre Caching Proxy grâce aux scripts fournis. Exécutez le script pacd comme indiqué ci-dessous.

- Sous Linux et UNIX :

```
/usr/sbin/pacd_restart.sh id_utilisateur_pacd
```

- Sur les plateformes Windows :

```
C:\Program Files\IBM\edge\cp\Bin\pacd_restart.bat racine_installation_CP
```

Remarque : Vous pouvez continuer à exécuter le processus pacd après l'arrêt du serveur proxy de mise en cache en entrant la commande **stopsrc -ibmproxy** sur les systèmes AIX ou la commande **ibmproxy -stop** sur les systèmes HP-UX, Linux et Solaris. Vous pouvez arrêter en toute sécurité le processus pacd en utilisant la commande **kill** de la manière suivante :

```
kill -15 ID_processus_pacd
```

Sous HP-UX : Le plug-in PAC-LDAP et pacd peuvent ne pas charger toutes leurs bibliothèques partagées dépendantes lors de l'exécution. Avant de les utiliser, vérifiez que les variables du système sont définies de la façon suivante :

```
SHLIB_PATH=/usr/lib:/usr/IBMldap/lib  
PATH=/usr/IBMldap/bin:$PATH  
PATH=/usr/IBMldap/bin
```

/usr/IBMldap/ est le chemin d'installation par défaut du client LDAP sous HP-UX. Modifiez les variables PATH et SHLIB_PATH si le client LDAP est installé dans un autre répertoire. Si vous ne définissez pas ces variables, les erreurs ci-dessous peuvent survenir.

- Une fois le plug-in PAC-LDAP activé, le message suivant apparaîtra dans le journal des erreurs :

```
"Serverinit Error: server did not load functions  
from DLL module /opt/ibm/edge/cp/lib/plugins/pac/libpacwte.sl"
```

- Lorsque vous essayerez de démarrer /usr/sbin/pacd, l'erreur de lien suivante s'affichera :

```
"/usr/lib/dld.sl: Can't find path for shared library: libibmldap.sl  
/usr/lib/dld.sl: No such file or directory  
Abort"
```

Sous Linux : Pour SUSE Linux Enterprise Server 9, ldd pacd peut indiquer que libldap.so n'a pas été trouvé. Pour éviter que cette erreur se produise, créez le lien symbolique suivant :

```
ln -s /usr/lib/libldap.so.19 /usr/lib/libldap.so
```

Sous AIX : Lors du lancement de pacd avec IBM Tivoli Directory Server 5.2, il est possible que le chargement du module PAC-LDAP échoue et génère l'erreur suivante :

```
exec(): 0509-036 Cannot load program /usr/sbin/pacd because of the following errors:  
0509-022 Cannot load module /usr/lib/libpacman.a.  
0509-150 Dependent module libldap.a could not be loaded.  
0509-022 Cannot load module libldap.a.
```

Pour éviter que cette erreur se produise, créez le lien symbolique suivant :

```
ln -s /usr/lib/libibmldap.a /usr/lib/libldap.a
```

Remarque : Lorsque vous configurez Caching Proxy pour qu'il utilise l'authentification LDAP, celui-ci affiche l'erreur suivante :
Could not extract a value for: Uid, return code:3

Cette erreur s'affiche même si l'authentification LDAP fonctionne correctement. N'en tenez pas compte.

Partie 6. Contrôle de Caching Proxy

Cette partie fournit des instructions sur le contrôle de Caching Proxy à l'aide de journal et du Moniteur d'activité du serveur.

Cette partie comporte les chapitres suivants :

Chapitre 30, «Configuration de la consignment», à la page 149

Chapitre 31, «Utilisation du Moniteur de l'activité du serveur», à la page 157

Chapitre 30. Configuration de la consignation

Pour personnaliser la consignation, vous pouvez utiliser les formulaires de configuration et d'administration ou modifier les directives dans le fichier de configuration du proxy. Vous pouvez définir les options suivantes :

- les chemins d'accès et les noms à utiliser pour le stockage des fichiers journaux,
- les filtres permettant d'inclure ou d'exclure des informations dans les journaux des accès,
- les options de maintenance pour l'archivage et la suppression des journaux.

A propos des journaux

Caching Proxy permet de créer trois types de journaux des accès ainsi qu'un journal des événements et un journal des erreurs :

- Journaux des accès :
 - **Journal des accès**—Effectue le suivi des demandes d'administration en local adressées à Caching Proxy.
 - **Journal des accès à la mémoire cache**—Assure le suivi des demandes portant sur des objets en mémoire cache.
 - **Journal des accès au proxy**—Assure le suivi des demandes des serveurs d'origine traitées par le proxy.
- **Journal des événements**—Assure le suivi des messages d'information en mémoire cache.
- **Journal des erreurs**—Assure le suivi des messages d'erreurs relatifs à Caching Proxy.

Caching Proxy crée de nouveaux fichiers journaux tous les jours à minuit. Si le serveur n'est pas en service à cette heure, des journaux sont générés le même jour dès qu'il démarre. Vous pouvez indiquer le répertoire et le préfixe des différents fichiers journaux, qui contiennent également un suffixe de date au format *.Mmmjjaaaa* (par exemple, *.Avr142000*).

Etant donné qu'ils risquent d'occuper beaucoup d'espace, les journaux peuvent être stockés sur une unité de stockage distincte de celles utilisées pour le système d'exploitation et la mémoire cache, afin d'éviter toute erreur. Vous devez également configurer les routines de maintenance des journaux, comme indiqué à la section «Maintenance et archivage des journaux», à la page 153.

Noms des fichiers journaux et options de base

Pour indiquer la configuration de base des journaux du serveur proxy dans les formulaires de configuration et d'administration, sélectionnez **Configuration du serveur -> Consignation -> Fichiers journaux**. Définissez le chemin et le nom de tous les fichiers journaux que vous voulez utiliser. Le nom en cours de chaque journal apparaît dans la zone de texte correspondante ; si vous n'avez pas indiqué le chemin, le chemin par défaut s'affiche.

Les données consignées dans les journaux du proxy ne sont pas enregistrées automatiquement dans le journal système mais vous pouvez configurer Caching Proxy de manière à ce que ces dernières soient enregistrées à la fois dans le journal

système et dans les journaux du proxy, ou uniquement dans le journal système. Dans le formulaire **Fichiers journaux**, cochez la case **Consignation des informations dans Syslog**. Le journal système doit être créé pour que l'option puisse être sélectionnée.

Pour que ces informations soient enregistrées uniquement dans le journal système, vous devez modifier le fichier de configuration du proxy ; pour cela, voir la section de référence de l'élément «LogToSyslog — Envoi des informations d'accès au journal système (Linux et UNIX uniquement)», à la page 236.

Directives du fichier de configuration associées

Pour configurer les journaux à l'aide du fichier de configuration du proxy, voir les sections de référence dans l'Annexe B, «Directives du fichier de configuration», à la page 175 pour les directives suivantes :

- «AccessLog — Nom du chemin d'accès du fichier journal des accès», à la page 177
- «CacheAccessLog — Spécifie le chemin des fichiers journaux des accès à la mémoire cache», à la page 189
- «ErrorLog — Spécifie le fichier dans lequel sont consignées les erreurs du serveur», à la page 213
- «EventLog — Spécifie le chemin du fichier journal des événements», à la page 216
- «LogToSyslog — Envoi des informations d'accès au journal système (Linux et UNIX uniquement)», à la page 236
- «MaxLogFileSize — Spécifie la taille maximale de chaque fichier journal», à la page 240
- «ProxyAccessLog — Indique le nom du chemin du fichier journal des accès au serveur proxy», à la page 264

Filtres des journaux des accès

Les journaux des accès enregistrent l'activité de la machine hôte, du proxy et de la mémoire cache. A chaque fois qu'une demande d'accès est envoyée au serveur proxy, une entrée est générée dans le journal des accès et fournit les informations suivantes :

- L'objet de la demande
- Le moment où la demande a été émise
- L'auteur de la demande
- La méthode de la demande
- Le type de fichier envoyé par le serveur en réponse à la demande
- Le code retour indiquant si la demande a abouti
- La taille des données envoyées

Les erreurs d'accès sont consignées dans le journal des erreurs du serveur.

Raisons justifiant le contrôle des données consignées

Il convient de restreindre les données consignées pour plusieurs raisons :

- Pour réduire la taille du journal.

Lorsque le serveur est occupé, les fichiers journaux peuvent occuper la totalité de l'espace disque. Par défaut, toutes les demandes d'accès sont consignées ; des entrées sont générées dans le journal pour une page HTML mais également pour

chaque image qu'elle contient. Limiter les consignations aux demandes d'accès significatives permet de réduire le nombre d'entrées dans le journal. Par exemple, vous pouvez configurer les journaux des accès de manière à ce qu'ils enregistrent les demandes d'accès concernant les pages HTML et non les images GIF.

- Pour collecter des informations ciblées.

Par exemple, si vous voulez savoir qui, à l'extérieur de l'entreprise, a accès au serveur, vous pouvez filtrer les demandes d'accès pour exclure celles qui proviennent d'adresses IP appartenant à la société. Si vous voulez connaître le nombre de visiteurs d'un site Web particulier, vous pouvez créer un journal des accès indiquant uniquement le nombre d'accès à cette URL.

Les informations exclues des journaux des accès ne sont enregistrées dans aucun rapport d'accès et ne sont pas disponibles pour une utilisation ultérieure. Ainsi, si vous ne savez pas estimer précisément la quantité d'informations dont vous voulez assurer le suivi, vous pouvez limiter l'utilisation des filtres d'exclusion tant que vous n'avez pas acquis suffisamment d'expérience concernant le contrôle du serveur.

Configuration des filtres du journal des accès

Il est possible de filtrer les entrées du journal des accès en se basant sur l'un des attributs suivants :

- URL (fichiers ou répertoires)
- Adresse IP ou nom d'hôte
- Agents utilisateur
- Méthode
- Type MIME
- Code retour

Pour définir les filtres dans les formulaires de configuration et d'administration, sélectionnez **Configuration du serveur** -> **Consignation** -> **Exclusions du fichier journal des accès**. Indiquez uniquement les exclusions de votre choix. Il n'est pas nécessaire d'utiliser toutes les catégories.

- Dans la section intitulée **Ne consignez pas les demandes dans les répertoires ou fichiers suivants du journal des accès**, affichez la liste des chemins d'URL pour lesquels vous ne voulez pas générer d'entrées dans le journal.
- Dans la section intitulée **Ne pas consigner les demandes provenant des agents utilisateurs suivants**, affichez la liste des agents proxy pour lesquels vous ne voulez pas générer d'entrées dans le journal.
- Dans la section intitulée **Ne pas consigner les demandes provenant des noms d'hôte ou des adresses IP suivantes**, affichez la liste des noms d'hôte ou des adresses IP pour lesquels vous ne voulez pas générer d'entrées dans le journal.
- Dans la section intitulée **Ne pas consigner les demandes avec les méthodes suivantes** :, cochez les cases correspondant aux méthodes pour lesquelles vous ne voulez pas générer d'entrées dans le journal.
- Dans la section intitulée **Ne pas consigner les demandes pour les fichiers dotés des types MIME suivants**, cochez les cases correspondant aux types MIME pour lesquels vous ne voulez pas générer d'entrées dans le journal.

Remarque : Cette directive n'affecte que le journal d'accès Proxy. Vous ne pouvez pas filtrer un journal consignait ces objets mis en cache d'après leurs types MIME. Pour ce faire, utilisez `AccessLogExcludeURL`.

- Dans la section intitulée **Ne pas consigner les demandes avec les codes retour suivants**, cochez les cases correspondant aux codes retour pour lesquels vous ne voulez pas générer d'entrées dans le journal.

Cliquez sur **Validation**.

Directives du fichier de configuration associées

Pour définir des filtres pour les journaux des accès à l'aide du fichier de configuration du proxy, voir les sections de référence dans l'Annexe B, «Directives du fichier de configuration», à la page 175 pour les directives suivantes :

- «`AccessLogExcludeMethod` — Supprime les entrées de fichier journal pour les fichiers et les répertoires demandés par une méthode donnée», à la page 178
- «`AccessLogExcludeMimeType` — Supprime les entrées de journal d'accès Proxy pour des types MIME spécifiques», à la page 179
- «`AccessLogExcludeReturnCode` — Supprime les entrées de fichier journal pour des codes retour spécifiques», à la page 179
- «`AccessLogExcludeURL` — Supprime les entrées de journal pour des répertoires ou des fichiers spécifiques», à la page 180
- «`AccessLogExcludeUserAgent` — Supprime les entrées de journal pour des navigateurs spécifiques», à la page 180
- «`NoLog` — Supprime les entrées de journal pour des hôtes spécifiques ou des domaines correspondant à un modèle», à la page 245

Paramètres des journaux par défaut

- **Chemins par défaut**

Tous les journaux sont activés dans la configuration par défaut de Caching Proxy. Ils sont stockés dans le sous-répertoire `logs/` du répertoire d'installation. Les chemins par défaut sont les suivants :

- Journaux des accès (d'administration) en local :
 - Linux et UNIX : `/opt/ibm/edge/cp/racine_serveur/logs/local`
 - Windows : `unité:\Program Files\IBM\edge\cp\logs\local`
- Journal des accès à la mémoire cache :
 - Linux et UNIX : `/opt/ibm/edge/cp/racine_serveur/logs/cache`
 - Windows : `unité:\Program Files\IBM\edge\cp\logs\cache`
- Journal des accès au proxy :
 - Linux et UNIX : `/opt/ibm/edge/cp/racine_serveur/logs/proxy`
 - Windows : `unité:\Program Files\IBM\edge\cp\logs\proxy`
- Journal des erreurs :
 - Linux et UNIX : `/opt/ibm/edge/cp/racine_serveur/logs/error`
 - Windows : `unité:\Program Files\IBM\edge\cp\logs\error`
- Journal des événements :
 - Linux et UNIX : `/opt/ibm/edge/cp/racine_serveur/logs/event`
 - Windows : `unité:\Program Files\IBM\edge\cp\logs\event`

Le nom de chaque fichier journal est une combinaison du nom de base et d'un suffixe de date au format *.Mmmjjaaaa*, par exemple, *proxy.Fev292000*.

- **Formats par défaut**

Les journaux sont stockés par défaut au format de fichier standard. Un format de journal combiné est également disponible et, pour le définir, ajoutez la ligne suivante dans le fichier de configuration du proxy (*ibmproxy.conf*).

`LogFileFormat combined`

Le format du journal combiné, similaire au format standard, comporte des zones supplémentaires contenant le référenceur, l'agent utilisateur et les informations sur les cookies. Le format horaire local est le format horaire par défaut.

- **Contenu par défaut**

Par défaut, toutes les demandes d'accès sont stockées dans le journal des accès approprié ; aucune donnée d'accès n'est enregistrée dans le journal système. Les informations du journal des erreurs sont consignées uniquement dans le journal des erreurs et les informations du journal des événements sont consignées uniquement dans le journal des événements.

- **Maintenance par défaut**

Dans la configuration par défaut, les journaux ne sont ni archivés ni supprimés.

Maintenance et archivage des journaux

Caching Proxy utilise un plug-in pour gérer les journaux. Pour plus d'informations, voir la page de référence dans l'Annexe B, «Directives du fichier de configuration», à la page 175 pour la directive du fichier de configuration «Midnight — Identifie le plug-in API permettant d'archiver les fichiers journaux», à la page 243.

Vous pouvez indiquer comment archiver et supprimer les journaux quotidiens. Les options de base sont les suivantes :

- compression et suppression des journaux antérieurs à une date donnée,
- suppression des journaux dont la date atteint le seuil indiqué ou dont la catégorie atteint le volume indiqué,
- exécution de votre propre programme chaque soir à minuit pour gérer et archiver les journaux.

Par défaut, les journaux du jour et de la veille ne sont jamais supprimés par les agents de maintenance. Les journaux d'accès à la mémoire cache du jour et de la veille ne sont jamais compressés par un agent de maintenance.

Pour configurer la maintenance du journal dans les formulaires de configuration et d'administration, sélectionnez **Configuration du serveur -> Consignation -> Archivage des journaux**. Choisissez la méthode de maintenance appropriée dans la zone de liste déroulante de ce formulaire.

- Si vous avez choisi **Purge**, indiquez l'âge ou la taille du fichier, ou les deux, pour déterminer les journaux à supprimer. Lorsque vous effectuez une purge en fonction de l'âge et de la taille, les fichiers dont l'âge dépasse la limite maximale sont purgés avant les fichiers dépassant la taille maximale. Lorsque vous effectuez une purge en fonction de la taille, les fichiers les plus anciens sont supprimés en premier.
- Si vous choisissez **Compression**, indiquez l'âge à partir duquel les journaux doivent être compressés et la commande à utiliser (spécifiez tous les

paramètres). Indiquez également l'âge maximal des journaux. Après avoir compressé les journaux, l'agent de maintenance supprime les fichiers dépassant l'âge maximal.

Directives du fichier de configuration associées

Pour configurer l'archivage des journaux à l'aide du fichier de configuration du proxy, voir les pages de référence dans l'Annexe B, «Directives du fichier de configuration», à la page 175 pour les directives suivantes :

- «CompressAge — Indique à quel moment compresser les fichiers journaux», à la page 200
- «CompressDeleteAge — Indique à quel moment supprimer les journaux», à la page 201
- «CompressCommand — Spécifie la commande et les paramètres de compression», à la page 200
- «LogArchive — Définit le comportement de la fonction d'archivage du journal», à la page 234
- «Midnight — Identifie le plug-in API permettant d'archiver les fichiers journaux», à la page 243
- «PurgeAge — Spécifie la limite d'âge pour un journal», à la page 268
- «PurgeSize — Spécifie la taille limite d'un fichier journal d'archivage», à la page 269.

Scénario de fichier journal

L'exemple suivant indique comment personnaliser la consignation en fonction de vos besoins. Supposons que vous veniez d'acquérir et d'installer Caching Proxy. Vous voulez configurer le serveur pour qu'il consigne les informations sur les accès et les erreurs en respectant les contraintes suivantes :

- Les journaux doivent utiliser un horodatage local et un format de fichier journal standard.
- Les journaux des accès doivent être purgés lorsqu'ils datent de plus de 30 jours ou lorsque l'ensemble des journaux représente un volume de 25 Mo.
- Les types de demandes suivants ne doivent pas être consignés dans les journaux d'accès :
 - Les demandes concernant les images GIF
 - Les demandes émises par des hôtes dont les adresses IP correspondent à 130.128.*.*
 - Les demandes de réacheminement (qui renvoient un code retour compris entre 300 et 399)

Pour que Caching Proxy gère les journaux selon ces critères dans les formulaires de configuration et d'administration, sélectionnez **Configuration du serveur -> Consignation**.

1. En option, sélectionnez le **formulaire des fichiers journaux** pour indiquer le chemin des fichiers journaux des accès. (Des chemins par défaut sont fournis.)
2. Utilisez le formulaire **Archivage des journaux** pour indiquer le mode d'archivage des fichiers :
 - Sélectionnez **Purge** comme méthode d'archivage.
 - Renseignez les zones sous **Utilisation de la purge** en procédant comme suit :
 - **Supprimez les journaux datant de plus de 30 jours.**

- **Supprimez les journaux dont la taille dépasse 25 Mo.**
- 3. Utilisez le formulaire **Exclusions du fichier journal des accès** pour filtrer les entrées de la manière suivante :
 - Dans la liste **Ne pas consigner les demandes provenant des noms d'hôte ou des adresses IP suivantes**, ajoutez 130.128.*.* dans la zone **Hôte exclu**.
 - Sous **Ne pas consigner les demandes pour les fichiers dotés des types MIME suivants**, cochez la case **image/gif**.
 - Sous **Ne pas consigner les demandes avec les codes retour suivants**, cochez la case **(3xx) Redirection**.

La mise en oeuvre de ces procédures entraîne l'insertion des lignes suivantes dans le fichier de configuration du proxy :

```
LogArchive purge
PurgeAge 30
PurgeSize 25
AccessLogExcludeURL *.gif
NoLog 130.128.*.*
AccessLogExcludeReturnCode 300
```

Chapitre 31. Utilisation du Moniteur de l'activité du serveur

Le Moniteur de l'activité du serveur de Caching Proxy présente des statistiques sur les performances du réseau et du serveur, l'état du serveur et du réseau et les entrées du journal des accès. Le moniteur peut être utilisé à distance et ne doit pas obligatoirement être installé sur la même machine que le serveur. Il est activé par défaut et ne requiert aucune configuration.

L'ouverture de l'outil Moniteur de l'activité du serveur peut s'effectuer de deux manières :

- A partir d'un navigateur Web connecté, entrez l'URL ci-après en utilisant le nom complet de serveur comme indiqué ci-dessous.
`http://nom.du.serveur/Usage/Initial`
- Dans les formulaires de configuration et d'administration, sélectionnez **Moniteur de l'activité du serveur**.

Contrairement aux autres formulaires du client de configuration, les formulaires de cette catégorie ne définissent pas les configurations du serveur mais affichent des données sur l'utilisation du serveur. Ils fournissent beaucoup plus d'informations que ne le ferait une fenêtre de console.

Les sections suivantes indiquent le type d'informations fournies par le **Moniteur de l'activité du serveur** et présentent des conseils sur l'utilisation de ces informations pour ajuster les performances.

Plusieurs pages **Moniteur de l'activité du serveur** sont disponibles :

- **Statistiques d'activité**
- **Statistiques réseau**
- **Statistiques d'accès**
- **Statistiques de l'accès au proxy**
- **Statistiques de mémoire cache**
- **Récapitulatif de la régénération de la mémoire cache**

Toutes ces pages comportent un bouton **Régénération** permettant de mettre à jour les informations qu'elles contiennent.

Statistiques d'activité

Le tableau 4 présente un exemple de page **Statistiques d'activité**.

Tableau 4. Statistiques d'activité

Statistiques d'activité	
Connexions	1 active, 431 au maximum
Temps de réponse	Non disponible
Débit	0 connexion(s)/seconde
Demandes traitées ce jour	0
Nombre total de demandes traitées	114
Erreurs de demande	3

Les statistiques sur les activités du serveur permettent de surveiller le trafic en termes de nombre d'accès, de temps de réponse, de débit, de demandes traitées le jour même, du nombre total de demandes traitées et d'erreurs. Les modifications de configuration suivantes ont une incidence sur les statistiques de la page **Activité**.

- **Nombre d'unités d'exécution actives**—Ce paramètre indique le nombre d'unités d'exécution utilisables pour les demandes du serveur. Vous pouvez augmenter ou réduire le nombre d'unités d'exécution disponibles en fonction de la quantité de mémoire dont vous disposez. Pour modifier ce nombre dans les formulaires de configuration et d'administration, sélectionnez **Configuration du serveur -> Gestion de système -> Performances** ou modifiez la directive `MaxActiveThreads` dans le fichier de configuration. (Voir «`MaxActiveThreads` — Spécifie le nombre maximal d'unités d'exécution actives», à la page 239.)
- **Connexions permanentes**—La prise en charge par le proxy de connexions permanentes avec un client peut avoir une influence sur le débit du réseau. Pour modifier ce paramètre dans les formulaires de configuration et d'administration, sélectionnez **Configuration du proxy -> Performances du proxy** pour activer ou désactiver les connexions permanentes et sélectionnez **Configuration du serveur -> Gestion de système** pour définir le mode de gestion des connexions. Pour modifier ces paramètres à l'aide du fichier de configuration, voir les sections de référence des directives suivantes :
 - «`MaxPersistRequest` — Spécifie le nombre maximal de demandes à recevoir au niveau d'une connexion permanente», à la page 241
 - «`PersistTimeout` — Spécifie la durée d'attente avant que le client n'envoie une autre demande», à la page 251
 - «`ProxyPersistence` — Autorise les connexions permanentes», à la page 266

Statistiques réseau

Le tableau 5 présente un exemple de page **Statistiques réseau**.

Tableau 5. Statistiques réseau

Statistiques réseau	
Données sortantes :	1 ko/seconde
Données entrantes :	1 ko/seconde
Largeur de bande sauvegardée :	3 ko (0 ko/seconde)
Largeur de bande enregistrée ce jour :	0 ko (0 ko/seconde)

Le formulaire **Statistiques réseau** fournit des informations concernant le réseau sur lequel est exécuté le proxy, notamment le débit des données émises et reçues.

Statistiques d'accès

La page **Statistiques d'accès** affiche les 20 entrées les plus récentes dans les journaux d'accès. Cette page affiche les entrées les plus récentes dans le journal des accès au proxy (indiquées en noir) et dans le journal des accès à la mémoire cache (indiquées en bleu). Vous pouvez personnaliser les données affichées en personnalisant les données consignées. Pour plus d'informations sur les statistiques du journal des accès, voir «`Filtres des journaux des accès`», à la page 150.

Statistiques des accès au proxy

Le formulaire **Statistiques des accès au proxy** fournit des informations sur l'activité du proxy, indiquant par exemple les URL ayant fait l'objet d'une demande et si celles-ci ont été servies à partir de la mémoire cache. Les URL sont suivies des codes retour fournis aux clients et de la taille du fichier en octets. Les paramètres suivants peuvent améliorer les statistiques d'accès au proxy :

- Utilisez la régénération automatique de la mémoire cache pour augmenter les probabilités de présence du document demandé en mémoire cache. Pour plus de détails, voir Chapitre 20, «Configuration de l'agent de la mémoire cache pour la régénération et le préchargement automatiques», à la page 91.
- Augmentez la durée minimale de conservation des fichiers en mémoire cache. Pour plus de détails, voir «Configuration de la validité de la mémoire cache», à la page 88.
- Ne placez pas en mémoire cache les fichiers traités à partir de votre domaine local. Si cette opération a tendance à réduire le nombre de demandes servies en mémoire cache, aucune baisse de performance n'est enregistrée si les fichiers sont servis aussi vite à partir de votre intranet local qu'à partir de la mémoire cache (et même plus rapidement dans certains cas). Pour plus de détails, voir Chapitre 18, «Contrôle du contenu de la mémoire cache», à la page 81.

Statistiques de mémoire cache

Si la mise en mémoire cache est activée, la page **Statistiques de mémoire cache** contient des informations sur les accès récents à la mémoire cache. Elle fournit des informations sur la mémoire cache et l'indice, comme indiqué ci-dessous :

- Etat de la mémoire cache, en cours d'exécution ou de réindexation au démarrage du serveur
- Processus de récupération de place en cours ou non
- Taux de réussite de la mémoire cache

Un grand nombre d'options de configuration de la mémoire cache modifient les résultats des statistiques (voir Partie 4, «Configuration de fonction de mise en cache du serveur proxy», à la page 71).

Récapitulatif de la régénération de la mémoire cache

Si l'agent de la mémoire cache est configuré pour un préchargement des fichiers en mémoire cache, la page **Récapitulatif de la régénération de la mémoire cache** présente des informations sur l'exécution la plus récente de l'agent de la mémoire cache. Ce dernier doit avoir été exécuté au moins une fois pour que des informations s'affichent. Pour modifier le fonctionnement de l'agent de la mémoire cache, tenez compte des facteurs suivants :

- Si la plus grande partie du trafic sur votre intranet ne concerne pas les sites Web locaux, vous pouvez envisager de désactiver la mise en mémoire cache du domaine local. Pour plus de détails, voir Chapitre 18, «Contrôle du contenu de la mémoire cache», à la page 81.
- Si un grand nombre de clients demandent une page ne figurant pas dans le journal des accès à la mémoire cache, vous pouvez configurer manuellement l'URL à charger. Pour obtenir des instructions, voir «Directives du fichier de configuration du proxy associées», à la page 97.
- Ajustez le nombre des URL les plus utilisées à précharger. Pour obtenir des instructions, voir «Directives du fichier de configuration du proxy associées», à la page 97.

- Indiquez la durée maximale d'exécution de l'agent de la mémoire cache. Pour obtenir des instructions, voir «Directives du fichier de configuration du proxy associées», à la page 97.

Annexe A. Utilisation de commandes de Caching Proxy

Cette annexe est la liste de référence des commandes de serveur proxy.

cgiparse, commande

Objet

La commande **cgiparse** analyse la variable d'environnement QUERY_STRING des scripts CGI. Si cette variable n'est pas définie, la commande lit les caractères CONTENT_LENGTH dans l'entrée standard. Toutes les sorties renvoyées sont enregistrées dans la sortie standard.

Syntaxe

`cgiparse -Indicateurs [Modificateur]`

Paramètres

Les indicateurs et leurs équivalents sous forme de caractère unique, (-k -f -v -r -i -s -p -c -q -P) sont présentés ci-dessous, ainsi que leur fonction :

-keywords | -k

Recherche les mots clés dans la variable QUERY_STRING. Les mots clés sont décodés et enregistrés dans la sortie standard, sur des lignes distinctes.

-form | -f

Analyse QUERY_STRING en tant que demande de formulaire. Renvoie une chaîne qui, une fois évaluée par le shell, définit des variables de shell composées du préfixe FORM_ et d'un nom de zone. Les valeurs des zones correspondent au contenu des variables.

-value nom-zone | -v nom-zone

Analyse QUERY_STRING en tant que demande de formulaire. Renvoie uniquement la valeur de *nom-zone*.

-read | -r

Lit les caractères de la variable CONTENT_LENGTH dans l'entrée standard et les enregistre dans la sortie standard.

-init | -i

Si la variable QUERY_STRING n'est pas définie, la commande lit la valeur de l'entrée standard et renvoie une instruction SET qui affecte cette valeur à la variable QUERY_STRING. Cette commande peut être utilisée avec les méthodes GET et POST. L'utilisation type de cette commande est la suivante :
`eval 'cgiparse -init'`

Cette commande définit la variable d'environnement QUERY_STRING, quelle que soit la méthode employée (GET ou POST).

cgiparse peut être appelée plusieurs fois dans un même script quand la méthode GET est utilisée ; avec la méthode POST, cette commande ne peut être appelée qu'une fois. Lorsque la méthode POST est utilisée après la lecture de l'entrée standard, la commande **cgiparse** suivante trouve l'entrée standard et se bloque (elle attend indéfiniment).

-sep séparateur | -s séparateur

Indique la chaîne utilisée pour séparer les valeurs. Si vous utilisez l'indicateur **-value**, le séparateur par défaut est une nouvelle ligne. Si vous utilisez l'indicateur **-form**, le séparateur par défaut est une virgule (,).

-prefix préfixe | -p préfixe

Utilisée avec **-POST** et **-form**, indique le préfixe à indiquer pour créer les noms de variables d'environnement. Le préfixe par défaut est "FORM_".

-count | -c

Utilisée avec **-keywords**, **-form**, et **-value**, renvoie le nombre d'éléments liés à ces indicateurs.

-keywords | -k

Renvoie le nombre de mots clés.

-form | -f

Renvoie le nombre de zones uniques (les valeurs multiples comptent pour une unité).

-value nom-zone | -v nom-zone

Renvoie le nombre de valeurs pour *nom-zone* (s'il n'existe aucune zone appelée *nom-zone*, la valeur 0 est renvoyée).

-numéro

Utilisée avec **-keywords**, **-form** et **-value**, renvoie l'occurrence spécifiée en fonction de ces indicateurs.

-keywords

Renvoie le *nième* mot clé. (Par exemple **-2 -keywords** renvoie le deuxième mot clé.)

-form

Renvoie toutes les valeurs de la *nième* zone. (Par exemple **-2 -form** renvoie toutes les valeurs de la deuxième zone.)

-value nom-zone

Renvoie la *nième* valeur de la zone *nom-zone*. (Par exemple **-2 -value -whatsit** renvoie la deuxième valeur de la zone **whatsit**).

-quiet | -q

Supprime tous les messages d'erreur. (Un état de sortie non nul indique encore une erreur.)

-POST | -P

Les informations contenues dans l'entrée standard (ou si un nom de fichier est attendu, le fichier stdin) sont directement décodées et analysées dans les variables du shell, sans que la variable QUERY_STRING soit utilisée. **-POST** équivaut à l'utilisation consécutive des options **-init** et **-form**.

Exemples

Les exemples suivants ne tiennent pas compte du fait que la variable QUERY_STRING est en réalité déjà définie par le serveur. Dans les exemples suivants, \$ est l'invite du shell Bourne.

- Recherche des mots clés

```
$ QUERY_STRING="is+2%2B2+really+four%3F"
$ export QUERY_STRING
$ cgifparse -keywords
is
2+2
really
four?
$
```

- Analyse de toutes les zones d'un formulaire

```
$ export QUERY_STRING="name1=Value1&name2=Value2%3f+That%27s+right%21";
$ cgifparse -form
FORM_name1='Value1'; FORM_name2='Value2? That'\s right!'
$ eval `cgifparse -form`
```

```
$ set | grep FORM
FORM_name1="Value1"
FORM_name2="Value2? That's right!"
$
```

- Extraction d'une valeur de zone unique

```
$ QUERY_STRING="name1=value1&name2=Second+value%3F+That'\ 's%27s
$ cgiparse -value name1
value1
$ cgiparse -value name2
Second value? That's right!
$
```

Résultats

- | | |
|---|--|
| 0 | Réussi |
| 1 | Ligne de commande incorrecte |
| 2 | Variables d'environnement définies de manière incorrecte |
| 3 | Les informations demandées n'ont pas été extraites (par exemple, aucune zone ou variable QUERY_STRING du type indiqué ne contient de mot clé lors d'une demande portant sur les valeurs de zone d'un formulaire) |

Remarque : Lorsque l'un de ces codes d'erreur s'affiche, vous pouvez également recevoir des messages explicatifs. Leur contenu varie en fonction de la commande lancée.

cgiutils, commande

Objet

Utilisez la commande **cgiutils** dans les programmes **nph** (no-parse header) pour générer une réponse HTTP 1.0 complète.

Remarque : Si vous voulez fournir vos propres programmes **nph** pour que des valeurs personnelles soient renvoyées, le nom du programme doit commencer par **nph-**. L'en-tête du serveur ne remplace pas votre valeur personnelle par la valeur de retour standard du serveur.

Syntaxe

`cgiutils -Indicateur [Modificateur]`

Si *Modificateur* contient des espaces, mettez-le entre guillemets ("").

Paramètres

-version

Renvoie les informations de version.

-nodate

Ne renvoie pas l'en-tête **Date:**.

-noel

Ne renvoie pas une ligne vide après les en-têtes. Cet indicateur permet d'insérer d'autres en-têtes MIME après la ligne d'en-tête initiale.

-status *nnn*

Renvoie une réponse HTTP complète avec le code d'état *nnn* au lieu d'un ensemble d'en-têtes HTTP. N'utilisez pas cet indicateur si vous voulez uniquement l'en-tête **Expires:**.

-reason *explication*

Indique la ligne d'explication de la réponse HTTP. Vous pouvez également utiliser cet indicateur avec l'indicateur **-status** *nnn*.

-ct [*type/sous-type*]

Indique l'en-tête MIME Content-Type. Cet exemple présente un type de contenu MIME `texte/html` :

```
cgiutils -ct text/html
```

Si vous n'indiquez pas le *type/sous-type*, le type de contenu MIME devient `text/plain` par défaut. Cet exemple définit un type de contenu MIME `text/plain`.

```
cgiutils -ct
```

-ce *codage*

Indique l'en-tête MIME Content-Encoding. Par exemple :

```
cgiutils -ce x-compress
```

-cl *code-langue*

Indique l'en-tête MIME Content-Language. Par exemple :

```
cgiutils -cl en_UK
```

-length *nnn*

Indique l'en-tête MIME Content-Length.

-expires *Durée*

Indique l'en-tête MIME **Expires:**. Cet indicateur définit la durée de vie (date d'expiration) d'un document en utilisant une combinaison de jours, de minutes et de secondes. Il correspond à la durée de validité d'un document. Par exemple :

```
cgiutils
-expires 2 jours 12 heures
```

La commande **cgiutils** ajoute la durée indiquée à l'heure GMT (Greenwich Mean Time) en cours pour déterminer la date d'expiration. Cette dernière est ajoutée dans l'en-tête **Expires:** au format HTTP.

-expires now

Génère un en-tête **Expires:** correspondant à l'en-tête **Date:**.

-uri *URI*

Indique l'URI (Universal Resource Identifier) du document renvoyé. Un URI peut être assimilé à une URL.

-extra xxx: *yyy*

Indique un en-tête supplémentaire qu'il serait impossible de définir autrement avec la commande **cgiutils**.

Exemples

- Cet exemple calcule la date d'expiration pour l'en-tête **Expires:**.

```
cgiutils -expires "1
année 3 mois 2 semaines 4 jours 12 heures 30 minutes"
```

- L'exemple suivant indique un code d'état et un motif, et attribue à l'en-tête **Expires:** la même valeur qu'à l'en-tête **Date:**.

```
cgiutils -status 200 -reason "Virtual doc follows" -expires now
```

Cette commande génère des en-têtes similaires à ceux-ci :

```
HTTP/1.0 200 Virtual doc follows
MIME-Version: 1.0
Server: IBM-ICS
Date: Tue, 05 Jan 1996 03:43:46 GMT
Expires: Tue, 05 Jan 1996 03:43:46 GM
```

La commande **cgiutils** génère automatiquement l'en-tête **Server:** car celui-ci est disponible dans l'environnement CGI. La zone **Date :** est générée automatiquement à moins que l'indicateur **-nodate** soit spécifié.

Une ligne vide est générée après la sortie pour indiquer la fin de la section de l'en-tête MIME. Si vous voulez ajouter d'autres en-têtes, utilisez l'indicateur **-noel** (NO-Empty-Line) comme indiqué dans l'exemple suivant.

- Si vous ne voulez pas insérer une ligne vide après la ligne d'en-tête, utilisez l'indicateur **-noel** :

```
cgiutils -noel
-expires "2 jours" -nodate
HTTP/1.0 200 Virtual doc follows
MIME-Version: 1.0
Server: IBM-ICS
Expires: Tue, 07 Jan 1996 03:43:46 GMT
```

htadm, commande

Objet

La commande **htadm** permet de contrôler les fichiers de mots de passe du serveur. Ce dernier utilise des fichiers de mots de passe pour contrôler les accès aux fichiers. Vous pouvez ajouter un nom d'utilisateur dans un fichier de mots de passe, supprimer un utilisateur, vérifier le mot de passe d'un utilisateur et créer un fichier de mots de passe vide. Vous pouvez également modifier le mot de passe d'un utilisateur en supprimant le mot de passe avant d'en créer un autre.

Remarque : Pour ajouter un utilisateur et modifier ou vérifier un mot de passe à l'aide de la commande **htadm**, vous devez entrer le mot de passe sur la ligne de commande. Du fait que la commande détruit rapidement le mot de passe saisi à la ligne de commande, il est très improbable que vous puissiez connaître cette information en examinant le processus en cours d'exécution (à l'aide de la commande **ps**, par exemple).

Syntaxe

`htadm -Indicateur [Modificateur]`

Paramètres

-adduser *fichier-mots-de-passe nom-utilisateur [mot de passe [nom]]*

Ajoute un utilisateur et un mot de passe dans le fichier de mots de passe. Si vous entrez la commande en spécifiant uniquement le paramètre *fichier-mots-de-passe*, le système vous invite à fournir les autres paramètres.

fichier-mots-de-passe

Chemin et nom du fichier de mots de passe dans lequel vous voulez ajouter l'utilisateur.

nom-utilisateur

Nom de l'utilisateur à ajouter.

Utilisez des caractères alphanumériques et aucun caractère spécial.

La commande échoue s'il existe un utilisateur du même nom dans le fichier de mots de passe.

mot de passe

Mot de passe que vous voulez définir pour le nom d'utilisateur.

Les mots de passe peuvent comporter jusqu'à 32 caractères. Utilisez des caractères alphanumériques et aucun caractère spécial.

Remarques :

1. Certains navigateurs ne peuvent pas lire ni envoyer des mots de passe de plus de huit caractères. Lorsque le mot de passe comporte plus de huit caractères, le serveur peut reconnaître le mot de passe tout entier ou les huit premiers caractères uniquement.
2. Les majuscules sont différenciées des minuscules dans le nom d'utilisateur de l'administrateur et son mot de passe même si elles ne sont pas différenciées dans le système d'exploitation. Veillez à saisir le nom d'utilisateur et le mot de passe exacts lorsque vous utilisez la commande **htadm** pour accéder aux formulaires de configuration et d'administration.

nom-r  el

Commentaire ou nom    utiliser pour identifier le nom d'utilisateur que vous ajoutez. Toutes les donn  es entr  es sont enregistr  es dans le fichier de mots de passe.

-deluser *fichier-mots-de-passe* [*nom-utilisateur*]

Supprime un utilisateur dans le fichier de mots de passe. Si vous entrez la commande en sp  cifiant uniquement le param  tre *fichier-mots-de-passe*, le syst  me vous invite    fournir le *nom-utilisateur*.

fichier-mots-de-passe

Chemin et nom du fichier de mots de passe dans lequel vous voulez supprimer un utilisateur.

nom-utilisateur

Nom de l'utilisateur    supprimer. La commande   choue si le nom d'utilisateur indiqu   n'existe pas dans le fichier de mots de passe.

-passwd *fichier-mots-de-passe* [*nom-utilisateur* [*mot-de-passe*]]

Modifie le mot de passe pour un nom d'utilisateur d  j d  fini dans le fichier de mots de passe. Si vous entrez la commande en sp  cifiant uniquement le param  tre *fichier-mots-de-passe*, le syst  me vous invite    fournir les autres param  tres.

fichier-mots-de-passe

Chemin et nom du fichier de mots de passe contenant le nom d'utilisateur pour lequel vous voulez modifier le mot de passe.

nom-utilisateur

Nom de l'utilisateur pour lequel vous voulez modifier le mot de passe. La commande   choue si le nom d'utilisateur indiqu   n'existe pas dans le fichier de mots de passe.

mot de passe

Nouveau mot de passe que vous voulez d  finir pour le nom d'utilisateur.

Les mots de passe peuvent comporter jusqu'   32 caract  res. Utilisez des caract  res alphanum  riques et aucun caract  re sp  cial.

Remarques :

1. Certains navigateurs ne peuvent pas lire ni envoyer des mots de passe de plus de huit caract  res. Lorsque le mot de passe comporte plus de huit caract  res, le serveur peut reconnaître le mot de passe tout entier ou les huit premiers caract  res uniquement.
2. The administrator user name and password are case-sensitive even if the operating system is not case-sensitive. Veuillez    saisir le nom d'utilisateur et le mot de passe exacts lorsque vous utilisez la commande `htadm` pour acc  der aux formulaires de configuration et d'administration.

-check *fichier-mots-de-passe* [*nom-utilisateur* [*mot-de-passe*]]

V  rifie le mot de passe correspondant    un nom d'utilisateur d  j d  fini dans le fichier de mots de passe et vous indique s'il est correct ou non. Si vous entrez la commande en sp  cifiant uniquement le param  tre *fichier-mots-de-passe*, le syst  me vous invite    fournir les autres param  tres.

fichier-mots-de-passe

Chemin et nom du fichier de mots de passe contenant le nom d'utilisateur pour lequel vous voulez v  rifier le mot de passe.

nom-utilisateur

Nom de l'utilisateur pour lequel vous voulez vérifier le mot de passe. La commande échoue si le nom d'utilisateur indiqué n'existe pas dans le fichier de mots de passe.

mot de passe

Mot de passe que vous voulez vérifier. Si le mot de passe que vous entrez correspond à celui que vous avez défini pour le nom d'utilisateur, la commande enregistre Correct dans la sortie standard et ajoute le code retour 0. Si tel n'est pas le cas, la commande enregistre Incorrect dans la sortie standard.

-create *fichier-mots-de-passe*

Crée un fichier de mots de passe vide.

fichier-mots-de-passe

Chemin et nom du fichier de mots de passe que vous voulez créer.

Exemples

- Pour ajouter un utilisateur à un fichier de mots de passe :

- Systèmes Linux et UNIX :

```
htadm -adduser /opt/ibm/edge/cp/server_root/protect/heroes.pwd  
clark superman "Clark Kent"
```

- Systèmes Windows :

```
htadm -adduser "C:\Program Files\IBM\edge\cp\server_root\protect\  
heroes.pwd" clark superman "Clark Kent"
```

Remarque : La commande **htadm** doit être entrée sur une seule ligne. Elle est représentée ici sur plusieurs lignes en raison de contraintes de formatage. Entrez la commande sur une ligne en insérant un espace entre clark et superman.

- Pour supprimer un utilisateur d'un fichier de mots de passe :

- Systèmes Linux et UNIX :

```
htadm -deluser /opt/ibm/edge/cp/server_root/protect/  
heroes.pwd clark superman "Clark Kent"
```

- Systèmes Windows :

```
htadm -deluser "C:\Program Files\IBM\edge\cp\server_root\protect\  
heroes.pwd" clark superman "Clark Kent"
```

htcformat, commande

Objet

La commande **htcformat** permet de préparer une unité en mode brut ou un fichier pour y stocker la mémoire cache du proxy. Cette commande de formatage doit être lancée avant que l'unité soit configurée à cette fin.

Le chemin de l'unité doit indiquer l'unité en mode brut. Pour plus de détails sur la méthode d'accès aux unités en mode brut, consultez la documentation de votre système de fichiers. Vous trouverez également des exemples dans la Partie 4, «Configuration de fonction de mise en cache du serveur proxy», à la page 71.

Remarque : Les noyaux Linux 2.2 ne prennent pas en charge la mise en mémoire cache sur des unités en mode brut. Sur les plateformes Linux, seuls les fichiers et la mémoire peuvent être utilisés pour une mise en mémoire cache.

La taille minimale d'une mémoire cache Caching Proxy est de 16392 ko, soit 2049 blocs.

Syntaxe

```
htcformat unité [-blocksize <taille bloc>] [-blocks nombre de blocs>]  
htcformat -file chemin du fichier [-blocksize taille bloc] -blocks nombre de blocs
```

Paramètres

-blocksize

Définit la taille des blocs sur l'unité de mémoire cache. La taille des blocs est indiquée en octets. La valeur par défaut est 8192 et doit être utilisée dans toutes les situations.

-blocks

Nombre de blocs à créer sur l'unité ou dans le fichier. Lors du formatage d'un fichier, cet argument est requis pour indiquer la taille du fichier. Cet argument permet également de limiter la quantité réservée à la mémoire cache sur une unité ou dans une partition donnée. Si aucun argument blocks n'est indiqué, le nombre de blocs créés dépend de la capacité de la partition.

-file

Formate un fichier et non une unité de stockage.

Utilisation

Le système de mise en mémoire cache classe les fichiers ou les unités dans des conteneurs pour l'indexation et la récupération de place. La taille des conteneurs est fixée à un certain nombre de blocs et ne peut être configurée. Pour que la récupération de place fonctionne, deux conteneurs au minimum sont requis ; la taille minimale de la mémoire cache est de 16392 ko.

La commande **htcformat** n'accepte pas une demande de formatage faisant appel à une unité de mise en mémoire cache comportant moins de deux conteneurs.

Exemples

L'exemple suivant formate une partition de disque appelée c0t0d0s0 sous Solaris.
`htcformat /dev/rdisk/c0t0d0s0`

L'exemple suivant formate une partition de disque appelée lv02 sous AIX.

```
htcformat /dev/r1v02
```

L'exemple suivant formate une partition de disque appelé d: sous Windows.

```
htcformat \\.\d:
```

L'exemple suivant formate un fichier appelé filecache de manière à ce que sa taille représente environ 1 Go.

```
htcformat -file /opt/ibm/edge/cp/filecache -blocks 131072
```

ibmproxy, commande

Objet

La commande **ibmproxy** permet de démarrer le serveur.

Vous pouvez définir tous ces indicateurs (à l'exception de **-r**) en utilisant les directives dans le fichier de configuration du serveur.

Il est d'usage de créer un fichier README qui contient des instructions ou des remarques que doit lire tout nouvel utilisateur du répertoire. Par défaut, **ibmproxy** intègre le fichier README dans la version hypertexte d'un répertoire. Les instructions du fichier README peuvent également être définies à l'aide de la directive de configuration DirReadme.

Syntaxe

```
ibmproxy [-Indicateur [-Indicateur [-Indicateur..]]]
```

Paramètres

-nobg

Exécute le serveur en tant que processus d'avant-plan et non d'arrière-plan. Par défaut, le serveur est exécuté en tant que processus d'arrière-plan.

-nosnmp

Désactive la prise en charge de SNMP.

-p *numéro-port*

Etablit une connexion à ce numéro de port. Le numéro de port par défaut est 80. Cet indicateur supplante la directive Port indiquée dans le fichier de configuration. Pour utiliser la valeur par défaut ou la valeur indiquée dans le fichier de configuration, ne spécifiez pas cet indicateur.

-r *fichier-configuration*

Indique le fichier à utiliser en tant que fichier de configuration. Vous devez utiliser cet indicateur pour démarrer le serveur avec un fichier de configuration autre que celui défini par défaut. Vous pouvez ainsi utiliser plusieurs fichiers de configuration.

-restart

Redémarre le serveur en cours d'exécution. La commande **ibmproxy** extrait le numéro de processus du serveur en cours d'exécution dans le fichier PidFile et envoie celui-ci au signal HangUP (HUP). Elle recharge ensuite les fichiers de configuration et ouvre à nouveau les fichiers journaux. Pour éviter tout risque d'altération, évitez d'exécuter simultanément deux instances du serveur ayant les mêmes fichiers PidFile, fichiers journaux et mémoire cache du proxy.

Etant donné que le démon **http** doit lire le fichier de configuration utilisé par le serveur pour accéder au fichier PidFile, vous devez indiquer le même fichier de configuration lors du redémarrage. Si vous avez utilisé l'indicateur **-r** et un fichier de configuration donné lors du démarrage du serveur, vous devez spécifier cet indicateur et ce même fichier avec **-restart**.

-snmp

Active la prise en charge de SNMP.

-unload

Sous Linux, cette commande supprime les règles de pare-feu associées.

Les options de traitement des signaux existent également sur les plateformes Linux et UNIX. Sur les plateformes Linux et UNIX, les options suivantes sont disponibles.

SIGTERM

La commande **ibmproxy** s'arrête et se ferme une fois le processus terminé. Vous pouvez utiliser SIGKILL ou CANCEL pour arrêter le processus immédiatement.

SIGHUP

S'il est actif, relance **ibmproxy**, recharge le fichier de configuration et continue le traitement.

Exemples

- Pour démarrer le serveur sur le port 8080, à l'aide du fichier de configuration /usr/etc/ibmproxy.conf au lieu du fichier par défaut, /etc/ibmproxy.conf, entrez :

```
ibmproxy -p 8080 -r /usr/etc/ibmproxy.conf
```

- Pour démarrer un serveur sous AIX à l'aide du fichier de configuration par défaut en utilisant le contrôleur des ressources système, entrez :

```
startsrc -s ibmproxy
```

Si le fichier de configuration par défaut n'existe pas, **ibmproxy** exporte l'arborescence /Public. Cette arborescence peut contenir des liens lointains vers d'autres arborescences.

Annexe B. Directives du fichier de configuration

Cette annexe présente les directives contenues dans le fichier de configuration `ibmproxy.conf`.

- **Sous Linux et UNIX.** Ces directives se trouvent dans le fichier de configuration `ibmproxy.conf` dans le répertoire `/etc/`.
- **Sur les systèmes Windows.** Ces directives se trouvent généralement dans `C:\Program Files\IBM\edge\cp\`.

Utilisez ces informations comme référence si vous configurez le serveur en éditant le fichier de configuration `ibmproxy.conf`. Si vous utilisez les formulaires de configuration et d'administration, il n'est pas nécessaire de consulter ce chapitre.

Les directives sont classées dans une liste par ordre alphabétique.

Directives non modifiées lors du redémarrage

Certaines directives ne sont pas régénérées lors du redémarrage du serveur. Si les directives suivantes sont modifiées lors de l'exécution du serveur, vous devrez arrêter manuellement ce dernier puis le redémarrer. (Voir Chapitre 5, «Démarrage et arrêt de Caching Proxy», à la page 15.)

Tableau 6. Directives non régénérées au redémarrage

Groupe de directives	Directives
CGI	DisinheritEnv, InheritEnv
Mise en mémoire cache	Mise en mémoire cache
Consignation	AccessLog, CacheAccessLog, ErrorLog, ProxyAccessLog, ServerRoot
Accès réseau	BindSpecific, Hostname, ListenBacklog, Port
Performance	MaxActiveThreads
RTSP	Toutes les directives RTSP
SSL	Toutes les directives SSL
Contrôle de processus Linux et UNIX	GroupId, UserId
Divers	TransparentProxy

Présentation des directives

Cette annexe fournit les informations suivantes sur chaque directive :

- un en-tête comportant le nom de la directive et une brève description,
- des instructions d'utilisation,
- le format de la directive, qui fait suite à la syntaxe générale :
NomDirective valeur
- le cas échéant, un exemple de paramètre possible pour la directive est inclus dans le fichier de configuration

Remarque : Les exemples des directives contenant des chemins d'accès spécifiques du système Windows peuvent contenir *racine_serveur>*, qui correspond au répertoire racine du serveur sélectionné lors de l'installation.

- la ou les valeurs par défaut de la directive.
Il s'agit des valeurs d'origine codées dans le fichier de configuration par défaut. Modifiez uniquement les parties du fichier de configuration devant être différentes des paramètres par défaut. Une directive pour laquelle aucune valeur par défaut n'est codée à l'origine apparaît dans le fichier précédée d'un symbole de commentaire (#). Pour spécifier une valeur pour cette directive, supprimez le symbole de commentaire et ajoutez la valeur sur la ligne dans le fichier de configuration.

Valeurs autorisées

La liste suivante répertorie les valeurs acceptées dans le fichier de configuration :

- Dans les informations de référence de certaines directives, la partie *valeur* contient les modèles des demandes, des noms de chemin ou des noms d'hôte. Sauf contre-indication, vous pouvez utiliser le caractère astérisque (*) dans les modèles. Pour que les modèles correspondent, un astérisque peut être remplacé par toute autre chaîne de caractères ou par tout autre caractère.
- Les directives de configuration permettent d'entrer une chaîne positive acceptant ces valeurs :
 - Yes
 - On
 - OK
 - Enable
- Les directives de configuration permettent d'entrer une chaîne négative acceptant ces valeurs :
 - No
 - Off
 - None
 - Disable
- Les directives de configuration permettent de spécifier une durée acceptant les combinaisons suivantes :
 - *hh*—heures
 - *hh:mm*—heures et minutes
 - *hh:mm:ss*—heures, minutes et secondes
 - *n years*—nombre d'années de 365 jours
 - *n months*—nombre de mois de 30 jours
 - *n weeks*—nombre de semaines de 7 jours
 - *n days*—nombre de jours de 24 heures
 - *n hours*—nombre d'heures de 60 minutes
 - *n minutes*—nombre de minutes de 60 secondes
 - *n seconds*—nombre de secondes
 - *n fortnights*—nombre d'intervalles de 14 joursToutes les entrées sont converties en secondes et ajoutées les unes aux autres.
- Les caractères vides ne sont pas admis à l'intérieur d'un nom de fichier spécifié dans le fichier de configuration. Les caractères vides sont traités comme des délimiteurs.

Syntaxe des enregistrements du fichier de configuration

Lorsque vous éditez le fichier de configuration, n'oubliez pas que :

- Chaque directive doit commencer sur une nouvelle ligne.
- Les valeurs sont séparées par un ou plusieurs caractères d'espacement. Le caractère d'espacement et le caractère de tabulation sont considérés comme identiques.
- Le début d'un commentaire est indiqué par un signe dièse (#). Tous les caractères à partir du signe # jusqu'à la fin de la ligne sont ignorés.
- Si vous devez indiquer le signe d'un nombre ou un caractère vide pour une directive, placez la barre oblique inverse (\) devant ce caractère en tant que caractère d'échappement. Un caractère d'échappement indique que le caractère suivant doit être interprété en tant que caractère et non en tant que commande. Par exemple, si le caractère \# se trouve sur une ligne, le serveur l'interprète en tant que caractère dièse et non comme le début d'un commentaire et continue à lire les caractères. Si le caractère \ se trouve sur une ligne, le serveur l'interprète comme étant un caractère d'espacement et non un délimiteur de valeurs et continue à lire les caractères pour construire la valeur.

Directives Caching Proxy

Vous trouverez ci-après les directives du module Caching Proxy.

AcceptAnything — Servir tous les fichiers

Cette directive permet de servir tous les fichiers vers le client même si le type MIME du fichier ne correspond à aucun en-tête ACCEPT: envoyé par le client. Si cette directive a la valeur OFF, les fichiers dont le type MIME diffère de ceux acceptés par le client ne seront pas affichés. A la place, une page d'erreur est affichée.

Format

AcceptAnything {on | off}

Exemple

AcceptAnything off

Valeur par défaut

AcceptAnything on

AccessLog — Nom du chemin d'accès du fichier journal des accès

Cette directive permet de spécifier le répertoire et le nom du fichier dans lequel le serveur doit consigner les statistiques d'accès au serveur. Par défaut, le serveur écrit une entrée dans ce fichier journal dès qu'un client envoie au serveur une demande relative aux données stockées sur le serveur local. Généralement, ces données incluent uniquement les demandes provenant du client de configuration ou les accès lorsque la machine Caching Proxy est utilisée en tant que serveur d'origine. Ce fichier journal ne contient pas d'informations sur l'accès à la mémoire cache ou au serveur proxy.

Utilisez la directive NoLog pour spécifier les clients dont vous ne souhaitez pas consigner les accès. Pour obtenir une description de la directive NoLog, voir «NoLog — Supprime les entrées de journal pour des hôtes spécifiques ou des domaines correspondant à un modèle», à la page 245.

Le serveur démarre un nouveau fichier journal chaque jour à minuit s'il est en cours d'exécution. Sinon, le serveur démarre un nouveau fichier journal dès que vous le démarrez. Lors de la création du fichier, le serveur utilise le nom du fichier spécifié et ajoute un suffixe de date. Le suffixe de date apparaît au format *Mmmjjaaaa*, où *Mmm* correspond aux trois premières lettres du mois, *jj* correspond au jour du mois et *aaaa* à l'année.

Remarque : Si vous modifiez les paramètres par défaut du serveur pour l'ID utilisateur, l'ID groupe ou les chemins d'accès au répertoire journal, créez des répertoires et mettez à jour leurs droits d'accès et leurs propriétés. Pour que le serveur puisse enregistrer des informations dans un répertoire de consignation défini par un utilisateur, attribuez à ce répertoire des droits d'accès 755 et définissez l'ID utilisateur du serveur défini par l'utilisateur comme propriétaire. Par exemple, si l'ID utilisateur du serveur est pdupont et que le répertoire de consignation par défaut est `server_root/account`, le répertoire `server_root/account` doit posséder les droits 755 et appartenir à pdupont.

Nous vous recommandons de supprimer les anciens fichiers journaux car ils peuvent occuper un espace disque important sur votre disque dur.

Format

AccessLog
/chemin_répertoire/nom_journal

Exemple

AccessLog /logs/accesslog

Valeurs par défaut

- **Systèmes Linux et UNIX :** AccessLog /opt/ibm/edge/cp/racine_serveur/logs/local
- **Systèmes Windows :** AccessLog *unité:* \Program Files\IBM\edge\cp\logs\local

AccessLogExcludeMethod — Supprime les entrées de fichier journal pour les fichiers et les répertoires demandés par une méthode donnée

Utilisez cette directive pour empêcher la consignation des demandes effectuées selon une méthode particulière pour accéder aux fichiers et répertoires. Par exemple, vous pouvez choisir de ne pas consigner les demandes de suppression pour les fichiers ou les répertoires.

Vous pouvez avoir plusieurs occurrences de cette directive dans votre fichier de configuration. Vous pouvez placer plusieurs méthodes au niveau de la même directive si vous les séparez par un ou plusieurs caractères d'espacement.

Format

AccessLogExcludeMethod *méthode*
[...]

Exemples

AccessLogExcludeMethod GET
AccessLogExcludeMethod PUT
AccessLogExcludeMethod POST
AccessLogExcludeMethod DELETE
AccessLogExcludeMethod GET PUT

Valeur par défaut

Aucun. Le serveur inclut dans le fichier journal des accès les fichiers et les répertoires requis par tous les types de méthode.

AccessLogExcludeMimeType — Supprime les entrées de journal d'accès Proxy pour des types MIME spécifiques

Cette directive permet de spécifier que vous ne voulez pas consigner dans le fichier journal de Proxy les demandes d'accès aux répertoires ou aux fichiers d'un type MIME donné. (text/html, image/gif et image/jpeg constituent des exemples de types MIME.) Par exemple, vous pouvez choisir de ne pas consigner les demandes d'accès pour les images GIF.

Vous pouvez avoir plusieurs occurrences de cette directive dans votre fichier de configuration. Vous pouvez également placer plusieurs types MIME au niveau de la même directive si vous les séparez par un ou plusieurs espaces.

Remarque : Cette directive n'affecte que le journal d'accès Proxy. Vous ne pouvez pas filtrer un journal consignait ces objets mis en cache d'après leurs types MIME. Pour ce faire, utilisez AccessLogExcludeURL.

Format

```
AccessLogExcludeMimeType type_MIME  
[...]
```

Exemple

```
AccessLogExcludeMimeType image/gif  
AccessLogExcludeMimeType text/html  
AccessLogExcludeMimeType image/gif text/html
```

Valeur par défaut

Aucun. Le fichier journal des accès inclut les demandes vers le serveur pour les fichiers et les répertoires de tous les types MIME.

AccessLogExcludeReturnCode — Supprime les entrées de fichier journal pour des codes retour spécifiques

Cette directive permet de spécifier que vous ne voulez pas consigner les demandes d'accès comprises dans une fourchette de numéros de codes d'erreur. Ces codes d'erreur sont des codes de statut de serveur proxy. Vous ne pouvez pas spécifier de codes individuels. Lorsque vous indiquez 300, vous voulez exclure les demandes d'accès comportant des codes de réacheminement (301, 302, 303 et 304).

Vous pouvez avoir plusieurs occurrences de cette directive dans votre fichier de configuration. Vous pouvez également placer plusieurs codes retour au niveau de la même directive si vous les séparez par un ou plusieurs espaces.

Format

```
AccessLogExcludeReturnCode fourchette
```

Exemple

```
AccessLogExcludeReturnCode 300
```

Valeur par défaut

Aucun. Le fichier journal des accès inclut toutes les demandes adressées au serveur, quel que soit le code.

AccessLogExcludeURL — Supprime les entrées de journal pour des répertoires ou des fichiers spécifiques

Cette directive permet de spécifier que vous ne voulez pas consigner les demandes d'accès à des fichiers ou des répertoires spécifiques qui correspondent à un modèle d'URL donné. Par exemple, vous pouvez ne pas consigner les demandes d'accès à des fichiers GIF ou ne pas consigner les demandes d'accès à un fichier ou un répertoire particulier du serveur.

Vous pouvez avoir plusieurs occurrences de cette directive dans votre fichier de configuration. Vous pouvez également placer plusieurs entrées pour la même directive si vous les séparez par un ou plusieurs espaces.

Format

```
AccessLogExcludeURL fichier_ou_type  
[...]
```

Exemples

```
AccessLogExcludeURL *.gif  
AccessLogExcludeURL /Freebies/*  
AccessLogExcludeURL *.gif /Freebies/*
```

Valeur par défaut

Aucun. Le serveur consigne les demandes d'accès à tous les fichiers et répertoires.

AccessLogExcludeUserAgent — Supprime les entrées de journal pour des navigateurs spécifiques

Cette directive permet d'indiquer que vous ne voulez pas consigner les demandes d'accès effectuées par des agents utilisateur spécifiques (par exemple, Internet Explorer 5.0).

Vous pouvez avoir plusieurs occurrences de cette directive dans votre fichier de configuration. Vous pouvez également placer plusieurs entrées pour la même directive si vous les séparez par un ou plusieurs espaces.

Format

```
AccessLogExcludeUserAgent  
agent_utilisateur  
[...]
```

Exemple

```
AccessLogExcludeUserAgent *Mozilla/2.0  
AccessLogExcludeUserAgent *MSIE 5*
```

Valeur par défaut

Par défaut, le fichier `ibmproxy.conf` contient les définitions suivantes pour la directive `AccessLogExcludeUserAgent` :

```
AccessLogExcludeUserAgent IBM_Network_Dispatcher_HTTP_Advisor  
AccessLogExcludeUserAgent IBM_Network_Dispatcher_WTE_Advisor
```

Les agents utilisateur répertoriés ci-dessus sont ceux qui ont été définis pour certains assistants du composant Load Balancer se trouvant généralement devant le serveur Caching Proxy. Pour améliorer les performances en minimisant le nombre d'écritures dans le journal, ces agents utilisateur ne sont pas consignés. Par défaut, les journaux du serveur accèdent aux demandes effectuées pour tous les autres agents utilisateur.

AddBlankIcon — Spécifie l'URL de l'icône utilisée pour aligner les en-têtes des listes de répertoires

Cette directive permet de spécifier une icône à utiliser pour l'alignement des en-têtes au niveau des listes de répertoire qui sont renvoyées lorsque le serveur joue le rôle d'un proxy pour les demandes FTP. Les icônes apparaissent en regard des fichiers associés pour aider les utilisateurs à les différencier.

L'icône peut être vide ou il peut s'agir d'une icône que vous avez choisie pour qu'elle apparaisse au niveau des en-têtes des listes de répertoire. Pour un bon alignement, l'icône utilisée doit être de la même taille que les autres icônes utilisées dans les listes de répertoires.

Format

AddBlankIcon *URL_icône*
texte_de_replacement

URL_icône

Correspond à la dernière partie de l'URL de l'icône. Le serveur ajoute cette valeur à /icons/ pour former la demande d'URL complète. Si la demande concerne un fichier local, le serveur convertit la demande via les directives de mappage. Pour que l'icône soit extraite, les directives de mappage doivent admettre la transmission de la demande.

Si vous utilisez le serveur en tant que proxy, la demande complète doit être constituée d'une URL complète désignant le serveur.

texte_de_replacement

Texte de remplacement à utiliser pour l'icône si le navigateur à l'origine de la demande n'affiche pas de graphiques.

Exemple

AddBlankIcon logo.gif logo

Valeurs par défaut

- **Linux et UNIX** : AddBlankIcon blank.m.pm.gif
- **Windows** : AddBlankIcon blank.gif

La valeur par défaut ne spécifie aucun texte de remplacement étant donné que l'icône est vide.

AddDirIcon — Spécifie l'icône d'URL des répertoires au niveau des listes de répertoire

Cette directive permet de spécifier une icône permettant de représenter un répertoire au niveau d'une liste de répertoire.

Format

AddDirIcon *URL_icône*
texte_de_replacement

URL_icône

Correspond à la dernière partie de l'URL de l'icône. Le serveur ajoute cette valeur à /icons/ pour former la demande d'URL complète. Si la demande concerne un fichier local, le serveur convertit la demande via les directives de mappage. Pour que l'icône soit extraite, les directives de mappage doivent admettre la transmission de la demande.

Si vous utilisez le serveur en tant que proxy, la demande complète doit être constituée d'une URL complète désignant le serveur. Vous devez mapper l'URL vers un fichier local et vous assurer que les directives de mappage permettent la transmission de l'URL.

texte_de_replacement

Texte de remplacement à utiliser pour l'icône si le navigateur à l'origine de la demande n'affiche pas de graphiques.

Exemple

```
AddDirIcon direct.gif DIR
```

Valeurs par défaut

- **Linux et UNIX** : AddDirIcon dir.m.pm.gif DIR
- **Windows** : AddDirIcon dir.gif DIR

AddEncoding — Spécifie le codage du contenu MIME des fichiers avec des suffixes particuliers

Cette directive permet d'associer des fichiers d'un suffixe particulier à un codage MIME particulier. Cette directive est rarement utilisée.

Format

```
AddEncoding .extension codage
```

.extension

Spécifie le modèle de suffixe des fichiers.

codage

Spécifie le type de codage MIME à associer aux fichiers respectant le modèle de suffixe correspondant.

Exemple

```
AddEncoding .qp quoted_printable
```

Valeur par défaut

```
AddEncoding .Z x-compress
```

AddIcon — Associe une icône à un type de contenu ou de codage MIME

Cette directive permet de spécifier des icônes pour la représentation de fichiers avec un type de contenu ou de codage MIME spécifique. Le serveur utilise les icônes au niveau des listes de répertoire, y compris les listes de répertoire FTP.

Format

```
AddIcon URL_icône texte_de_replacement  
modèle_type_MIME
```

URL_icône

Correspond à la dernière partie de l'URL de l'icône. Le serveur ajoute cette valeur à /icons/ pour former la demande d'URL complète. Si la demande concerne un fichier local, le serveur convertit la demande via les directives de mappage. Pour que l'icône soit extraite, les directives de mappage doivent admettre la transmission de la demande.

Si vous utilisez le serveur en tant que proxy, la demande complète doit être constituée d'une URL complète désignant le serveur. Vous devez mapper l'URL vers un fichier local et vous assurer que les directives de mappage permettent la transmission de l'URL.

texte_de_replacement

Texte de remplacement à utiliser pour l'icône si le navigateur à l'origine de la demande n'affiche pas de graphiques.

modèle_type

Spécifie un modèle de type de contenu ou de codage MIME. Les modèles de type de contenu contiennent toujours une barre oblique (/). Les modèles de type de codage ne contiennent jamais de barre oblique.

Exemple

```
AddIcon video_file.m.pm.gif MOV video/*
```

Valeurs par défaut

Plusieurs valeurs par défaut sont définies pour la directive AddIcon dans le fichier de configuration ibmproxy.conf.

AddParentIcon — Spécifie l'URL de l'icône pour un répertoire parent au niveau de la liste de répertoire

Cette directive permet de spécifier une icône permettant de représenter un répertoire parent au niveau des listes de répertoire.

Format

```
AddParentIcon URL_icône texte_de_replacement
```

URL-icône

Correspond à la dernière partie de l'URL de l'icône. Le serveur ajoute cette valeur à /icons/ pour former la demande d'URL complète. Si la demande concerne un fichier local, le serveur convertit la demande via les directives de mappage. Pour que l'icône soit extraite, les directives de mappage doivent admettre la transmission de la demande.

Si vous utilisez le serveur en tant que proxy, la demande complète doit être constituée d'une URL complète désignant le serveur. Vous devez mapper l'URL vers un fichier local et vous assurer que les directives de mappage permettent la transmission de l'URL.

texte_de_replacement

Texte de remplacement à utiliser pour l'icône si le navigateur à l'origine de la demande n'affiche pas de graphiques.

Exemple

```
AddParentIcon parent.gif UP
```

Valeur par défaut

```
AddParentIcon dir-up.gif UP
```

AddType — Spécifie le type de données des fichiers ayant une extension particulière

Cette directive permet d'associer des fichiers ayant un suffixe particulier à un type/sous-type MIME. Vous pouvez avoir plusieurs occurrences de cette directive dans votre fichier de configuration. Le serveur fournit des valeurs par défaut pour les suffixes les plus fréquemment utilisés.

Format

AddType *.extension type/sous-type codage*
[*qualité[jeu_caractères]*]

.extension

Modèle du suffixe de fichier. Vous pouvez utiliser le caractère générique (*) uniquement avec les deux modèles de suffixe spéciaux suivants :

- *.*** Correspond à tous les noms de fichier contenant un point (.) et ne répondant à aucune autre règle.
- *** Correspond à tous les noms de fichier ne comportant pas de point (.) et ne répondant à aucune autre règle.

type/sous-type

Type et sous-type MIME à associer aux fichiers correspondant au modèle de suffixe correspondant.

codage

Codage de contenu MIME auquel ces données ont été converties. Le codage est également utilisé par le serveur proxy FTP pour déterminer si le fichier doit être extrait en mode binaire. Dans la plupart des cas, le codage approprié est 7bit, 8bit ou binaire et est déterminé de la manière suivante :

7bit Les données sont toutes représentées sous la forme de lignes courtes (moins de 1 000 caractères) de données 8859-1 ASCII. Les fichiers de texte ou de code source font généralement partie de cette catégorie. Les fichiers contenant des caractères de traçage de lignes ou des caractères accentués constituent des exceptions.

8bit Les données sont représentées sous forme de lignes courtes, mais peuvent contenir des caractères appartenant au jeu de caractères élevé (des caractères de traçage de ligne ou des caractères accentués, par exemple). Les fichiers PostScript ainsi que les fichiers de texte provenant de sites européens font généralement partie de cette catégorie.

binaire

Vous pouvez utiliser ce codage pour tous les types de données. Les données peuvent contenir non seulement des caractères non ASCII mais également des longues lignes (supérieures à 1 000 caractères). La plupart des fichiers de type image/*, audio/* et video/* font partie de cette catégorie, de même que les fichiers de données binaires de type application/*.

Toute autre valeur de codage subit le même traitement que le codage binaire et est transmise dans des en-têtes MIME en tant qu'en-tête MIME de codage de contenu. Les codages 7bit et 8bit ne sont pas transmis dans des en-têtes MIME.

qualité

Spécifie un indicateur facultatif de valeur relative (sur une échelle de 0.0 à 1.0) pour le type de contenu. La valeur de qualité est utilisée si plusieurs représentations d'un fichier correspondent à une demande. Le serveur sélectionne le fichier associé à la valeur de qualité la plus élevée. Par exemple, si le fichier internet.ps est demandé, et que le serveur dispose des directives AddType suivantes, le serveur utilise la ligne application/postscript car son numéro de qualité est élevé.

```
AddType .ps application/postscript 8bit 1.0
AddType *.* application/binary binary 0.3
```


jeu_caractères

Indicateur facultatif du jeu de caractères à associer aux fichiers de texte. Pour les fichiers auxquels vous attribuez un jeu de caractères, le serveur indique aux navigateurs client le jeu de caractères à utiliser pour l’affichage du fichier. Si vous définissez une valeur pour le champ *jeu_caractères*, vous devez également inclure une valeur pour le champ *qualité*.

Exemple

```
AddType .bin application/octet-stream binary 0.8
```

Valeurs par défaut

Plusieurs paramètres par défaut pour la directive AddType sont contenus dans le fichier de configuration (ibmproxy.conf).

AddUnknownIcon — Spécifie l’URL d’icône pour les types de fichier inconnus au niveau des listes de répertoire

Cette directive permet de spécifier une icône pour la représentation de fichiers dotés d’un type de fichier inconnu au niveau d’une liste de répertoire.

Format

```
AddUnknownIcon URL_icône texte_de_replacement
```

URL_icône

Correspond à la dernière partie de l’URL de l’icône. Le serveur ajoute cette valeur à /icons/ pour former la demande d’URL complète. Si la demande concerne un fichier local, le serveur convertit la demande via les directives de mappage. Pour que l’icône soit extraite, les directives de mappage doivent admettre la transmission de la demande.

Si vous utilisez le serveur en tant que proxy, la demande complète doit être constituée d’une URL complète désignant le serveur. Vous devez mapper l’URL vers un fichier local et vous assurer que les directives de mappage permettent la transmission de l’URL.

texte_de_replacement

Texte de remplacement à utiliser pour l’icône si le navigateur à l’origine de la demande n’affiche pas de graphiques.

Exemple

```
AddUnknownIcon saywhat.gif unknown
```

Valeurs par défaut

- **Linux et UNIX** : AddUnknownIcon unknown.gif ???
- **Windows** : AddUnknownIcon unknown.gif ???

AdminPort — Spécifie le port pour les demandes de pages ou de formulaires d’administration

Cette directive permet de spécifier un port pouvant être utilisé par les administrateurs pour accéder aux pages de statut du serveur ou aux formulaires de configuration. Les demandes vers ce port ne sont pas placées en file d’attente avec les autres demandes en entrée au niveau du port standard défini par la directive Port. Cependant, les demandes au niveau de l’élément AdminPort passent par les mêmes règles de mappage de demande et de contrôle d’accès (Pass, Exec, Protect, par exemple).

Remarque : Le port d'administration ne doit *pas* être le(s) port(s) standard défini par la directive Port.

Format

AdminPort *numéro_port*

Exemple

AdminPort 2001

Valeur par défaut

AdminPort 8008

AggressiveCaching — Spécifie la mise en mémoire en cache des fichiers ne pouvant pas être mis en mémoire cache

Cette directive permet de spécifier si les fichiers renvoyés par le serveur d'origine et pour lesquels il est indiqué qu'ils ne peuvent être mis en mémoire cache doivent l'être malgré tout. Les fichiers ne pouvant être placés en mémoire cache, et qui le sont malgré tout selon cette directive, sont marqués à revalider. Chaque fois que le fichier est demandé, le serveur proxy envoie une demande If-Modified-Since au serveur d'origine afin de valider à nouveau la réponse avant qu'elle ne soit traitée par la mémoire cache. A l'heure actuelle, les seuls fichiers concernés par cette directive sont les réponses provenant du serveur d'origine contenant un en-tête cache-control : no cache/xph>. Cette directive peut être spécifiée plusieurs fois.

Format

AggressiveCaching *modèle_URL*

Exemples

AggressiveCaching http://www.hôtea.com/*

AggressiveCaching http://www.hôteb.com/*

Par assurer la compatibilité en amont, la syntaxe précédente de cette directive (AggressiveCaching {on | off}) est désormais traitée comme suit :

AggressiveCaching on est traité comme AggressiveCaching * .

AggressiveCaching off est ignoré.

Remarque : Si AggressiveCaching off et AggressiveCaching *modèle_URL* sont spécifiés, AggressiveCaching off est ignoré et un message d'avertissement s'affiche.

Valeur par défaut

Aucun

AlwaysWelcome — Indique de rechercher les fichiers de bienvenue dans le répertoire demandé

Lorsque les demandes contiennent un nom de répertoire et aucun nom de fichier, la directive AlwaysWelcome vérifie que le serveur recherche dans le répertoire un fichier de bienvenue à renvoyer. Par défaut, la directive AlwaysWelcome a pour valeur on. Cela signifie que le serveur recherche toujours dans le répertoire demandé un fichier correspondant au nom indiqué dans une directive Welcome. Si une correspondance est trouvée, le fichier est renvoyé au demandeur. Si le serveur trouve plusieurs correspondances entre les noms de fichier d'un répertoire et ceux

des directives Welcome, l'ordre d'apparition des directives Welcome détermine le fichier renvoyé. Le serveur utilise la première directive Welcome concordante du fichier de configuration.

Format

`AlwaysWelcome on | off`

Valeur par défaut

`AlwaysWelcome on`

Directives connexes

- «Welcome — Spécifie le nom des fichiers de bienvenue», à la page 292

appendCRLFtoPost — Ajoute CRLF aux demandes POST

Cette directive permet de spécifier des URL pour lesquelles Caching Proxy doit ajouter des caractères de saut de ligne et de retour chariot à la fin du corps d'une demande POST. Cette directive peut être spécifiée plusieurs fois.

Remarque : Cette directive ne doit être spécifiée que pour les URL pour lesquelles un incident a été détecté lors du traitement des demandes POST.

Format

`appendCRLFtoPost modèle_URL`

Exemple

`appendCRLFtoPost http://www.hosta.com/`

Valeur par défaut

Aucun

ArrayName — Attribue un nom au tableau de la mémoire cache à distance

Cette directive permet de spécifier le tableau de la mémoire cache à distance à partager par les serveurs.

Remarque : Lors de la configuration d'un tableau, la directive Hostname doit être configuré de la même manière pour tous les membres du tableau.

Format

`ArrayName nom_tableau`

Valeur par défaut

Aucun

Authentication — Personnalise l'étape d'authentification

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de l'étape d'authentification du processus de demande de serveur. Ce code est exécuté en suivant le schéma d'authentification. Seule l'authentification BASIC est prise en charge.

Remarque : L'authentification fait partie du processus d'autorisation. Elle a lieu uniquement lorsque des droits d'accès sont requis.

Format

Authentication *type*
/chemin/fichier:nom_fonction

type

Spécifie un schéma d'authentification qui détermine ultérieurement si la fonction d'application est appelée. Les deux valeurs possibles sont un astérisque (*) et BASIC.

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme.

Exemple

Authentication (BASIC) /ics/api/bin/icsextpgm.so:basic_authentication

Valeur par défaut

Aucun

Authorization — Personnalise l'étape d'autorisation

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de l'étape d'autorisation du processus de demande de serveur. Ce code vérifie que l'objet demandé peut être servi au client.

Format

Authorization *modèle_demande*
/chemin/fichier:nom_fonction

modèle_demande

Spécifie un modèle pour les demandes qui déterminent ultérieurement si la fonction d'application est appelée. La spécification peut inclure le protocole, le domaine et l'hôte. Elle peut être précédée d'une barre oblique (/) et peut utiliser un astérisque (*) en tant que caractère générique. Par exemple, /front_page.html, http://www.ics.raleigh.ibm.com, /pub*, /* et * sont tous valides. Lorsque vous utilisez Caching Proxy comme proxy inversé, le modèle de la demande doit commencer par la racine du document (/).

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme.

Exemple

Authorization /index.html /api/bin/icsextpgm.so:auth_url

Valeur par défaut

Aucun

AutoCacheRefresh — Spécifie si la régénération de la mémoire cache doit être utilisée

Cette directive permet d'activer ou de désactiver la régénération de la mémoire cache. Si cette fonction est activée, la mémoire cache est automatiquement régénérée. Si elle est désactivée, l'agent de la mémoire cache n'est pas appelé et

tous ses paramètres sont ignorés. Si vous lancez l'agent de la mémoire cache en utilisant une autre méthode, par exemple en exécutant un travail **cron** sur des systèmes Linux et UNIX, désactivez cette directive.

Format

AutoCacheRefresh {on | off}

Valeur par défaut

AutoCacheRefresh On

BindSpecific — Spécifie si le serveur est lié à une ou à plusieurs adresses IP

Sur un système connecté à plusieurs réseaux, cette directive indique si le serveur contrôle une seule adresse réseau. Si la valeur correspond à `On`, le serveur se connecte à l'adresse IP indiquée dans la directive `Hostname` au lieu de se connecter à toutes les adresses locales.

Si cette directive n'est pas spécifiée, le serveur est lié au nom d'hôte par défaut.

Si vous modifiez cette directive, vous devez arrêter manuellement le serveur puis le redémarrer. La modification n'est pas prise en compte si vous redémarrez le serveur sans l'arrêter. (Voir Chapitre 5, «Démarrage et arrêt de Caching Proxy», à la page 15.)

Format

BindSpecific {on | off} [OutgoingSrcIp *adresse_ip* | *nom_hôte*]

[**OutgoingSrcIp** *adresse_ip* | *nom_hôte*]

L'option `OutgoingSrcIp` permet à Caching Proxy d'utiliser une adresse IP source spécifique pour établir des connexions sortantes. Elle est utile pour les paramètres Caching Proxy dans DMZ et lorsque les règles de pare-feu le requiert.

Valeur par défaut

BindSpecific Off

BlockSize — Définit la taille des blocs sur l'unité de mémoire cache

Cette directive permet de spécifier la taille (en octets) des blocs dans l'unité de mise en mémoire cache. La valeur par défaut est de 8192. Comme il s'agit de la seule taille prise en charge, ne la modifiez pas. Pour plus d'informations, voir la section de référence «htcformat, commande», à la page 170.

Format

BlockSize *taille*

Valeur par défaut

Par défaut, le fichier de configuration ne contient pas de valeur pour ce paramètre. (La valeur par défaut est de 8192.)

CacheAccessLog — Spécifie le chemin des fichiers journaux des accès à la mémoire cache

Cette directive permet d'identifier le chemin et le nom du fichier dans lequel le serveur doit stocker un journal des accès à la mémoire cache du proxy. Cette

directive est valide uniquement si le serveur est exécuté en tant que proxy. Pour plus d'informations, voir «CacheRefreshTime — Indique à quel moment démarrer l'agent de la mémoire cache», à la page 198.

Pour activer la consignation des demandes adressées à la mémoire cache du proxy, la directive Caching doit avoir la valeur ON, et des valeurs doivent être définies pour les directives CacheMemory et CacheAccessLog. Vous pouvez également définir une ou plusieurs unités de mémoire cache à l'aide de la directive CacheDev.

La valeur de CacheAccessLog peut être soit un chemin absolu soit un chemin relatif d'accès à la racine du serveur. (Des exemples sont fournis.)

Format

CacheAccessLog *chemin/fichier*

Exemples

CacheAccessLog /absolute/path/logfile
CacheAccessLog /logs/logfile

Valeurs par défaut

- **Systèmes Linux et UNIX** : CacheAccessLog /opt/ibm/edge/cp/racine_serveur/logs/cache
- **Systèmes Windows** : CacheAccessLog *unité*:\Program Files\IBM\edge\cp\logs\cache

CacheAlgorithm — Identifie l'algorithme de mémoire cache

Cette directive permet de spécifier l'algorithme de mémoire cache utilisée par le serveur lors de la récupération d'espace.

Format

CacheAlgorithm {bandwidth | responsetime | blend}

bandwidth

Tente de maximiser l'économie de largeur de bande réseau.

responsetime

Tente de réduire le temps de réponse pour l'utilisateur.

blend

Combinaison équilibrée de bandwidth et de responsetime

Valeur par défaut

CacheAlgorithm bandwidth

CacheByIncomingUrl — Spécifie la base pour la génération des noms de fichier de mémoire cache

Cette directive permet de spécifier si les noms de fichier de mémoire cache générés dépendent de l'URL d'entrée de la demande.

Si la directive a la valeur on, les noms de fichier de mémoire cache dépendent de l'URL d'entrée. Si la directive est associée à la valeur off, l'URL d'entrée transite d'abord via tous les plug-ins de conversion de nom applicables, les règles MAP et les règles PROXY, puis le nom de fichier de mémoire cache généré est basé sur l'URL résultante.

Remarque : Lorsque vous définissez des filtres de cache dans le cas d'un proxy inversé avec des filtres de cache de type URL, utilisez un format commençant par le répertoire racine d'un document / (barre oblique). Par exemple : /test/index.html. Le format ne doit *pas* inclure de protocole, par exemple, *http://*.

Format

CacheByIncomingUrl {on | off}

Valeur par défaut

CacheByIncomingURL off

CacheClean — Indique la durée de conservation des fichiers en mémoire cache

Cette directive permet de spécifier la durée de conservation des fichiers mis en mémoire cache. Lorsque la récupération de place s'exécute, le serveur supprime les fichiers en mémoire cache qui ont dépassé cette durée, et ce quelle que soit la date d'expiration de ces fichiers. Chaque fois qu'un fichier ayant dépassé la durée fixée est demandé, le serveur valide à nouveau le fichier avant de le fournir afin de garantir sa validité.

Format

CacheClean *spécification_durée*

Exemple

CacheClean 2 semaines

Valeur par défaut

CacheClean 1 mois

CacheDefaultExpiry — Indique l'heure d'expiration par défaut des fichiers

Cette directive permet de définir une heure d'expiration par défaut pour les fichiers auxquels le serveur n'a pas attribué d'en-tête Expires ou Last-Modified. Indiquez un modèle d'URL et une heure d'expiration pour les fichiers ayant des URL correspondant au modèle. Vous pouvez avoir plusieurs occurrences de cette directive dans le fichier de configuration. Incluez une directive séparée pour chaque modèle. Le modèle d'URL doit inclure le protocole. Indiquez la valeur de temps en utilisant n'importe quelle combinaison de mois, semaines, jours et heures.

Format

CacheDefaultExpiry *modèle_URL*
heure_expiration

Valeurs par défaut

CacheDefaultExpiry ftp:* 1 jour
CacheDefaultExpiry gopher:* 2 jours
CacheDefaultExpiry http:* 0 jour

Remarque : La valeur d'expiration par défaut pour le protocole HTTP est de 0 jours. Il est conseillé de conserver cette valeur car de nombreux programmes de script ne fournissent pas de date d'expiration et leur résultat expire donc immédiatement. Une valeur différente de 0 pourrait amener les clients à voir un contenu périmé.

CacheDev — Spécifie l'unité de stockage de la mémoire cache

Cette directive permet de spécifier une unité de mise en mémoire cache. Vous pouvez spécifier soit un fichier soit une partition de disque. Sur des plateformes AIX, vous pouvez spécifier un volume logique. (Si vous n'utilisez pas de mémoire cache, la mise en mémoire cache sur disque offre les meilleures performances.)

Il est à noter que les unités de mise en mémoire cache doivent être préparées avant de pouvoir être spécifiées. Pour préparer une unité de mise en mémoire cache, formatez-la à l'aide de la commande **htcformat**. Pour plus d'informations, voir «htcformat, commande», à la page 170.

Vous pouvez spécifier plusieurs unités de mise en mémoire cache. Chaque unité sera associée aux mêmes valeurs CacheMemory et BlockSize. Cependant, chaque unité de mise en mémoire cache représente une surcharge de mémoire sur le serveur proxy d'environ 8 Mo. Un petit nombre d'unités de grande taille est plus efficace que de nombreuses unités de petite taille. Pour une meilleure efficacité, utilisez un disque entier en tant que partition de taille importante. Vous trouverez des informations détaillées sur la mise en mémoire cache à la section «Optimisation des performances du cache disque», à la page 107.

Format

CacheDev {*partition_disque_brut* | *fichier*}

Exemples

AIX : CacheDev /dev/r1v02

HP-UX : CacheDev /dev/rdsk/clt15d0

Linux : CacheDev /opt/IBMWTE/filecache1

Solaris : CacheDev /dev/rdsk/clt3d0s0

Windows : CacheDev \\.\E:

Valeur par défaut

Aucun

CacheExpiryCheck — Indique si le serveur renvoie les fichiers expirés

Cette directive permet d'indiquer si le serveur doit renvoyer les fichiers mis en mémoire cache qui ont expiré. Entrez Off pour la valeur si vous voulez que le serveur puisse renvoyer les fichiers ayant expiré. Utilisez la valeur par défaut On si vous voulez que le proxy cherche dans le serveur d'origine une version plus récente lorsque le client demande un fichier ayant expiré. En principe, les administrateurs ne souhaitent pas que le serveur renvoie des fichiers expirés, sauf s'ils travaillent en mode démonstration et que le contenu renvoyé par le serveur ne présente aucun intérêt en lui-même.

Format

CacheExpiryCheck {on | off}

Valeur par défaut

CacheExpiryCheck On

CacheFileSizeLimit — Spécifie la taille maximale des fichiers à placer en mémoire cache

Cette directive permet d'indiquer la taille maximale des fichiers à mettre en mémoire cache. Les fichiers supérieurs à cette taille ne seront pas mis en mémoire cache. La valeur peut être spécifiée en octets (O), kilooctets (K) ou en gigaoctets (G). Vous pouvez éventuellement insérer un caractère d'espacement entre le nombre et la valeur (O, K, M, G).

Format

CacheFileSizeLimit *maximum* {B | K | M | G}

Valeur par défaut

CacheFileSizeLimit 4000 K

CacheLastModifiedFactor — Spécifie la valeur permettant de déterminer les dates d'expiration

Cette directive permet d'indiquer la valeur à utiliser pour calculer les dates d'expiration pour des URL spécifiques ou pour toutes les URL correspondant à un modèle.

Les serveurs HTTP attribuent fréquemment une heure de dernière modification à un fichier mais non une date d'expiration. De même, les fichiers FTP peuvent avoir un horodatage de dernière modification mais ne possèdent pas d'heure d'expiration. Caching Proxy calcule une heure d'expiration pour ces fichiers en fonction de l'heure de dernière modification. Il utilise l'heure de dernière modification pour déterminer depuis combien de temps le fichier a été modifié et il multiplie cette durée par la valeur de la directive CacheLastModifiedFactor. Le résultat de ce calcul correspond à la durée de vie du fichier ou la période pendant laquelle il est encore valide.

Vous pouvez également entrer off ou -1 pour désactiver la directive et ne pas calculer de date d'expiration. Le serveur proxy lit les directives CacheLastModifiedFactor dans l'ordre dans lequel elles apparaissent dans le fichier de configuration. Il utilise la première directive qu'il peut appliquer au fichier mis en mémoire cache.

Format

CacheLastModifiedFactor *url* *facteur*

url

Spécifie l'URL complète, y compris le protocole du fichier mis en mémoire cache. Vous pouvez utiliser un modèle d'URL avec des astérisques (*) en tant que caractères génériques pour appliquer un masque.

facteur

Indique le facteur à utiliser pour le calcul. Les valeurs off ou -1 peuvent également être spécifiées.

Exemples

CacheLastModifiedFactor	*://hôtea/*	off
CacheLastModifiedFactor	ftp://hôteb/*	0.30
CacheLastModifiedFactor	ftp://*	0.25
CacheLastModifiedFactor	http://*	0.10
CacheLastModifiedFactor	*	0.50

Valeurs par défaut

```
CacheLastModifiedFactor http://*/ 0.10
CacheLastModifiedFactor http://*.htm* 0.20
CacheLastModifiedFactor http://*.gif 1.00
CacheLastModifiedFactor http://*.jpg 1.00
CacheLastModifiedFactor http://*.jpeg 1.00
CacheLastModifiedFactor http://*.png 1.00
CacheLastModifiedFactor http://*.tar 1.00
CacheLastModifiedFactor http://*.zip 1.00
CacheLastModifiedFactor http:* 0.15
CacheLastModifiedFactor ftp:* 0.50
CacheLastModifiedFactor * 0.10
```

La valeur par défaut 0.14 fait que les fichiers modifiés la semaine précédente expirent en un jour.

CacheLocalDomain — Indique s'il est nécessaire de mettre le domaine local en mémoire cache

Cette directive permet d'indiquer s'il faut mettre en mémoire cache les URL provenant d'hôtes du même domaine que le proxy. Les sites locaux du réseau interne ne nécessitent généralement pas de mise en mémoire cache car la largeur de bande interne est suffisante pour charger les URL rapidement. En ne mettant pas en mémoire cache les sites locaux, vous conservez de l'espace en mémoire cache pour les URL pour lesquelles le temps d'extraction est plus long.

Format

```
CacheLocalDomain {on | off}
```

Valeur par défaut

```
CacheLocalDomain on
```

CacheMatchLanguage — Définition de la préférence de langue pour le contenu du cache renvoyé

Si le serveur dorsal est en mesure de renvoyer différentes langues aux clients pour la même adresse URL, utilisez cette directive pour prendre en charge la mise en cache de différentes langues pour une même adresse. Cette directive permet à Caching Proxy de vérifier la préférence de langue définie dans les requêtes par rapport à la langue de la réponse mise en cache.

Lorsque l'option CacheMatchLanguage est activée, le système compare la préférence de langue indiquée dans l'en-tête Accept-Language de la requête à la langue du contenu disponible en cache. Caching Proxy compare l'écart des préférences. Si l'écart de préférences est inférieur à la limite indiquée, le système renvoie la copie en mémoire cache ; Dans le cas contraire, le serveur proxy réachemine la demande au serveur dorsal pour obtenir une copie récente dans la langue demandée.

Format

```
CacheMatchLanguage {on | off} lang-prefer-distance-limit special-id-for-all-lang
```

lang-prefer-distance-limit

Indiquez une valeur dans la plage 0.001– 0.9999.

special-id-for-all-lang

Indiquez une langue renvoyée par le serveur dans l'en-tête Content-Language pour informer le serveur proxy que la réponse peut être utilisée pour toutes les préférences de langue.

Exemples

Voici un exemple de configuration de la directive, de l'objet en cache et de la demande.

```
CacheMatchLanguage On 0.2
```

Si l'objet en cache correspond au chinois simplifié (zh_cn) et que la requête est :

```
GET / HTTP/1.1
```

```
...
```

```
Accept-Language: en_US;q=1.0, zh_cn;q=0.7, ja;q=0.3
```

```
....
```

Dans cet exemple, l'utilisateur demande une page en anglais (associée au code et au niveau en_US/1.0), en chinois simplifié (associée au code et au niveau zh_cn/0.7), puis en japonais (associée au code et au niveau ja/0.3). L'objet mis en cache est en chinois simplifié. L'écart de préférences entre le niveau optimal prévu et le niveau de langue disponible est $1.0 - 0.7 = 0.3$. Comme la directive CacheMatchLanguage est associée à la valeur 0.2, le serveur proxy demande au serveur une nouvelle copie de cette adresse URL au lieu de renvoyer l'objet disponible en cache.

Si le serveur n'indique pas de page spécifique ni de valeur special-id-for-all-lang dans l'en-tête Content-Language lors du renvoi de la réponse, le serveur proxy ne prend pas en compte la préférence de langue et renvoie la copie disponible en cache.

Valeur par défaut

```
CacheMatchLanguage off
```

CacheMaxExpiry — Spécifie la durée de vie maximale des fichiers en mémoire cache

Cette directive permet de définir la durée maximale pendant laquelle les fichiers peuvent rester en mémoire cache. La durée de vie d'un fichier mis en mémoire cache correspond à la durée pendant laquelle il peut être transmis à partir de la mémoire cache sans vérification de l'origine des mises à jour. Dans certains cas, la durée de vie calculée pour un fichier mis en mémoire cache peut être supérieure à la durée pendant laquelle vous désirez conserver ce fichier. La durée de vie du fichier, soit spécifiée par l'origine, soit calculée par Caching Proxy, ne peut pas être supérieure à la limite spécifiée par la directive CacheMaxExpiry.

Vous pouvez avoir plusieurs occurrences de cette directive dans le fichier de configuration. Incluez une directive séparée pour chaque modèle.

Format

```
CacheMaxExpiry URL durée
```

URL

Spécifie l'URL complète, y compris le protocole, du fichier mis en mémoire cache. Vous pouvez utiliser un modèle d'URL avec des astérisques (*) en tant que caractères génériques pour appliquer un masque.

durée de vie

Indique la durée de vie maximale pour les fichiers en mémoire cache correspondant aux modèles d'URL. La durée peut être spécifiée en associant des mois, des semaines, des jours, des heures, des minutes et des secondes.

Exemples

CacheMaxExpiry ftp:* 1 mois

CacheMaxExpiry http://www.santaclaus.np/* 2 jours 12 heures

Valeur par défaut

CacheMaxExpiry 1 mois

CacheMemory — Spécifie la mémoire vive de la mémoire cache

Cette directive permet de spécifier la quantité de mémoire à associer à la mémoire cache. Pour optimiser les performances des mémoires cache sur disque, un minimum de 64 Mo de mémoire cache est recommandé pour la prise en charge de l'infrastructure de mise en cache, y compris l'index de la mémoire cache. L'index de la mémoire cache augmente à mesure que la taille de la mémoire cache augmente, de sorte que l'espace mémoire nécessaire pour stocker l'index s'accroît également. Une mémoire cache de 64 Mo suffit pour prendre en charge l'infrastructure de mise en cache et pour stocker un index de mémoire cache pour une mémoire cache sur disque d'environ 6,4 Go. Les mémoires cache sur disque plus volumineuses doivent avoir une fois et demie la taille de la mémoire cache.

Si la mise en mémoire cache est utilisée, ce paramètre doit inclure la mémoire cache plus la quantité de mémoire nécessaire pour l'index de la mémoire cache.

La valeur maximale conseillée pour ce paramètre est 1600 Mo. Cette limite est déterminée par le fait que Caching Proxy, en tant qu'application 32 bits, peut utiliser 2 Go de mémoire au maximum. Si la quantité de mémoire nécessaire pour la mémoire cache plus celle utilisée pour le traitement des routines approchent ou dépassent 2 Go, Caching Proxy ne fonctionnera pas correctement.

La quantité peut être spécifiée en octets (b), kilo-octets (K) et gigaoctets (G).

Format

CacheMemory *quantité* {B | K | M | G}

Valeur par défaut

CacheMemory 64 M

CacheMinHold — Indique la durée de disponibilité des fichiers

Cette directive permet de spécifier les URL des fichiers dont la date d'expiration doit être ignorée. Certains sites définissent une date d'expiration des fichiers antérieure à leur durée de vie, ce qui oblige le serveur à demander le fichier plus fréquemment. La directive CacheMinHold permet de conserver le fichier expiré en mémoire cache pendant la durée indiquée avant de le redemander. Cette directive peut être spécifiée plusieurs fois.

Remarque : Si les dates d'expiration sont ignorées, les fichiers en mémoire cache peuvent devenir obsolètes ou périmés.

Exemple

CacheMinHold http://www.cachebusters.com/* 1 heure

Valeur par défaut

Aucun

CacheNoConnect — Spécifie le mode de mémoire cache autonome

Cette directive permet d'indiquer si le serveur proxy doit récupérer les fichiers à partir de serveurs distants. La valeur par défaut (Off) indique que le serveur proxy doit extraire les fichiers se trouvant sur des serveurs distants. La valeur On impose l'exécution du serveur en mode de mémoire cache autonome. De cette manière, le serveur peut renvoyer uniquement les fichiers déjà stockés dans sa mémoire cache. Généralement, vous attribuez également la valeur Off à la directive CacheExpiryCheck lors de l'exécution du serveur avec ce mode.

L'exécution du serveur en mode mémoire cache autonome peut être utile si vous utilisez le serveur pour des démonstrations. Si vous savez que tous les fichiers que vous voulez utiliser pour la démonstration sont présents en mémoire cache, vous n'avez pas besoin de connexion réseau.

Format

CacheNoConnect {on | off}

Valeur par défaut

CacheNoConnect Off

CacheOnly — Met en mémoire cache uniquement les fichiers dont les URL correspondent à un modèle

Cette directive permet de définir que seuls les fichiers ayant des URL correspondant à un modèle donné doivent être mis en mémoire cache. Vous pouvez avoir plusieurs occurrences de cette directive dans le fichier de configuration. Incluez une directive séparée pour chaque modèle. Le modèle d'URL doit inclure le protocole. Si aucune valeur n'est définie pour cette directive, toute URL ne répondant à aucune directive NoCaching peut être placée en mémoire cache. Si le fichier de configuration ne contient ni directive CacheOnly ni directive NoCaching, n'importe quelle URL peut être mise en mémoire cache.

Format

CacheOnly *modèle_URL*

Exemple

CacheOnly http://vraitruc/*

Valeur par défaut

Aucun

CacheQueries — Met en mémoire cache les réponses aux URL contenant le caractère ?

Cette directive permet de spécifier les URL pour lesquelles les réponses aux demandes de requête doivent être mises en mémoire cache. Si la valeur PUBLIC *modèle_URL* est utilisée, les réponses aux demandes GET contenant un point d'interrogation dans l'URL seront mises en mémoire cache si le serveur d'origine comprend un en-tête cache-control: public et que la réponse peut être mise en mémoire cache. Si la valeur ALWAYS *modèle_URL* est spécifiée, les réponses aux demandes GET contenant un point d'interrogation dans l'URL sont stockées dans la mémoire cache à condition que la réponse puisse être mise en mémoire cache.

Cette directive peut être spécifiée plusieurs fois.

```
CacheQueries {ALWAYS | PUBLIC}  
modèle_URL
```

Exemples

```
CacheQueries ALWAYS http://www.hosta.com/*  
CacheQueries PUBLIC http://www.hostb.com/*
```

Remarque : Pour assurer la compatibilité amont, la syntaxe précédente de `CacheQueries {ALWAYS | PUBLIC | NEVER}` est traitée comme suit :

- `CacheQueries ALWAYS` et `CacheQueries PUBLIC` sont traitées comme `CacheQueries ALWAYS *` et `CacheQueries PUBLIC *`.
- `CacheQueries NEVER` est ignorée.
- Si `CacheQueries NEVER` et `CacheQueries modèle_URL` sont toutes deux spécifiées, `CacheQueries NEVER` est ignorée mais un message d'avertissement est affiché.

Valeur par défaut

Aucun

CacheRefreshInterval — Indique l'intervalle de temps pour la revalidation des objets placés en mémoire cache

Cette directive permet d'indiquer à quel moment effectuer une vérification auprès du serveur d'origine pour déterminer si un fichier en mémoire cache a changé.

Bien que `CacheClean` semble être similaire à cette directive, il existe une différence. `CacheRefreshInterval` fait uniquement en sorte que le proxy valide à nouveau le document avant de l'utiliser alors que `CacheClean` fait en sorte que le fichier soit supprimé de la mémoire cache après une durée définie.

Format

- Le format suivant définit l'intervalle de régénération pour les fichiers correspondant au modèle d'URL :

```
CacheRefreshInterval  
modèle_URL durée
```

- Le format suivant définit l'intervalle de régénération pour les fichiers qui ne correspondent *pas* à un modèle d'URL. Seul un intervalle de régénération est spécifié.

```
CacheRefreshInterval  
durée
```

Exemples

```
CacheRefreshInterval *.gif 8 heures  
CacheRefreshInterval 1 semaine
```

Valeur par défaut

`CacheRefreshInterval 2 semaines`

CacheRefreshTime — Indique à quel moment démarrer l'agent de la mémoire cache

Cette directive permet de spécifier le moment du démarrage de l'agent de la mémoire cache. Vous pouvez démarrer l'agent de la mémoire cache à un moment spécifique.

Format

CacheRefreshTime *HH:MM*

Valeur par défaut

CacheRefreshTime 03:00

CacheTimeMargin — Indique la durée minimale de mise en mémoire cache d'un fichier

La directive CacheTimeMargin détermine si la durée de vie minimale d'un fichier est suffisante pour que ce dernier soit mis en mémoire cache.

Caching Proxy calcule une heure d'expiration pour chaque fichier. S'il est peu probable qu'une autre demande soit reçue concernant le fichier avant expiration du délai, Caching Proxy considère que la durée de vie du fichier est trop courte pour justifier la mise en mémoire cache de ce dernier. Par défaut, Caching Proxy ne met pas en mémoire cache les fichiers dont la durée de vie est inférieure à 10 minutes. Si la mémoire cache ne se rapproche pas de sa capacité maximale, laissez la valeur initiale pour la directive. Si la mémoire cache est proche de la saturation, vous pouvez envisager d'augmenter la valeur de la durée de vie minimale.

Format

CacheTimeMargin *durée_de_vie_minimum*

Valeur par défaut

CacheTimeMargin 10 minutes

Remarque : Si vous attribuez une valeur supérieure à quatre heures, vous réduisez de manière importante l'efficacité de la mémoire cache.

CacheUnused — Indique la durée de conservation des fichiers en mémoire cache et non utilisés

Cette directive permet de définir la durée maximale pendant laquelle conserver en mémoire cache les fichiers non utilisés et ayant des URL correspondant à un modèle donné. Le serveur supprime les fichiers non utilisés ayant des URL correspondant au modèle une fois qu'ils ont été mis en mémoire cache pour la durée spécifiée, quelle que soit la date d'expiration. Vous pouvez utiliser plusieurs occurrences de cette directive dans le fichier de configuration. Incluez une directive séparée pour chaque modèle. Le modèle d'URL doit inclure le protocole. Indiquez la valeur de temps en utilisant n'importe quelle combinaison de mois, semaines, jours et heures.

Format

CacheUnused *modèle_URL*
durée

Exemples

CacheUnused ftp:* 3 semaines
CacheUnused gopher:* 3 jours 12 heures
CacheUnused * 4 semaines

Valeurs par défaut

CacheUnused ftp:* 3 days
CacheUnused gopher:* 12 hours
CacheUnused http:* 2 days

Caching — Active la mémoire cache du serveur proxy

Cette directive permet d'activer la mise en mémoire cache des fichiers. Lorsque la mise en mémoire cache est activée, le serveur proxy place les fichiers extraits des autres serveurs dans une mémoire cache locale. Le serveur proxy répond ensuite aux demandes suivantes pour les mêmes fichiers sans avoir à les extraire d'autres serveurs.

Format

Caching {on | off}

Valeur par défaut

Caching On

Remarque : Si vous modifiez la directive Caching, vous devez arrêter manuellement le serveur puis le redémarrer. (Voir Chapitre 5, «Démarrage et arrêt de Caching Proxy», à la page 15.)

CompressAge — Indique à quel moment compresser les fichiers journaux

Cette directive permet de spécifier au bout de combien de temps les fichiers journaux sont compressés. Lorsque les journaux sont plus anciens que la valeur définie pour CompressAge, ils sont compressés. Si CompressAge a la valeur 0, les journaux ne sont jamais compressés. Les journaux de la journée en cours et de la veille ne sont jamais compressés.

Format

CompressAge *nombre_de_jours*

Valeur par défaut

CompressAge 1

Directives connexes

- «CompressDeleteAge — Indique à quel moment supprimer les journaux», à la page 201
- «CompressCommand — Spécifie la commande et les paramètres de compression»
- «LogArchive — Définit le comportement de la fonction d'archivage du journal», à la page 234
- «Midnight — Identifie le plug-in API permettant d'archiver les fichiers journaux», à la page 243
- «PurgeAge — Spécifie la limite d'âge pour un journal», à la page 268
- «PurgeSize — Spécifie la taille limite d'un fichier journal d'archivage», à la page 269

CompressCommand — Spécifie la commande et les paramètres de compression

Cette directive permet de créer une commande qui identifie l'utilitaire de compression permettant de compacter les journaux et transmet les paramètres à cet utilitaire. Indiquez le chemin des journaux archivés.

L'utilitaire de compression doit être installé dans un répertoire se trouvant dans le chemin d'accès pour cette machine.

Format

CompressCommand *commande*

commande

Inclut la commande et les paramètres à utiliser, sur une seule ligne.
Généralement, les paramètres incluent %%FICHIERSJOURNAUX%% et %%DATE%%.

%%FICHIERSJOURNAUX%%

Correspond à la liste des fichiers journaux disponibles pour une %%DATE%% particulière.

%%DATE%%

Spécifie la valeur de date d'un fichier journal.

Exemples

• Linux et UNIX :

```
CompressCommand tar -cf /logarchs/log%%DATE%%.tar %%FICHIERSJOURNAUX%% ;  
gzip /logarchs/log%%DATE%%.tar  
CompressCommand tar -cf /logarchs/log%%DATE%%.tar %%FICHIERSJOURNAUX%% ;  
compress /logarchs/log%%DATE%%.tar  
CompressCommand zip -q /logarchs/log%%DATE%%.zip %%FICHIERSJOURNAUX%%
```

Remarque : La commande et tous les paramètres doivent être entrés sur une seule ligne. Dans les exemples qui précèdent, les deux premiers exemples de commande sont divisés pour plus de lisibilité.

• Sous Windows :

```
CompressCommand pkzip -q d:\logarchs\log%%DATE%%.tar %%FICHIERSJOURNAUX%%
```

Valeur par défaut

Aucun

Directives connexes

- «CompressAge — Indique à quel moment compresser les fichiers journaux», à la page 200
- «CompressDeleteAge — Indique à quel moment supprimer les journaux»
- «LogArchive — Définit le comportement de la fonction d'archivage du journal», à la page 234
- «Midnight — Identifie le plug-in API permettant d'archiver les fichiers journaux», à la page 243
- «PurgeAge — Spécifie la limite d'âge pour un journal», à la page 268
- «PurgeSize — Spécifie la taille limite d'un fichier journal d'archivage», à la page 269

CompressDeleteAge — Indique à quel moment supprimer les journaux

Cette directive permet de spécifier le moment de suppression d'un journal après sa compression. Lorsqu'un journal est antérieur au nombre de jours définis pour CompressDeleteAge, il est supprimé. Si CompressDeleteAge a la valeur 0, ou si sa valeur est inférieure à celle définie pour la directive CompressAge, aucun journal n'est supprimé.

Remarque : Le plug-in de compression ne supprime jamais les journaux du jour en cours ou du jour précédent.

Format

`CompressDeleteAge nombre_de_jours`

Valeur par défaut

`CompressDeleteAge 7`

Directives connexes

- «`CompressAge` — Indique à quel moment compresser les fichiers journaux», à la page 200
- «`CompressCommand` — Spécifie la commande et les paramètres de compression», à la page 200
- «`LogArchive` — Définit le comportement de la fonction d’archivage du journal», à la page 234
- «`Midnight` — Identifie le plug-in API permettant d’archiver les fichiers journaux», à la page 243
- «`PurgeAge` — Spécifie la limite d’âge pour un journal», à la page 268
- «`PurgeSize` — Spécifie la taille limite d’un fichier journal d’archivage», à la page 269

CompressionFilterAddContentType — Indique le type de contenu de la réponse HTTP à compresser

Cette directive permet de spécifier le type de contenu de la réponse HTTP à compresser.

Le compression HTTP permet de réduire la charge du réseau et augmente les performances du serveur proxy. En cas d’activation de la fonction de filtre de compression, si le navigateur accepte la compression HTTP et si la réponse HTTP n’est pas actuellement compressée, Caching Proxy compresses la réponse HTTP et renvoie le contenu compressé au navigateur.

Exemples

Vous pouvez activer la fonction de filtre de compression en ajoutant les deux directives suivantes au fichier `ibmproxy.conf` :

• Pour les systèmes HP-UX :

```
CompressionFilterEnable /opt/ibm/edge/cp/lib/mod_z.sl  
CompressionFilterAddContentType type-1[,type-n]
```

• Pour les autres systèmes UNIX et pour les systèmes Linux :

```
CompressionFilterEnable /opt/ibm/edge/cp/lib/mod_z.so  
CompressionFilterAddContentType type-1[,type-n]
```

• Pour les systèmes Windows :

```
CompressionFilterEnable C:\Progra~1\IBM\edge\cp\Bin\mod_z.dll  
CompressionFilterAddContentType type-1[,type-n]
```

La bibliothèque `mod_z` référencée dans la directive `CompressionFilterEnable` est la version dynamique de `zlib1.1.4`.

La variable `type-n` représente n’importe quelle valeur de l’en-tête `Content-Type` (par exemple, `text/html` ou `image/bmp`).

Remarque : Le contenu de certains types de réponses HTTP, par exemple des images JPEG ou des flux vidéo, est déjà hautement compressé par les applications : ne le compressez donc pas avec cette fonction.

Valeur par défaut

Aucun

CompressionFilterEnable — Active le filtre de compression pour qu'il compresse les réponses HTTP

Cette directive permet d'activer le filtre de compression de façon qu'il compresse les réponses HTTP à partir du serveur dorsal ou à partir de la mémoire cache du serveur proxy.

Pour des exemples d'utilisation de cette directive, voir «CompressionFilterAddContentType — Indique le type de contenu de la réponse HTTP à compresser», à la page 202.

Valeur par défaut

Aucun

ConfigFile — Spécifie le nom d'un fichier de configuration supplémentaire

Cette directive permet d'indiquer le nom et l'emplacement d'un fichier de configuration supplémentaire. Les directives se trouvant dans le fichier de configuration spécifié sont traitées après le fichier de configuration en cours.

Remarque : Assurez-vous que dans le fichier de configuration supplémentaire, le droit `Read` est défini pour l'utilisateur `nobody` afin de permettre à l'agent de la mémoire cache de lire ce fichier.

Exemples

- **Linux et UNIX :** `ConfigFile /etc/rca.conf`
- **Windows :** `ConfigFile c:\WINNT\rca.conf`

Valeur par défaut

Aucun

ConnThreads — Définition du nombre d'unités d'exécution de connexions à utiliser pour la gestion des connexions

Utilisez cette directive pour définir le nombre d'unités d'exécution de connexions à utiliser pour la gestion des connexions

Format

`ConnThreads` *numéro*

Valeur par défaut

`ConnThreads` 5

Directives connexes

- «`MaxActiveThreads` — Spécifie le nombre maximal d'unités d'exécution actives», à la page 239

ContinueCaching — Indique quelle proportion du fichier est requise pour la mise en mémoire cache

Cette directive permet d'indiquer la proportion du fichier demandé devant être transférée pour que Caching Proxy puisse créer le fichier de mémoire cache même si la connexion client est terminée. Les valeurs admises pour cette variable sont comprises entre 0 et 100.

Par exemple, si ContinueCaching 75 est utilisé, Caching Proxy continue le transfert du fichier à partir du serveur de contenu et génère le fichier de mémoire cache si 75 % ou plus du fichier a déjà été transféré avant que Caching Proxy ne détecte que la connexion client est terminée.

Format

ContinueCaching *pourcentage*

Valeur par défaut

ContinueCaching 75

DefinePicsRule — Fournit une règle de filtrage de contenu

Cette directive permet de fournir au proxy les informations nécessaires au filtrage des URL en fonction du contenu, notamment les informations de service de classification. Cette directive peut être spécifiée plusieurs fois.

Format

DefinePicsRule "*nom_filtre*" {

Valeur par défaut

DefinePicsRule "Exemple RSAC" {

DefProt — Spécifie la configuration de protection par défaut pour les demandes correspondant à un modèle

Cette directive permet d'associer une configuration de protection par défaut à des demandes correspondant à un modèle.

Remarque : Pour que la protection fonctionne correctement, les directives DefProt et Protect doivent être placées avant les directives Pass ou Exec dans le fichier de configuration.

Format

DefProt *modèle_demande* *nom_configuration*
[FOR *adresse_serveur_IP* | *nom_hôte*]

modèle_demande

Spécifie le modèle de demande à associer à une configuration de protection par défaut. Le serveur compare les demandes client entrantes au modèle et associe une configuration de protection s'il trouve une correspondance.

La protection n'est pas activée pour les demandes correspondant au modèle sauf si la demande correspond également au modèle d'une directive Protect suivante. Pour plus d'informations sur l'utilisation de la directive Protect avec Defprot, voir «Protect — Active une configuration de protection pour les demandes correspondant à un modèle», à la page 255.

configuration

Configuration de protection nommée définie dans le fichier de configuration à associer aux demandes correspondant à *modèle_demande*. La configuration de

protection est définie par les sous-directives de protection. Ce paramètre peut prendre une des trois formes suivantes :

- Un chemin complet et un nom de fichier identifiant un fichier séparé contenant les sous-directives de protection.
- Un nom de libellé de configuration de protection correspondant à un nom défini précédemment dans une directive Protection. La directive Protection contient les sous-directives de protection.
- Les sous-directives de protection en cours. Les sous-directives doivent être comprises dans des accolades ({}). L'accolade de gauche doit être le dernier caractère sur la même ligne que la directive DefProt. Chaque sous-directive suit sur sa propre ligne. L'accolade de droite doit être sur sa propre ligne suivant la dernière ligne de sous-directive. Vous ne pouvez pas placer de lignes de commentaire entre les accolades. Pour obtenir des descriptions des sous-directives de protection, voir :
 - «AuthType — Spécifie le type d'authentification», à la page 261
 - «DeleteMask — Spécifie les noms utilisateur, les groupes et les adresses admises pour la suppression des fichiers», à la page 261
 - «GetMask — Spécifie les noms d'utilisateur, les groupes et les adresses admis pour l'extraction des fichiers», à la page 261
 - «GroupFile — Spécifie l'emplacement du fichier de groupes associé», à la page 261
 - «Mask — Spécifie les noms d'utilisateur, les groupes et les adresses admises pour effectuer des demandes HTTP», à la page 262
 - «PasswdFile — Spécifie l'emplacement du fichier de mots de passe associé», à la page 262
 - «PostMask — Spécifie les noms utilisateur, les groupes et les adresses admis pour la transmission de fichiers», à la page 262
 - «PutMask — Spécifie les noms d'utilisateur, les groupes et les adresse admis pour placer des fichiers», à la page 263
 - «ServerID — Spécifie un nom à associer au fichier de mots de passe», à la page 263

[FOR adresse_serveur_IP | nom_hôte]

Si vous utilisez plusieurs adresses IP ou hôtes virtuels, utilisez ce paramètre pour spécifier une adresse IP ou un nom d'hôte. Le serveur utilise la directive uniquement pour les demandes arrivant sur le serveur à cette adresse IP ou pour cet hôte. Pour une adresse IP, il s'agit de l'adresse de la connexion réseau du serveur et non de l'adresse du client à l'origine de la demande.

Vous pouvez spécifier une adresse IP (par exemple, FOR 240.146.167.72) ou un nom d'hôte (par exemple, FOR hostA.bcd.com).

Ce paramètre est facultatif. Sans ce paramètre, le serveur utilise la directive pour toutes les demandes quelle que soit l'adresse IP d'où elles proviennent ou le nom d'hôte de l'URL.

Remarques :

1. Pour utiliser ce paramètre, le paramètre *configuration* doit être sous la forme d'un chemin et d'un nom de fichier ou d'un libellé de configuration de protection. Vous ne pouvez pas utiliser ce paramètre avec le paramètre *configuration* spécifié sous la forme de sous-directives de protection réelles placées entre accolades.

2. Pour utiliser ce paramètre, vous devez placer FOR ou une autre chaîne de caractères (sans caractères d'espace) entre le paramètre *configuration* et *adresse-IP* ou *nomhôte*.

Il n'est pas possible d'indiquer de caractère générique pour une adresse IP de serveur.

Remarque : La directive doit être entrée sur une seule ligne.

Exemples

- L'exemple ci-dessus présente un fichier séparé contenant les sous-directives de protection.

```
DefProt /secret/* /server/protect/setup1.acc
```
- L'exemple ci-dessus utilise un nom de libellé pour désigner les sous-directives de protection. Le nom de libellé doit correspondre à un nom de libellé au niveau d'une directive Protection. La directive Protection doit être placée avant la directive DefProt.

```
DefProt /secret/* SECRET-PROT
```

- L'exemple ci-après inclut les sous-directives de protection dans la directive DefProt.

```
DefProt {
  AuthType Basic
  ServerID restricted
  PasswdFile /docs/etc/WWW/restrict.password
  GroupFile /docs/etc/WWW/restrict.group
  GetMask authors
  PutMask authors
}
```

- Les exemples suivants utilisent le paramètre d'adresse IP facultatif. Si votre serveur reçoit des demandes commençant par /secret/, il associe une configuration de protection par défaut à la demande en fonction de l'adresse IP de la connexion réseau d'où elle provient. Pour les demandes provenant de 0.67.106.79, le serveur associe la demande à la protection par défaut définie au niveau d'une directive Protection avec un libellé CustomerA-PROT. Pour les demandes provenant de 0.83.100.45, le serveur associe la demande à la protection par défaut définie au niveau d'une directive Protection avec un libellé CustomerB-PROT.

```
DefProt /secret/* CustomerA-PROT 0.67.106.79
DefProt /secret/* CustomerB-PROT 0.83.100.45
```

- Les exemples ci-après utilisent le paramètre de nom d'hôte facultatif. Si votre serveur reçoit des demandes commençant par /secret/, il associe une configuration de protection par défaut à la demande en fonction du nom d'hôte de l'URL. Pour les demandes destinées à l'hôte A, le serveur associe la demande à la protection par défaut définie au niveau d'une directive Protection avec un libellé CustomerA-PROT. Pour les demandes destinées à l'hôte B, le serveur associe la demande à la protection par défaut définie au niveau d'une directive Protection avec un libellé CustomerB-PROT.

```
DefProt /secret/* CustomerA-PROT hôteA.bcd.com
DefProt /secret/* CustomerB-PROT hôteB.bcd.com
```

Valeur par défaut

Aucun

DelayPeriod — Définit une pause entre les demandes

Cette directive permet d'indiquer si l'agent de la mémoire cache doit attendre entre l'envoi des demandes aux serveurs de destination. La définition d'un délai entre les demandes réduit la charge sur la machine proxy et le lien réseau, ainsi que sur les serveurs de destination. L'absence de délai permet à l'agent de la mémoire cache d'être exécuté à sa vitesse maximale. Dans le cas de connexions Internet lentes, il est conseillé de ne pas définir de délai afin d'exploiter au maximum les possibilités de votre réseau.

Remarque : Si votre connexion à Internet est supérieure à 128 kbps, affectez la valeur `On` à `DelayPeriod` afin d'éviter l'arrivée d'un trop grand nombre de demandes simultanées sur des sites en cours de régénération.

Format

`DelayPeriod {on | off}`

Valeur par défaut

`DelayPeriod On`

DelveAcrossHosts — Active la mise en mémoire cache dans les domaines

Cette directive permet d'identifier si l'agent de la mémoire cache suivra les liens hypertexte entre les hôtes. Si une URL mise en mémoire cache contient des liens vers d'autres serveurs, le serveur peut ignorer le lien ou le suivre. Si la directive `DelveInto` a la valeur `jamais`, cette directive n'est pas appliquée.

Format

`DelveAcrossHosts {on | off}`

Valeur par défaut

`DelveAcrossHosts Off`

DelveDepth — Indique jusqu'à quel niveau suivre les liens lors de la mise en mémoire cache

Cette directive permet d'identifier le nombre de niveaux de liens à suivre lors de la recherche de pages devant être chargées dans la mémoire cache. Si la directive `DelveInto` a la valeur `jamais`, cette directive n'est pas appliquée.

Format

`DelveDepth`
nombre_de_niveaux

Valeur par défaut

`DelveDepth 2`

DelveInto — Indique si l'agent de la mémoire cache doit suivre les liens

Cette directive permet d'indiquer si l'agent de la mémoire cache doit charger les pages liées à des URL en mémoire cache.

Format

`DelveInto {toujours | jamais | admin | topn}`

toujours

L'agent de la mémoire cache suit les liens de toutes les URL précédemment mises en mémoire cache

jamais

L'agent de la mémoire cache ignore tous les liens des URL.

admin

L'agent de la mémoire cache suit uniquement les liens des URL spécifiées dans les directives LoadURL

topn

L'agent de la mémoire cache suit uniquement les liens des fichiers les plus fréquemment utilisés dans la mémoire cache.

Valeur par défaut

DelveInto always

DirBackgroundImage — Définit une image d'arrière-plan pour les listes de répertoire

Cette directive permet d'appliquer une image d'arrière-plan aux listes de répertoire générées par le serveur proxy. Les listes de répertoire sont générées lorsque le serveur proxy parcourt les sites FTP.

Définissez un chemin d'accès absolu pour l'image d'arrière-plan. Si l'image se trouve sur un autre serveur, vous devez indiquer une URL complète pour l'image d'arrière-plan. Si aucune image d'arrière-plan n'est utilisée, un arrière-plan blanc s'affiche.

Format

DirBackgroundImage
/chemin/file

Exemples

DirBackgroundImage /images/corplogo.png
DirBackgroundimage http://www.somehost.com/graphics/embossed.gif

Valeur par défaut

Aucun

DirShowBytes — Affiche le nombre d'octets des petits fichiers dans les listes de répertoires

Cette directive permet de spécifier si les listes de répertoire doivent inclure le montant exact d'octets des fichiers dont la taille est inférieure à 1 Ko. Si la valeur Off est indiquée, la valeur 1 Ko est attribuée à tous les fichiers dont la taille est inférieure ou égale à 1 Ko.

Format

DirShowBytes {on | off}

Valeur par défaut

DirShowBytes Off

DirShowCase — Différencie les majuscules et les minuscules lors du tri des fichiers des listes de répertoire

Cette directive permet de spécifier si la distinction doit être faite entre les majuscules et les minuscules lors du tri des noms de fichiers des listes de répertoire.

Si vous indiquez `On`, les majuscules sont placées avant les minuscules.

Format

`DirShowCase {on | off}`

Valeur par défaut

`DirShowCase On`

DirShowDate — Affiche la date de dernière modification dans la liste de répertoire

Cette directive permet de spécifier si les listes de répertoire doivent inclure la date de la dernière modification de chaque fichier.

Format

`DirShowDate {on | off}`

Valeur par défaut

`DirShowDate On`

DirShowDescription — Affiche la description des fichiers de la liste des répertoires

Cette directive permet de spécifier si les listes de répertoire doivent inclure les descriptions des fichiers HTML. Les descriptions sont extraites à partir des balises HTML `<title>` des fichiers.

Les descriptions des listes de répertoire FTP affichent le type MIME si ce dernier peut être déterminé.

Format

`DirShowDescription {on | off}`

Valeur par défaut

`DirShowDescription On`

DirShowHidden — Affiche les fichiers cachés dans les listes de répertoire

Cette directive permet de spécifier si les listes de répertoire doivent inclure les fichiers cachés se trouvant dans le répertoire. Pour le serveur, chaque fichier dont le nom commence par un point (.) est un fichier caché.

Format

`DirShowHidden {on | off}`

Valeur par défaut

`DirShowHidden On`

DirShowIcons — Affiche les icônes dans les listes de répertoire

Cette directive permet de spécifier si le serveur doit inclure des icônes dans les listes de répertoire. Les icônes peuvent être utilisées pour fournir une représentation graphique du type de contenu des fichiers se trouvant dans la liste. Les icônes sont définies par les directives AddBlankIcon, AddDirIcon, AddIcon, AddParentIcon et AddUnknownIcon.

Format

DirShowIcons {on | off}

Valeur par défaut

DirShowIcons On

DirShowMaxDescrLength — Indique la longueur maximum des descriptions dans les listes de répertoire

Cette directive permet de spécifier le nombre maximal de caractères à afficher dans la zone de description de la liste de répertoire.

Format

DirShowMaxDescrLength
nombre_de_caractères

Valeur par défaut

DirShowMaxDescrLength 25

DirShowMaxLength — Définit la longueur maximale des noms de fichiers dans les listes de répertoire

Cette directive permet de définir le nombre maximal de caractères à utiliser pour les noms de fichiers dans les listes de répertoire.

Format

DirShowMaxDescrLength
nombre_de_caractères

Valeur par défaut

DirShowMaxLength 25

DirShowMinLength — Définit la longueur minimale des noms de fichiers dans les listes de répertoire

Cette directive permet de spécifier le nombre minimal de caractères devant toujours être réservés pour les noms de fichiers des listes de répertoire. Les noms de fichiers du répertoire peuvent dépasser ce nombre. Cependant, la longueur des noms de fichiers ne peut pas dépasser le nombre défini au niveau de la directive DirShowMaxLength.

Format

DirShowMinLength
nombre de caractères

Valeur par défaut

DirShowMinLength 15

DirShowSize — Affiche la taille des fichiers dans la liste de répertoire

Cette directive permet de spécifier si les listes de répertoire doivent mentionner la taille de chaque fichier.

Format

DirShowSize {on | off}

Valeur par défaut

DirShowSize On

Disable — Désactive les méthodes HTTP

Cette directive permet de spécifier les méthodes HTTP que votre serveur n'accepte pas. Pour chaque méthode que le serveur doit rejeter, entrez une directive Disable distincte.

Dans le fichier de configuration par défaut, les méthodes GET, HEAD, OPTIONS, POST et TRACE sont activées et toutes les autres méthodes HTTP prises en charge sont désactivées. Pour désactiver une méthode activée, supprimez-la de la directive Enable et ajoutez-la à la directive Disable.

Format

Disable *méthode*

Remarque : Les formulaires de configuration et d'administration utilisent la méthode POST pour apporter des mises à jour à la configuration du serveur. Si vous désactivez la méthode POST, vous ne serez plus en mesure d'utiliser les formulaires de configuration et d'administration.

Valeurs par défaut

Disable PUT
Disable DELETE
Disable CONNECT

DisInheritEnv — Spécifie les variables d'environnement ne devant pas être héritées par les programmes CGI

Cette directive permet de spécifier les variables d'environnement ne devant pas être héritées par les programmes CGI (hormis les variables d'environnement spécifiques du traitement CGI).

Par défaut, toutes les variables d'environnement sont héritées par des programmes CGI. Utilisez cette directive pour exclure certaines variables d'environnement de l'héritage.

Format

DisInheritEnv *variable_environnement*

Exemples

DisInheritEnv PATH
DisInheritEnv LANG

Dans cet exemple, toutes les variables d'environnement sauf PATH et LANG sont héritées par les programmes CGI.

Valeur par défaut

Aucun

DNS-Lookup — Indique si le serveur recherche les noms d'hôte client

Cette directive permet d'indiquer si le serveur doit rechercher les noms d'hôte des clients demandeurs.

Format

DNS-Lookup {on | off}

La valeur utilisée a des incidences sur le comportement du serveur.

- Performances du serveur. En utilisant la valeur par défaut Off, les performances et le temps de réponse du serveur sont améliorés car le serveur n'utilise pas de ressources pour effectuer la recherche du nom d'hôte.
- Informations enregistrées par le serveur dans les fichiers journaux à propos des clients.
 - Off— Clients identifiés par l'adresse IP.
 - On— Clients identifiés par le nom d'hôte.
- Utilisation des noms d'hôte au niveau des modèles d'adresse dans les configurations de protection, les fichiers de groupe de serveurs et les fichiers ACL.
 - Off— Vous ne pouvez pas utiliser les noms d'hôte au niveau des modèles d'adresse, vous devez utiliser les adresses IP.
 - On— Vous pouvez utiliser les noms d'hôte au niveau des modèles d'adresse, vous ne pouvez pas utiliser les adresses IP.

Remarque : Pour utiliser des noms de domaine dans les règles de protection, vous devez attribuer la valeur On à la directive DNS-Lookup.

Valeur par défaut

DNS-Lookup Off

Enable — Active les méthodes HTTP

Cette directive permet de spécifier les méthodes HTTP que votre serveur accepte.

Vous pouvez activer autant de méthodes HTTP que nécessaire. Pour chaque méthode devant être acceptée par le serveur, entrez une directive Enable distincte.

Format

Enable *méthode*

S'il n'existe aucune directive Service pour une URL spécifique, vous pouvez utiliser la directive Enable pour effectuer une programmation personnalisée pour les méthodes HTTP. Le programme spécifié au niveau de cette directive remplace le traitement standard de cette méthode.

Enable *méthode*
/chemin/fichierDLL:nom_fonction

Pour des informations sur le format et les options disponibles pour la méthode Enable CONNECT, voir «Configuration de l'établissement des tunnels SSL», à la page 120.

Valeurs par défaut

Enable GET
Enable HEAD
Enable POST
Enable TRACE
Enable OPTIONS

EnableTcpNodelay — Activation de l'option de socket TCP NODELAY

Utilisez cette directive pour activer l'option de socket TCP NODELAY.

La directive EnableTcpNodelay améliore les performances lorsque des petits paquets IP, par exemple, l'établissement d'une liaison SSL ou une courte réponse HTTP, sont transmis entre le système Caching Proxy et le client. Par défaut, l'option TCP NODELAY est activée pour toutes les sockets.

Format

EnableTcpNodelay {All | HTTP | HTTPS | None}

Valeur par défaut

EnableTcpNodelay All

Error — Personnalise l'étape d'erreur

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur en cas d'erreur. Ce code s'exécute en cas d'erreur afin de fournir des routines d'erreur personnalisées.

Format

Error

modèle_demande /chemin/fichier:nom_fonction

modèle_demande

Spécifie un modèle pour les demandes qui déterminent ultérieurement si la fonction d'application est appelée. La spécification peut inclure le protocole, le domaine et l'hôte. Elle peut être précédée d'une barre oblique (/) et peut utiliser un astérisque (*) en tant que caractère générique. Par exemple, /front_page.html , http://www.ics.raleigh.ibm.com, /pub*, /* et * sont tous valides.

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme.

Exemple

Error /index.html /ics/api/bin/icsext05.so:error_rtns

Valeur par défaut

Aucun

ErrorLog — Spécifie le fichier dans lequel sont consignées les erreurs du serveur

Cette directive permet de spécifier le chemin et le nom du fichier dans lequel le serveur doit consigner les erreurs internes.

Remarque : Si vous modifiez les paramètres par défaut du serveur pour l’ID utilisateur, l’ID groupe ou les chemins d’accès au répertoire journal, créez des répertoires et mettez à jour leurs droits d’accès et leurs propriétés. Pour que le serveur puisse enregistrer des informations dans un répertoire de consignation défini par un utilisateur, attribuez à ce répertoire des droits d’accès 755 et définissez l’ID utilisateur du serveur défini par l’utilisateur comme propriétaire. Par exemple, si l’ID utilisateur du serveur est pdupont et que le répertoire de consignation par défaut est server_root/account, le répertoire server_root/account doit posséder les droits 755 et appartenir à pdupont.

S’il est en cours d’exécution, le serveur démarre un nouveau fichier journal chaque jour à minuit. Sinon, le serveur démarre un nouveau fichier journal dès que vous le lancez. Lors de la création du fichier, le serveur utilise le nom du fichier spécifié et ajoute un suffixe de date. Le suffixe de date apparaît au format *Mmmjjaaaa*, où *Mmm* correspond aux trois premières lettres du mois, *jj* correspond au jour du mois et *aaaa* à l’année.

Format

ErrorLog
/chemin/répertoire-journaux/nom_fichier

Valeurs par défaut

- **Systèmes Linux et UNIX :** ErrorLog */opt/ibm/edge/cp/racine_serveur/logs/error*
- **Systèmes Windows :** ErrorLog *unité:\Program Files\IBM\edge\cp\logs\error*

ErrorPage — Spécifie un message personnalisé pour une condition d’erreur particulière

Cette directive permet de spécifier le nom d’un fichier à envoyer au client à l’origine de la demande lorsque le serveur rencontre une erreur particulière. Les directives ErrorPage sont fournies dans le fichier *ibmproxy.conf* qui associe les mots clés d’erreur aux fichiers de messages d’erreur.

Pour personnaliser les messages d’erreur, vous pouvez modifier les directives ErrorPage afin d’associer les mots clés d’erreur à différents fichiers. Vous pouvez également modifier les fichiers de messages d’erreur. Par exemple, vous pouvez modifier un message afin d’inclure des informations supplémentaires sur la cause de l’incident et suggérer des solutions possibles. Pour des réseaux internes, vous pouvez indiquer un contact que les utilisateurs peuvent appeler.

Les directives ErrorPage peuvent être placées n’importe où dans le fichier de configuration. Lorsque l’erreur se produit, le fichier est traité en fonction des règles de mappage définies dans votre fichier de configuration. C’est pourquoi le fichier à envoyer doit être dans un emplacement accessible via les règles de mappage, comme défini par les directives Fail, Map, NameTrans, Pass, Redirect et Service. Vous devez au moins définir une directive Pass qui permette au serveur de transmettre le fichier de messages d’erreur.

Format

ErrorPage *keyword*
/chemin/nomfichier.html

mot clé

Spécifie l'un des mots clés associé à une erreur. Les mots clés sont répertoriés dans les directives ErrorPage dans le fichier ibmproxy.conf. Vous ne pouvez pas changer les mots clés.

/chemin/nomfichier.html

Indique le nom Web complet du fichier d'erreurs, tel qu'il est affiché par un client sur le Web. Les fichiers de messages d'erreur par défaut se trouvent dans /HTML/errorpages/.

Exemple

```
ErrorPage scriptstart /HTML/errorpages/scriptstart.htmls
```

Dans cet exemple, lorsque la condition scriptstart se produit, le serveur envoie le fichier scriptstart.htmls se trouvant dans /HTML/errorpages/ au client.

Le texte HTML suivant est un exemple de ce que peut contenir le fichier :

```
<HTML>
<HEAD>
<TITLE>Message de la condition SCRIPTSTART</TITLE>
</HEAD>
<BODY>
Impossible de démarrer le programme CGI.
<P>
<A HREF="mailto:admin@websvr.com">Notifiez l'administrateur</A>
de cet incident.
</BODY>
</HTML>
```

Si la directive qui correspond au chemin dans le fichier de configuration du serveur est PASS /* /wwwhome/*, alors le chemin complet du fichier de messages sera /wwwhome/HTML/errorpages/scriptstart.htmls.

Personnalisation des messages d'erreur envoyés par le serveur

Chaque condition d'erreur est identifiée par un mot clé. Pour savoir quels sont les messages d'erreur à personnaliser, consultez tout d'abord les fichiers de messages d'erreur se trouvant dans /HTML/errorpages fournis avec Caching Proxy. La page d'erreur inclut le numéro de l'erreur, le message par défaut, une explication de la cause et une action de récupération appropriée.

Pour modifier un message d'erreur, procédez de l'une des manières suivantes :

- Modifiez le fichier HTML ou HTMLS existant (créez une copie de sauvegarde tout d'abord) ou créez un nouveau fichier HTML ou HTMLS avec le texte désiré. Vous pouvez utiliser un éditeur HTML ou ASCII. Un fichier HTMLS doit être utilisé si vous voulez utiliser des instructions côté serveur.
- Si vous avez créé un fichier de message d'erreur portant un nom différent (ou dans un chemin différent), modifiez la directive ErrorPage pour ce mot clé afin qu'elle désigne ce fichier.

Conditions d'erreur, causes et messages par défaut

Tous les mots clés d'erreur et les fichiers de messages d'erreur par défaut sont répertoriés dans le fichier ibmproxy.conf, dans la section de la directive ErrorPage. Les fichiers de messages d'erreur incluent le numéro, le mot clé, le message par défaut, l'explication et la réponse utilisateur (action) du message d'erreur.

Valeurs par défaut

Le fichier ibmproxy.conf contient de nombreuses valeurs par défaut.

Si vous ne modifiez aucune directive `ErrorPage` pour une condition d'erreur, la page d'erreur par défaut du serveur de cette condition sera envoyée.

EventLog — Spécifie le chemin du fichier journal des événements

Cette directive permet de spécifier le chemin et le nom du fichier journal des événements. Le journal des événements enregistre des messages d'information à propos de la mémoire cache elle-même.

Remarque : Si vous modifiez les paramètres par défaut du serveur pour l'ID utilisateur, l'ID groupe ou les chemins d'accès au répertoire journal, créez des répertoires et mettez à jour leurs droits d'accès et leurs propriétés. Pour que le serveur puisse enregistrer des informations dans un répertoire de consignation défini par un utilisateur, attribuez à ce répertoire des droits d'accès 755 et définissez l'ID utilisateur du serveur défini par l'utilisateur comme propriétaire. Par exemple, si l'ID utilisateur du serveur est `pdupont` et que le répertoire de consignation par défaut est `server_root/account`, le répertoire `server_root/account` doit posséder les droits 755 et appartenir à `pdupont`.

S'il est en cours d'exécution, le serveur démarre un nouveau fichier journal chaque jour à minuit. Sinon, le serveur démarre un nouveau fichier journal dès que vous le lancez. Lors de la création du fichier, le serveur utilise le nom du fichier spécifié et ajoute un suffixe de date. Le suffixe de date apparaît au format *Mmmjjaaaa*, où *Mmm* correspond aux trois premières lettres du mois, *jj* correspond au jour du mois et *aaaa* à l'année.

Format

```
EventLog  
/chemin/répertoire_journaux/nom_fichier
```

Valeurs par défaut

- **Systèmes Linux et UNIX :** `EventLog /opt/ibm/edge/cp/racine_serveur/logs/event`
- **Systèmes Windows :** `EventLog unité:\Program Files\IBM\edge\cp\logs\event`

Exec — Exécute un programme CGI pour les demandes ayant abouti

Cette directive permet de spécifier un modèle pour les demandes à accepter et auxquelles vous répondez en utilisant un programme CGI. Une fois qu'une demande correspond à un modèle d'une directive `Exec`, la demande n'est pas comparée aux modèles de demandes des directives suivantes.

Format

```
Exec modèle_demande chemin_programme  
[adresse_serveur_IP | nom_hôte]
```

modèle_demande

Spécifie un modèle pour les demandes devant être acceptées par le serveur et auxquelles vous répondez en exécutant un programme CGI.

Vous devez utiliser un astérisque (*) en tant que caractère générique dans *modèle_demande* et *chemin_programme*. La partie de la demande qui correspond au caractère générique *modèle_demande* doit commencer par le nom du fichier qui contient le programme CGI.

La demande peut également contenir des données supplémentaires qui sont transmises au programme CGI dans la variable d'environnement `PATH_INFO`. Les données supplémentaires suivent la première barre oblique se trouvant après le nom de fichier du programme CGI dans la demande. Les données sont transmises en fonction des spécifications CGI.

chemin_programme

Spécifie le chemin du fichier contenant le programme CGI devant être exécuté par le serveur pour la demande. *chemin-programme* doit également contenir un caractère générique. Le caractère générique est remplacé par le nom du fichier contenant le programme CGI.

La directive `Exec` est réursive et s'applique à tous les sous-répertoires. Vous n'avez pas besoin d'une directive `Exec` séparée pour chaque répertoire sous `cgi-bin` et `admin-bin`.

[*adresse_IP_serveur* | *nom_hôte*]

Si vous utilisez plusieurs adresses IP ou noms d'hôte, utilisez ce paramètre pour spécifier une adresse IP ou un nom d'hôte. Le serveur utilise la directive uniquement pour les demandes arrivant sur le serveur à cette adresse IP ou pour cet hôte. Pour une adresse IP, il s'agit de l'adresse de la connexion réseau du serveur et non de l'adresse du client à l'origine de la demande.

Vous pouvez spécifier une adresse IP (par exemple, 240.146.167.72) ou un nom d'hôte (par exemple, hostA.bcd.com).

Ce paramètre est facultatif. Sans ce paramètre, le serveur utilise la directive pour toutes les demandes quel que soit le nom d'hôte de l'URL ou l'adresse IP d'où elles proviennent.

Vous ne pouvez pas utiliser de caractères génériques pour spécifier les adresses IP.

Exemples

Dans cet exemple, si votre serveur reçoit une demande de `/idd/depts/plan/c92`, il exécute le programme CGI dans `/depts/bin/plan.exe` en transmettant `c92` au programme en tant qu'entrée.

L'exemple ci-dessus utilise le paramètre facultatif d'adresse IP. Si le serveur reçoit des demandes qui commencent par `/cgi-bin/`, il sert les demandes d'un répertoire différent en fonction de l'adresse IP de la connexion réseau d'où provient la demande. Pour les demandes provenant de 130.146.167.72, le serveur utilise le répertoire `/CGI-BIN/customerA`. Pour les demandes provenant d'une autre connexion ayant une adresse IP 0.83.100.45, le serveur utilise le répertoire `/CGI-BIN/customerB`.

```
Exec    /cgi-bin/*    /CGI-BIN/customerA/*    130.129.167.72
Exec    /cgi-bin/*    /CGI-BIN/customerB/*    0.83.100.45
```

L'exemple ci-dessus utilise le paramètre facultatif de nom d'hôte. Si votre serveur reçoit des demandes commençant par `/cgi-bin/`, il sert la demande d'un répertoire différent en fonction du nom d'hôte de l'URL. Pour les demandes destinées à hôteA.bcd.com, le serveur utilise le répertoire `/CGI-BIN/customerA`. Pour les demandes destinées à hôteB.bcd.com, le serveur utilise le répertoire `/CGI-BIN/customerB`.

```
Exec    /cgi-bin/*    /CGI-BIN/customerA/*    hôteA.bcd.com
Exec    /cgi-bin/*    /CGI-BIN/customerB/*    hôteB.bcd.com
```

Valeurs par défaut

- **Systèmes Linux et UNIX**

```
Exec /cgi-bin/*      /opt/ibm/edge/cp/server_root/cgi-bin/*
Exec /admin-bin/*    /opt/ibm/edge/cp/server_root/admin-bin/*
```

- **Systèmes Windows**

```
Exec server_root/cgi-bin/*
Exec server_root/admin-bin/*
Exec server_root/DOCS/admin-bin/*
```

ExportCacheImageTo — Exportation de la mémoire cache sur le disque

Cette directive permet d'exporter le contenu de la mémoire cache vers un fichier de vidage. Cette opération est utile lorsque la mémoire cache est perdue lors du redémarrage ou lors du déploiement de la même mémoire cache sur plusieurs proxys.

Format

ExportCacheImageTo *nom_fichier_exportation*

Valeur par défaut

Aucun

ExternalCacheManager — Configure Caching Proxy pour la mise en mémoire cache dynamique à partir de IBM WebSphere Application Server

S'applique aux configurations avec proxy inversé uniquement.

Utilisez cette directive pour configurer Caching Proxy afin qu'il reconnaisse un serveur IBM WebSphere Application Server (configuré avec un module de carte Caching Proxy) à partir duquel il pourra placer en mémoire cache des ressources dynamiques. Caching Proxy sauvegarde les copies des résultats JSP qui sont aussi stockés dans la mémoire cache dynamique du serveur d'applications. Caching Proxy met en mémoire cache uniquement le contenu d'un serveur IBM WebSphere Application Server dont l'ID groupe correspond à une entrée ExternalCacheManager.

Sachez que pour activer cette fonction, il est également nécessaire d'ajouter une directive Service au fichier de configuration de Caching Proxy. Vous devez aussi effectuer d'autres opérations de configuration sur le serveur d'applications. Pour plus d'informations, voir Chapitre 22, «Stockage en mémoire cache d'un contenu généré dynamiquement», à la page 103.

Format

ExternalCacheManager
ID_gestionnaire_cache_externe *délai_expiration_maximal*

ID_gestionnaire_cache_externe

ID attribué au serveur IBM WebSphere Application Server qui sert le proxy. Cet ID doit correspondre à celui qui est défini dans l'attribut externalCacheGroup: group id dans le fichier dynacache.xml figurant sur le serveur d'applications.

Maximum_Expiry_Time

Délai d'expiration par défaut défini pour les ressources placées en mémoire cache au nom du gestionnaire de cache externe. Si le gestionnaire de cache externe n'invalide pas une ressource placée en mémoire cache dans le délai spécifié, la ressource expire à l'heure indiquée. L'heure peut être indiquée en minutes ou en secondes.

Exemple

L'entrée suivante définit un gestionnaire de cache externe (un serveur IBM WebSphere Application Server), situé dans le domaine `www.xyz.com` et dont les ressources expirent dans 20 secondes au plus tard.

```
ExternalCacheManager  IBM-CP-XYZ-1  20 secondes
```

Valeur par défaut

Aucun

Fail — Rejette les demandes ayant abouti

Cette directive permet de spécifier un modèle pour les demandes à ne pas traiter. Une fois qu'une demande correspond à un modèle d'une directive Fail, la demande n'est pas comparée aux modèles de demande des directives suivantes.

Format

```
Fail modèle_demande  
[adresse_IP_serveur | nom_hôte]
```

modèle_demande

Spécifie un modèle pour les demandes que le serveur doit rejeter. Si une demande correspond au modèle, le serveur envoie un message d'erreur à l'utilisateur à l'origine de la demande.

Vous pouvez utiliser un astérisque en tant que caractère générique dans le modèle. Le caractère tilde (~) placé juste après une barre oblique (/) doit être indiqué explicitement. Vous ne pouvez pas utiliser de caractère générique.

[*adresse_IP_serveur* | *nom_hôte*]

Si vous utilisez plusieurs adresses IP ou noms d'hôte, utilisez ce paramètre pour spécifier une adresse IP ou un nom d'hôte. Le serveur utilise la directive uniquement pour les demandes arrivant sur le serveur à cette adresse IP ou pour cet hôte. Pour une adresse IP, il s'agit de l'adresse de la connexion réseau du serveur et non de l'adresse du client à l'origine de la demande.

Vous pouvez spécifier une adresse IP (par exemple, 240.146.167.72) ou un nom d'hôte (par exemple, hostA.bcd.com).

Ce paramètre est facultatif. Sans ce paramètre, le serveur utilise la directive pour toutes les demandes quel que soit le nom d'hôte de l'URL ou l'adresse IP d'où elles proviennent.

Il n'est pas possible d'indiquer de caractère générique pour une adresse IP de serveur.

Exemples

Dans l'exemple ci-dessus, le serveur rejette les demandes commençant par `/usr/local/private/`.

```
Fail /usr/local/private/*
```

Les exemples suivants utilisent le paramètre d'adresse IP facultatif. Le serveur rejette toutes les demandes commençant par `/customerB/` si la demande provient d'une connexion réseau dont l'adresse IP est 240.146.167.72. Le serveur rejette toutes les demandes commençant par `/customerA/` si la demande provient d'une connexion réseau dont l'adresse IP est 0.83.100.45.

```
Fail    /customerB/*    240.146.167.72  
Fail    /customerA/*    0.83.100.45
```

Les exemples ci-après utilisent le paramètre de nom d'hôte facultatif. Le serveur rejette les demandes commençant par /customerB/ si elles sont destinées à hôteA.bcd.com. Le serveur rejette les demandes commençant par /customerA/ si elles sont destinées à hôteB.bcd.com.

```
Fail    /customerB/*    hôteA.bcd.com
Fail    /customerA/*    hôteB.bcd.com
```

Valeur par défaut

Aucun

FIPSEnable — Codes de chiffrement conformes à la norme FIPS (Enable Federal Information Processing Standard) pour SSLV3 et TLS

Cette directive permet d'activer les codes de chiffrement conformes à la norme FIPS pour le protocole SSLV3 et TLS dans les connexions SSL. Lorsqu'elle est activée, la liste des spécifications de code de chiffrement prises en charge pour SSLV3 (directive V3CipherSpecs) est ignorée. De plus, les spécifications de code de chiffrement TLS autorisées sont définies à la valeur 352F0AFF09FE et les spécifications de code de chiffrement SSLV3 sont définies à la valeur FFFE.

Format

```
FIPSEnable {on | off}
```

Valeur par défaut

```
FIPSEnable off
```

flexibleSocks — Active l'implémentation SOCKS flexible

Cette directive permet d'indiquer au proxy d'utiliser la configuration de SOCKS pour déterminer le type de connexion à établir.

Format

```
flexibleSocks {on | off}
```

Valeur par défaut

```
flexibleSocks on
```

FTPDDirInfo — Génère un message de bienvenue ou de description pour un répertoire

Cette directive permet d'activer le serveur FTP afin de générer un message de bienvenue ou de description pour un répertoire. Ce message peut être affiché en tant que partie des listes FTP. La directive FTPDirInfo permet de contrôler l'emplacement d'affichage du message.

Format

```
FTPDDirInfo {top | bottom | off}
```

haut

Affiche le message de bienvenue dans la partie supérieure de la page, avant la liste des fichiers du répertoire.

bas

Affiche le message de bienvenue dans la partie inférieure de la page, après la liste des fichiers du répertoire.

off

N'affiche pas la page de bienvenue.

Valeur par défaut

FTPDInfo top

ftp_proxy — Spécifie un autre serveur proxy pour les demandes FTP

Si votre serveur proxy fait partie d'une chaîne de proxys, cette directive permet de spécifier le nom d'un autre proxy devant être contacté par ce serveur pour des demandes FTP. Vous devez préciser une URL complète, y compris la barre oblique de fin (/). Pour plus d'informations sur l'utilisation d'un modèle ou d'un nom de domaine facultatif, voir «no_proxy — Spécifie les modèles pour la connexion directe aux domaines», à la page 246.

S'applique aux configurations avec proxy d'acheminement uniquement.

Format

proxy_ftp *URL_complète* [*modèle_ou_nom_domaine*]

Exemple

ftp_proxy http://outer.proxy.server/

Valeur par défaut

Aucun

FTPUrlPath — Indique comment interpréter les URL FTP

Cette directive permet de spécifier si les informations de chemin dans l'URL FTP doivent être interprétées comme étant relatives au répertoire de travail de l'utilisateur connecté ou comme étant relatives au répertoire principal.

Format

FTPUrlPath {relative | absolute}

Si la directive FTPUrlPath a la valeur *absolute*, le répertoire de travail FTP de l'utilisateur connecté doit être inclus dans le chemin de l'URL FTP. Si FTPUrlPath *Relative* est spécifié, le répertoire de travail FTP de l'utilisateur connecté doit être omis dans le chemin de l'URL FTP. Par exemple, pour accéder au fichier test1.html, contenu dans le répertoire de travail /export/home/user1 pour un utilisateur connecté, les chemins d'URL suivants sont requis, selon la définition de la directive FTPUrlPath :

- Si le paramètre est FTPUrlPath *absolute*, le chemin d'URL requis est ftp://ftphost/export/home/user1/test1.html.
- Si le paramètre est FTPUrlPath *relative*, le chemin d'URL requis est alors ftp://ftphost/test1.html.

Valeur par défaut

Aucun

Gc — Spécifie la récupération de place en mémoire cache

Cette directive permet de spécifier si la récupération de place en mémoire cache est utilisée. Si vous avez activé la mise en mémoire cache, le serveur utilise le processus de récupération de place pour supprimer les fichiers ne devant plus figurer en mémoire cache. Les fichiers sont supprimés en fonction de la date

d'expiration et d'autres valeurs de directive de proxy. En principe, si la mise en mémoire cache est utilisée, la récupération de place est utilisée. Dans le cas contraire, l'exploitation de la mémoire cache du proxy est peu performante.

Format

Gc {on | off}

Valeur par défaut

Gc On

GCAvigator — Personnalise le processus de récupération de place

Cette directive permet de spécifier une application personnalisée devant être utilisée par le serveur pour le processus de récupération de place.

Format

GCAvigator /chemin/fichier:nom_fonction

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme.

Exemple

GCAvigator /api/bin/customadvise.so:gadv

GcHighWater — Indique le moment du lancement de la récupération de place

Cette directive permet de spécifier le pourcentage de la capacité totale de la mémoire cache qui doit être atteint pour déclencher la récupération de place. Ce pourcentage est appelé *cote d'alerte*. La cote d'alerte est spécifiée en tant que pourcentage de la capacité totale de la mémoire cache. La récupération de place se poursuit jusqu'à ce que la cote d'alerte inférieure soit atteinte. Pour la définir, voir «GcLowWater — Spécifie le moment d'arrêt de la récupération de place». Le pourcentage de cote d'alerte peut être compris entre 50 et 95.

Format

GcHighWater *pourcentage*

Valeur par défaut

GcHighWater 90

GcLowWater — Spécifie le moment d'arrêt de la récupération de place

Cette directive permet de spécifier le pourcentage de la capacité totale de la mémoire cache qui doit être atteint pour déclencher l'arrêt de la récupération de place. Ce pourcentage est appelé *cote d'alerte inférieure*. La cote d'alerte inférieure est spécifiée en tant que pourcentage de la capacité totale de la mémoire cache. Elle doit avoir une valeur inférieure à la cote d'alerte. Pour la définir, voir «GcHighWater — Indique le moment du lancement de la récupération de place».

Format

GcLowWater *pourcentage*

Valeur par défaut

GcLowWater 60

gopher_proxy — Spécifie un autre serveur proxy pour les demandes Gopher

Si votre serveur proxy fait partie d'une chaîne de proxys, cette directive permet de spécifier le nom d'un autre proxy devant être contacté par ce serveur pour des demandes Gopher. Vous devez préciser une URL complète, y compris la barre oblique de fin (/). Pour plus d'informations sur l'utilisation d'un modèle ou d'un nom de domaine facultatif, voir «no_proxy — Spécifie les modèles pour la connexion directe aux domaines», à la page 246.

S'applique aux configurations avec proxy d'acheminement uniquement.

Format

proxy_gopher *URL_complète*[*modèle_ou_nom_domaine*]

Exemple

gopher_proxy http://outer.proxy.server/

Valeur par défaut

Aucun

GroupId — Spécifie l'ID de groupe

Cette directive permet de spécifier le nom ou le numéro du groupe dans lequel passe le serveur avant d'accéder aux fichiers.

Si vous changez cette directive, vous devez arrêter le serveur puis le redémarrer pour que le changement soit effectif. La modification n'est pas prise en compte si vous vous contentez de redémarrer le serveur. (Voir Chapitre 5, «Démarrage et arrêt de Caching Proxy», à la page 15.)

Remarque : Si vous modifiez les paramètres par défaut du serveur pour l'ID utilisateur, l'ID groupe ou les chemins d'accès au répertoire journal, créez des répertoires et mettez à jour leurs droits d'accès et leurs propriétés. Pour que le serveur puisse enregistrer des informations dans un répertoire de consignation défini par un utilisateur, attribuez à ce répertoire des droits d'accès 755 et définissez l'ID utilisateur du serveur défini par l'utilisateur comme propriétaire. Par exemple, si l'ID utilisateur du serveur est pdupont et que le répertoire de consignation par défaut est server_root/account, le répertoire server_root/account doit posséder les droits 755 et appartenir à pdupont.

Format

GroupId {*nom_groupe* |
numéro_groupe}

Valeurs par défaut

AIX : GroupId nobody

HP-UX : GroupId other

Linux :

Red Hat : GroupId nobody

SUSE : GroupId nogroup

Solaris : GroupId nobody

HeaderServerName — Indique le nom du serveur proxy retourné dans l'entête HTTP

Cette directive permet d'indiquer le nom du serveur proxy retourné dans l'entête HTTP

Format

HeaderServerName *nom*

Valeur par défaut

Aucun

Hostname — Spécifie le nom de domaine complet ou l'adresse IP du serveur

Cette directive permet de spécifier le nom de domaine ou une adresse IP renvoyé aux clients à partir des demandes de fichiers. Si vous spécifiez un nom de domaine, vous devez disposer d'un serveur de nom de domaine capable de résoudre le nom en une adresse IP. Si vous spécifiez une adresse IP, le serveur de nom de domaine n'est pas nécessaire ou accessible.

Remarque : Lors de la configuration d'un tableau, la directive Hostname doit être configuré de la même manière pour tous les membres du tableau.

Format

Hostname {*nom* | *adresse_IP*}

Valeur par défaut

Par défaut, cette directive n'est pas spécifiée dans le fichier de configuration d'origine. Si vous ne spécifiez pas cette directive dans le fichier de configuration, la valeur par défaut permet l'acceptation et l'envoi des requêtes définies sur n'importe quel serveur de noms de domaine.

http_proxy — Spécifie un autre serveur proxy pour les demandes HTTP

Si votre serveur proxy fait partie d'une chaîne de proxys, cette directive permet de spécifier le nom d'un autre proxy devant être contacté par ce serveur pour des demandes HTTP. Vous devez préciser une URL complète, y compris la barre oblique de fin (/). Pour plus d'informations sur l'utilisation d'un modèle ou d'un nom de domaine facultatif, voir «no_proxy — Spécifie les modèles pour la connexion directe aux domaines», à la page 246.

Format

proxy_http *URL_complète* [*modèle_ou_nom_domaine*]

Exemple

http://outer.proxy.server/

Valeur par défaut

Aucun

HTTPSCheckRoot — Filtre les demandes HTTPS

Cette directive permet de spécifier si Caching Proxy doit extraire la page d'accueil non sécurisée pour l'URL et tenter d'y trouver des libellés. Si le programme trouve des libellés, ils sont appliqués à la demande sécurisée. Par exemple, si vous demandez `https://www.ibm.com/`, Caching Proxy extrait `http://www.ibm.com/`, cherche des libellés et utilise les libellés trouvés pour filtrer `https://www.ibm.com/`.

Si HTTPSCheckRoot a la valeur `off`, Caching Proxy n'extrait pas la page d'accueil non sécurisée et ne cherche pas de libellés.

Format

HTTPSCheckRoot {on | off}

Valeur par défaut

HTTPSCheckRoot on

ICP_Address — Spécifie l'adresse IP des requêtes ICP

Utilisez cette directive pour indiquer une adresse IP utilisée pour envoyer et recevoir les requêtes ICP. Elle doit figurer dans les directives `<MODULEBEGIN> ICP` et `<MODULEEND>`.

Format

ICP_Address *adresse_IP*

Valeur par défaut

Par défaut, cette directive n'est pas spécifiée dans le fichier de configuration d'origine. Si vous ne spécifiez pas cette directive dans le fichier de configuration, la valeur par défaut permet l'acceptation et l'envoi des requêtes ICP sur n'importe quelle interface.

ICP_MaxThreads — Spécifie le nombre maximal d'unités d'exécution pour requêtes ICP

Utilisez cette sous-directive pour spécifier le nombre d'unités d'exécution générées pour attendre les requêtes ICP. Elle doit figurer dans les directives `<MODULEBEGIN> ICP` et `<MODULEEND>`.

Remarque : Sur Redhat Linux 6.2 et versions inférieures, ce nombre doit être bas car le système ne peut créer qu'un petit nombre d'unités d'exécution par processus. La spécification d'un grand nombre d'unités d'exécution pour l'utilisation d'ICP peut limiter le nombre d'unités d'exécution disponibles pour les demandes de service.

Format

ICP_MaxThreads *nombre_d'unités_d'exécution*

Valeur par défaut

ICP_MaxThreads 5

Occupier — Spécifie un membre de cluster ICP

Si le serveur proxy fait partie d'un cluster ICP, utilisez cette sous-directive pour spécifier les homologues ICP. Il doit figurer dans les directives `<MODULEBEGIN> ICP` et `<MODULEEND>`.

Lorsqu'un nouvel homologue est ajouté au cluster ICP, les informations relatives à l'homologue ICP doivent être ajoutées au fichier de configuration de tous les homologues existants. Utilisez une ligne par homologue. Sachez que l'hôte en cours peut également être inclus dans la liste des homologues. À l'initialisation, l'ICP ignore l'entrée de l'hôte en cours. Il est ainsi possible de disposer d'un fichier de configuration unique qui peut être copié vers d'autres machines homologues sans le modifier pour supprimer l'hôte en cours.

Format

`ICP_Peer nomhôte port_http port_icp`

nomhôte

Nom de l'homologue

port_http

port http du proxy de l'homologue

port_icp

Port serveur ICP de l'homologue

Exemple

La ligne ci-après ajoute l'hôte abc.xcompany.com, dont le port du proxy est 80 et le port ICP 3128, en tant qu'hôte.

```
ICP_Peer abc.xcompany.com 80 3128
```

Valeur par défaut

Aucun

ICP_Port — Spécifie le numéro de port des requêtes ICP

Utilisez cette sous-directive pour spécifier le numéro du port sur lequel le serveur ICP écoute les requêtes ICP. Elle doit figurer dans les directives `<MODULEBEGIN> ICP` et `<MODULEEND>`.

Format

`ICP_Port numéro_de_port`

Valeur par défaut

`ICP_Port 3128`

ICP_Timeout — Spécifie le délai d'attente maximal des requêtes ICP

Utilisez cette sous-directive pour spécifier le délai d'attente maximal de Caching Proxy avant la réponse aux requêtes ICP. Ce délai est indiqué en millisecondes. Elle doit figurer dans les directives `<MODULEBEGIN> ICP` et `<MODULEEND>`.

Format

`ICP_Timeout délai_en_millisecondes`

Valeur par défaut

`ICP_Timeout 2000`

IgnoreURL — Spécifie les URL qui ne sont pas régénérées

Cette directive permet d'identifier les URL ne devant pas être chargées par l'agent de la mémoire cache. Cette directive est utile lorsque l'agent de la mémoire cache charge des pages liées à partir des URL en mémoire cache. Vous pouvez avoir plusieurs occurrences de la directive IgnoreURL identifiant différentes URL ou

masques d'URL. La valeur de cette directive peut contenir des astérisques (*) en tant que caractères génériques pour l'application d'un masque.

Format

IgnoreURL *URL*

Exemples

IgnoreURL `http://www.yahoo.com/`

IgnoreURL `http://*.ibm.com/*`

Valeur par défaut

IgnoreURL `*/cgi-bin/*`

imbeds — Indique si le traitement côté serveur est utilisé

Cette directive permet de spécifier si vous voulez que le traitement d'instructions côté serveur soit effectué pour les fichiers servis à partir du système de fichiers ou des programmes CGI. Le traitement des instructions côté serveur est effectué sur les fichiers dont le contenu est de type `ext/x-ssi-html`. De manière facultative, vous pouvez spécifier que le traitement des instructions côté serveur doit être effectué pour les fichiers dont le type de contenu est `text/html`. Pour plus d'informations sur les types de contenu, voir «AddType — Spécifie le type de données des fichiers ayant une extension particulière», à la page 183.

Vous pouvez utiliser le traitement des instructions côté serveur pour insérer de manière dynamique des informations dans le fichier renvoyé. Ces informations peuvent être la date, la taille d'un fichier, la date de dernière modification d'un fichier, les variables d'environnement côté serveur ou CGI ou des fichiers de type texte. Le traitement des instructions côté serveur est effectué uniquement sur les fichiers émis localement. Caching Proxy n'effectue pas ce type de traitement sur les objets du serveur proxy ou en mémoire cache.

Le traitement des instructions côté serveur fait que le serveur recherche dans vos fichiers des commandes spéciales chaque fois qu'il sert les fichiers. Cette action peut avoir un effet néfaste sur les performances du serveur et peut ralentir le temps de réponse aux clients.

Format

`imbeds {on | off | files | cgi | noexec} {SSIOnly | html}`

on Le traitement des instructions côté serveur est effectué pour les fichiers provenant du système de fichiers et des programmes CGI.

off

Le traitement des instructions côté serveur n'est effectué pour aucun fichier.

fichiers

Le traitement des instructions côté serveur est effectué uniquement pour les fichiers provenant du système de fichiers.

cgi

Le traitement des instructions côté serveur est effectué uniquement pour les fichiers renvoyés par les programmes CGI.

noexec

SSIOnly

Le traitement des instructions côté serveur est effectué pour les fichiers dont le type de contenu est `text/x-ssi-html`.

html

Le traitement des instructions côté serveur est effectué pour les fichiers dont le type de document est text/html ou text/x-ssi-html.

Le serveur vérifie le type de contenu de chaque fichier extrait ainsi que la sortie de chaque programme CGI traité.

Le traitement des instructions côté serveur est normalement effectué uniquement pour les fichiers dont le contenu est de type text/x-ssi/html. Cependant, vous pouvez spécifier que les fichiers dont le contenu est de type text/html soient traités pour les instructions côté serveur.

Remarque : Le serveur traite les éléments html, .html, et .htm en tant que html. Tous les autres éléments sont traités en tant que SSIOnly.

Pour chaque suffixe, une directive AddType doit être définie avec le type de contenu correct. Si vous utilisez des suffixes autres que .htm ou .html, assurez-vous que la directive AddType est définie avec un contenu de type text/x-ssi/html.

Valeur par défaut

imbeds on SSIOnly

ImportCacheImageFrom — Importation de la mémoire cache à partir d'un fichier

Cette directive permet d'importer le contenu de la mémoire cache à partir d'un fichier de vidage. Cette opération est utile lorsque la mémoire cache est perdue lors du redémarrage ou lors du déploiement de la même mémoire cache sur plusieurs proxys.

Format

ImportCacheImageFrom *nom_fichier_importation*

Valeur par défaut

Aucun

InheritEnv — Spécifie les variables d'environnement héritées par les programmes CGI

Cette directive permet de spécifier les variables d'environnement devant être héritées par les programmes CGI (hormis les variables d'environnement spécifiques du traitement CGI).

Si vous n'incluez pas de directive InheritEnv, toutes les variables d'environnement sont héritées par les programmes CGI. Si vous incluez une directive InheritEnv, seules les variables d'environnement spécifiées dans les directives InheritEnv seront héritées en même temps que les variables d'environnement spécifiques de CGI. La directive permet d'initialiser la valeur des variables héritées.

Format

InheritEnv
variable_environnement

Exemples

InheritEnv PATH
InheritEnv LANG=ENUS

Dans cet exemple, seules les variables d'environnement PATH et LANG seront héritées par les programmes CGI et la variable d'environnement LANG sera initialisée avec la valeur ENUS.

Valeur par défaut

Aucun. Par défaut, toutes les variables d'environnement sont héritées par des programmes CGI.

InputTimeout — Spécifie le délai d'entrée

Cette directive permet de définir le temps attribué à un client pour l'envoi d'une demande après l'établissement d'une connexion au serveur. Un client se connecte tout d'abord au serveur puis envoie une demande. Si le client n'envoie aucune demande dans le laps de temps défini par cette directive, le serveur met fin à la connexion. Spécifiez la durée en combinant des heures, des minutes (ou mn) et des secondes (ou s).

Format

`InputTimeout délai`

Exemple

`InputTimeout 3 mn 30 s`

Valeur par défaut

`InputTimeout 2 minutes`

JunctionReplaceUrlPrefix — Remplacement d'une URL au lieu d'insérer un préfixe lors de l'utilisation du plug-in JunctionRewrite

Cette directive remplace l'action par défaut du plug-in JunctionRewrite et permet au serveur proxy de corriger certains liens d'URL dans la page HTML. Elle est utilisée avec la directive JunctionRewrite.

S'applique aux configurations avec proxy inversé uniquement.

La directive JunctionReplaceUrlPrefix demande au plug-in JunctionRewrite de remplacer l'URL *modèle_url_1* par *modèle_url_2* au lieu d'insérer un préfixe au début de l'URL.

Format

`JunctionReplaceUrlPrefix modèle_url_1 modèle_url_2`

Exemple

`JunctionReplaceUrlPrefix /server1.internaldomain.com/* /server1/*`

Dans cet exemple, supposons que l'URL est `/server1.internaldomain.com/notes.nsf` et que le préfixe est `/server1`. Au lieu d'insérer le préfixe pour réécrire l'URL et indiquer `/server1/server1.internaldomain.com/notes.nsf`, le plug-in JunctionRewrite remplace l'URL par `/server1/notes.nsf`.

Valeur par défaut

Aucun

JunctionRewrite — Active réécriture de l'URL

Cette directive active la routine de réécriture de jonction au sein de Caching Proxy de manière à réécrire les réponses provenant des serveurs d'origine pour garantir que les URL de serveur sont mappés avec le serveur d'origine approprié lors de l'utilisation de jonctions.

S'applique aux configurations avec proxy inversé uniquement.

Le plug-in de réécriture de jonction doit également être activé si vous définissez **JunctionRewrite on** sans l'option UseCookie. Les jonctions sont définies à l'aide des règles de mappage du proxy.

Consultez les sections «Utilisation de cookies à la place de JunctionRewrite», à la page 47 et «Exemple de plug-in transmogifier pour l'extension de la fonctionnalité JunctionRewrite», à la page 48 pour des informations supplémentaires sur JunctionRewrite.

Format

```
JunctionRewrite {on | on UseCookie | off}
```

Valeur par défaut

```
JunctionRewrite off
```

JunctionRewriteSetCookiePath — Réécriture de l'option dans l'en-tête Set-Cookie lors d'une utilisation avec le plug-in JunctionRewrite

Cette directive permet au serveur proxy de réécrire l'option du chemin dans l'en-tête Set-Cookie lorsque le nom du cookie est mis en correspondance. Si la réponse requiert une jonction et que le préfixe de jonction est défini, celui-ci est inséré devant chaque chemin. Cette directive peut être utilisée avec le plug-in JunctionRewrite ou la directive RewriteSetCookieDomain.

S'applique aux configurations avec proxy inversé uniquement.

Format

```
JunctionRewriteSetCookiePath nom_cookie1 nom_cookie2...
```

nom_cookie

Nom de cookie dans l'en-tête Set-Cookie.

Valeur par défaut

Aucun

JunctionSkipUrlPrefix — Ignorer la réécriture d'URL contenant déjà le préfixe lors d'une utilisation avec le plug-in JunctionRewrite

Cette directive remplace l'action par défaut du plug-in JunctionRewrite en ignorant la réécriture d'URL si le modèle d'URL est concordant. Elle est utilisée avec le plug-in JunctionRewrite pour corriger certains liens d'URL dans la page HTML. En règle générale, cette directive permet d'ignorer les URL incluant déjà un préfixe.

S'applique aux configurations avec proxy inversé uniquement.

Format

`JunctionSkipUrlPrefix modèle_url`

Exemple

`JunctionSkipUrlPrefix /server1/*`

Dans cet exemple, supposons que l'URL correspond à `/server1/notes.nsf` et que le préfixe de jonction est `/server1/`. Au lieu de réécrire l'adresse URL pour indiquer `/server1/server1/notes.nsf`, le plug-in `JunctionRewrite` ignore cette opération et l'adresse URL reste inchangée en apparaissant sous la forme `/server1/notes.nsf`.

Valeur par défaut

Aucun

KeepExpired — Indique que la copie périmée de la ressource doit être renvoyée si cette dernière est mise à jour sur le proxy

Cette directive permet d'éviter un afflux de demandes sur les serveurs dorsaux lorsqu'un objet en cache est revalidé.

Lorsqu'un objet en cache est revalidé avec le contenu sur le serveur dorsal, les demandes portant sur la même ressource sont transmises au serveur dorsal, qui les traite en tant que proxy. Il arrive parfois que l'afflux de demandes identiques entraîne l'arrêt du serveur dorsal. Vous pouvez éviter que cela se produise en activant cette directive. Lorsque cette directive est activée, une copie périmée de la ressource est renvoyée si cette dernière est mise à jour sur le proxy.

Format

`KeepExpired {on | off}`

Valeur par défaut

`KeepExpired off`

KeyRing — Spécifie le chemin du fichier de la base de données des fichiers de clés

Cette directive permet de spécifier le chemin du fichier de la base de données des fichiers de clés utilisée par le serveur pour les demandes SSL. Les fichiers de clés sont générés via l'utilitaire de gestion de clés `iKeyman`.

Remarque : Les directives SSL ne sont pas prises en charge sous SUSE Linux.

Format

`KeyRing nom_fichier`

Exemples

Windows : `KeyRing c:\Program Files\IBM\edge\cp\\key.kdb`

Linux et UNIX : `KeyRing /etc/key.kdb`

Valeur par défaut

Aucun

KeyRingStash — Spécifie le chemin du fichier des mots de passe de la base de données de clés

Cette directive permet de spécifier le chemin du fichier de mots de passe de la base de données des fichiers de clés. Le fichier de mots de passe est généré via l'utilitaire de gestion de clés iKeyman lors de la création d'un fichier de base de données de fichiers de clés.

Remarque : Les directives SSL ne sont pas prises en charge sous SUSE Linux.

Format

KeyRingStash *chemin_fichier*

Exemples

Windows : KeyRingStash c:\Program Files\IBM\edge\cp\key.sth

Linux et UNIX : KeyRingStash /etc/key.sth

Valeur par défaut

Aucun

LimitRequestBody — Définition de la taille maximale du corps dans les demandes PUT ou POST

Cette directive permet de contrôler la taille maximale du corps dans les demandes PUT ou POST. Les directives LimitRequest permettent de protéger le proxy d'éventuelles attaques.

La valeur peut être indiquée en kilo-octets (K), méga-octets (M) ou giga-octets (G).

Format

LimitRequestBody *taille_corps_max* {K | M | G}

Valeur par défaut

LimitRequestBody 10 M

LimitRequestFields — Définition du nombre maximal d'en-têtes dans les demandes client

Cette directive permet de spécifier le nombre maximal d'en-têtes qui peuvent être envoyées dans des demandes client. Les directives LimitRequest permettent de protéger le proxy d'éventuelles attaques.

Format

LimitRequestFields *nombre_en-têtes*

Valeur par défaut

LimitRequestFields 32

LimitRequestFieldSize — Définition de la longueur maximale d'un en-tête et d'une ligne de demande

Cette directive permet de spécifier la longueur maximale de la ligne de demande et la longueur maximale de chaque en-tête dans une demande. Les directives LimitRequest permettent de protéger le proxy d'éventuelles attaques.

La valeur peut être indiquée en octets (B) ou kilo-octets (K).

Format

`LimitRequestFieldSize` *longueur_max_en-tête* {B | K}

Valeur par défaut

`LimitRequestFieldSize` 4096 B

ListenBacklog — Spécifie le nombre de connexions client en file d'attente devant être gérées par le serveur

Cette directive permet de spécifier le nombre de connexions client en file d'attente devant être gérées par le serveur avant que ce dernier n'envoie des messages aux clients indiquant que les connexions sont refusées. Ce nombre dépend du nombre de demandes que le serveur peut traiter en l'espace de quelques secondes. Ne définissez pas une valeur supérieure à ce que le serveur peut traiter avant que les clients n'arrivent à expiration et ne mettent fin à la connexion.

Remarque : Si la valeur `ListenBacklog` est supérieure à la valeur `SOMAXCONN` prise en charge par TCP/IP, la valeur `SOMAXCONN` sera utilisée.

Format

`ListenBacklog`
nombre_de_demandes

Valeur par défaut

`ListenBacklog` 128

LoadInlinelImages — Contrôle la régénération des images intégrées

Cette directive permet d'indiquer si les images en ligne doivent être extraites par l'agent de la mémoire cache. Si `LoadInlinelImages` a la valeur `on`, les images intégrées à une page mise en mémoire cache seront également placées en mémoire cache. Si la valeur est `off`, les images intégrées ne sont pas mises en mémoire cache.

Format

`LoadInlineImages` {on | off}

Valeur par défaut

`LoadInlineImages` on

LoadTopCached — Indique le nombre de pages préférées à régénérer

Cette directive permet d'indiquer à l'agent de la mémoire cache qu'il doit accéder au journal des accès à la mémoire cache de la nuit précédente et charger les URL les plus demandées.

La directive `Caching` doit avoir la valeur `On`, et une valeur doit être définie pour la directive `CacheAccessLog` lorsqu'une valeur est spécifiée pour la directive `LoadTopCached`.

Format

`LoadTopCached` *nombre_de_pages*

Valeur par défaut

`LoadTopCached` 100

LoadURL — Spécifie les URL à régénérer

Cette directive permet d'indiquer les URL devant être chargées dans la mémoire cache par l'agent de la mémoire cache. Il est possible d'inclure plusieurs directives LoadURL dans le fichier de configuration, mais les caractères génériques ne sont pas autorisés.

Format

LoadURL *url*

Exemple

LoadURL http://www.ibm.com/

Valeur par défaut

Aucun

Log — Personnalise l'étape de personnalisation

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de l'étape de personnalisation. Ce code fournit la journalisation ainsi que tout autre traitement effectué une fois la connexion fermée.

Format

Log *modèle_demande*
/chemin/fichier:nom_fonction

modèle_demande

Spécifie un modèle pour les demandes qui déterminent ultérieurement si la fonction d'application est appelée. La spécification peut inclure le protocole, le domaine et l'hôte. Elle peut être précédée d'une barre oblique (/) et peut utiliser un astérisque (*) en tant que caractère générique. Par exemple, /front_page.html, http://www.ics.raleigh.ibm.com, /pub*, /* et * sont tous valides.

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme. Vous devez fournir les noms des fonctions d'ouverture, d'écriture et de fermeture.

Exemple

Log /index.html /api/bin/icsextpgm.so:log_url

Valeur par défaut

Aucun

LogArchive — Définit le comportement de la fonction d'archivage du journal

Cette directive permet de spécifier le comportement de la routine d'archivage. Cette directive affecte tous les journaux disposant de paramètres généraux. Elle indique que les journaux doivent être compressés ou purgés, ou qu'aucun traitement ne doit leur être appliqué.

Si vous spécifiez `Compress`, utilisez les directives `CompressAge` et `CompressDeleteAge` pour spécifier le moment de la compression ou de la suppression des journaux. La directive `CompressCommand` permet d'identifier la commande et les paramètres à utiliser.

Si vous spécifiez `Purge`, utilisez les directives `PurgeAge` et `PurgeSize` pour spécifier le moment de la purge des journaux.

Format

```
LogArchive {Compress | Purge | aucun}
```

Compress

Indique que la routine d'archivage compresse les journaux.

Purge

Indique que la routine d'archivage efface les journaux.

aucun

Indique que la routine d'archivage n'effectue aucun traitement.

Valeur par défaut

```
LogArchive Purge
```

Directives connexes

- «`CompressAge` — Indique à quel moment compresser les fichiers journaux», à la page 200
- «`CompressDeleteAge` — Indique à quel moment supprimer les journaux», à la page 201
- «`CompressCommand` — Spécifie la commande et les paramètres de compression», à la page 200
- «`Midnight` — Identifie le plug-in API permettant d'archiver les fichiers journaux», à la page 243
- «`PurgeAge` — Spécifie la limite d'âge pour un journal», à la page 268
- «`PurgeSize` — Spécifie la taille limite d'un fichier journal d'archivage», à la page 269

LogFileFormat — Spécifie le format du fichier journal des accès

Cette directive permet de spécifier le format de fichier des fichiers journaux des accès.

Format

```
LogFileFormat {common | combined}
```

Par défaut, le format de journal commun NCSA constitue le format d'affichage. Spécifiez `combined` pour afficher les journaux au format de journal combiné NCSA. Le format combiné ajoute des zones pour l'URL de référence, l'agent utilisateur et le cookie (si ces éléments sont présents dans la demande).

Valeur par défaut

```
LogFileFormat common
```

LogToGUI (Windows uniquement) — Affiche les entrées de journal dans la fenêtre du serveur

Systèmes Windows uniquement. Lorsque vous exécutez le proxy à partir de la ligne de commande, utilisez cette directive pour afficher les entrées dans le journal des accès. Pour optimiser les performances du serveur, cette directive est associée à la valeur off (désactivé) par défaut.

Remarque : Cette directive n'a pas d'effet si vous exécutez le proxy en tant que service.

Format

LogToGUI {on | off}

Valeur par défaut

LogToGUI off

LogToSyslog — Envoi des informations d'accès au journal système (Linux et UNIX uniquement)

Systèmes Linux et UNIX uniquement. Utilisez cette directive pour spécifier si le serveur doit consigner les demandes d'accès et les erreurs dans le journal système en complément des fichiers journaux et des accès et des erreurs.

Format

LogToSyslog {on | off}

Le fichier journal système doit exister sur le serveur pour que vous puissiez y inscrire des informations de journal d'erreurs. Vous pouvez choisir de consigner uniquement les informations d'accès ou d'erreur ou de consigner ces deux éléments.

Pour envoyer uniquement les informations d'erreur au journal système, ajoutez la ligne suivante au fichier /etc/syslog.conf :

```
user.err  
fichier_sortie_syslog_pour_informations_erreur
```

Pour envoyer uniquement les informations d'accès au journal système, ajoutez la ligne suivante au fichier /etc/syslog.conf :

```
user.info  
fichier_info_syslog_pour_informations_accès
```

Pour envoyer à la fois des informations d'accès et d'erreur au journal système, ajoutez les lignes suivantes au fichier /etc/syslog.conf :

Spécifiez *fichier_sortie_syslog* et *fichier_info_syslog* au format suivant :

- **AIX :** /var/adm/*nom_fichier_syslog*
- **HP-UX :** /var/adm/syslog/syslog.log
- **Linux :** /var/adm/messages
- **Solaris :** /var/adm/messages

Après avoir créé le fichier journal système, vous pouvez le redémarrer avec la commande suivante :

```
kill -HUP 'cat /etc/syslog.pid'
```

Valeur par défaut

LogToSyslog Off

Map — Change les demandes ayant abouti en une nouvelle chaîne de demandes, à l'aide de la chaîne du chemin de demande pour correspondance avec la règle

Cette directive permet de spécifier un modèle pour les demandes que vous voulez modifier en une nouvelle chaîne de demandes. Une fois que le serveur a changé la demande, il utilise la nouvelle chaîne de demandes et la compare aux modèles de demandes des directives suivantes.

La directive Map utilise la chaîne du chemin de demande entrante en vue d'une ///correspondance avec la règle. Voir aussi «MapQuery — Change les demandes ayant abouti en une nouvelle chaîne de demandes, à l'aide de la chaîne de demandes et du chemin de demande pour correspondance avec la règle», à la page 238.

Format

Map *modèle_demande nouvelle_demande*
[*adresse_IP_serveur* | *nom_hôte*]

modèle_demande

Spécifie un modèle pour les demandes devant être modifiées par le serveur. Le serveur compare ensuite la nouvelle chaîne de demandes aux autres modèles.

Vous pouvez utiliser un astérisque (*) en tant que caractère générique dans le modèle. Le caractère tilde (~) placé juste après une barre oblique (/) doit être indiqué explicitement. Vous ne pouvez pas utiliser de caractère générique.

nouvelle_demande

Spécifie la nouvelle chaîne de demandes à laquelle le serveur doit comparer les modèles de demande dans les directives suivantes. La chaîne spécifiée à l'aide de *nouvelle_demande* peut contenir un caractère générique si le *modèle_demande* en contient un. La partie de la demande qui correspond au caractère générique du *modèle_demande* est inséré à la place du caractère générique de l'élément *nouvelle_demande*.

[*adresse_serveur_IP* | *nom_hôte*]

Si vous utilisez plusieurs adresses IP ou noms d'hôte, utilisez ce paramètre pour spécifier une adresse IP ou un nom d'hôte. Le serveur utilise la directive uniquement pour les demandes arrivant sur le serveur à cette adresse IP ou pour cet hôte. Pour une adresse IP, il s'agit de l'adresse de la connexion réseau du serveur et non de l'adresse du client à l'origine de la demande.

Vous pouvez spécifier une adresse IP (par exemple, 240.146.167.72) ou un nom d'hôte (par exemple, hostA.raleigh.ibm.com).

Ce paramètre est facultatif. Sans ce paramètre, le serveur utilise la directive pour toutes les demandes quel que soit le nom d'hôte de l'URL ou l'adresse IP d'où elles proviennent.

Il n'est pas possible d'indiquer de caractère générique pour une adresse IP de serveur.

Exemples

- Dans l'exemple ci-dessus, le serveur extrait les demandes commençant par /truc/ et change la partie /truc/ de la demande par /bon/truc/. Tous les éléments suivant /truc/ dans la demande d'origine seront également inclus dans

la nouvelle chaîne de la demande. Par conséquent `/truc/àsavoir/` devient `/bon/truc/àsavoir/`. Le serveur utilise la nouvelle chaîne de demande et continues de la comparer aux modèles de demandes des directives suivantes.

```
Map /truc/* /bon/truc/*
```

- Les exemples suivants utilisent le paramètre d'adresse IP facultatif. Si le serveur reçoit des demandes commençant par `/truc/`, il modifie la demande en une chaîne de demandes différente en fonction de l'adresse IP de la connexion réseau d'où provient la demande. Pour les demandes provenant de 240.146.167.72, le serveur modifie la portion `/truc/` de la demande en `/clientA/bon/truc/`. Pour les demandes provenant de toute connexion ayant une adresse de 0.83.100.45, le serveur modifie la portion `/truc/` de la demande en `/clientB/bon/truc/`.

```
Map /truc/*  
/clientA/bon/truc/* 240.146.167.72  
Map /truc/* /clientB/bon/truc/* 0.83.100.45
```

- Les exemples ci-après utilisent le paramètre de nom d'hôte facultatif. Si le serveur reçoit des demandes commençant par `/truc/`, il modifie la demande en une chaîne de demandes différente en fonction du nom d'hôte dans l'URL. Pour les demandes destinées à `hôteA`, le serveur modifie la partie `/truc/` de la demande en `/clientA/bon/truc/`. Pour les demandes destinées à `hôteB`, le serveur modifie la partie `/truc/` de la demande en `/clientB/bon/truc/`.

```
Map /truc/* /clientA/bon/truc/* hôteA.bcd.com  
Map /truc/* /clientB/bon/truc/* hôteB.bcd.com
```

Valeur par défaut

Aucun

MapQuery — Change les demandes ayant abouti en une nouvelle chaîne de demandes, à l'aide de la chaîne de demandes et du chemin de demande pour correspondance avec la règle

Cette directive permet de spécifier un modèle pour les demandes que vous voulez modifier en une nouvelle chaîne de demandes. Une fois que le serveur a changé la demande, il utilise la nouvelle chaîne de demandes et la compare aux modèles de demandes des directives suivantes.

La fonctionnalité de la directive est presque la même que celle de la règle Map («Map — Change les demandes ayant abouti en une nouvelle chaîne de demandes, à l'aide de la chaîne du chemin de demande pour correspondance avec la règle», à la page 237). Toutefois, pour gérer une URL avec une chaîne de demandes, MapQuery utilise à la fois le chemin et la chaîne de demandes pour la correspondance avec la règle. Si l'URL entrante est mise en correspondance sur une règle MapQuery, l'URL convertie `///servira` à la correspondance par rapport au reste des règles.

MapQuery peut également convertir une URL avec une chaîne de demandes à une autre URL avec un autre chemin ou une autre chaîne de demandes. Toutefois, comme toutes les autres directives de mappage utilisent uniquement le chemin de demandes, la chaîne de demandes modifiée ne sera ajoutée (ne sera pas utilisée pour la correspondance des modèles) à l'URL convertie qu'en cas de correspondance du chemin de demandes.

Format

```
MapQuery modèle_demande nouvelle_demande  
[adresse_IP_serveur | nom_hôte]
```

modèle_demande

Spécifie un modèle pour les demandes devant être modifiées par le serveur. Le serveur compare ensuite la nouvelle chaîne de demandes aux autres modèles.

Vous pouvez utiliser un astérisque (*) en tant que caractère générique dans le modèle. Le caractère tilde (~) placé juste après une barre oblique (/) doit être indiqué explicitement. Vous ne pouvez pas utiliser de caractère générique.

nouvelle_demande

Spécifie la nouvelle chaîne de demandes à laquelle le serveur doit comparer les modèles de demande dans les directives suivantes. La chaîne spécifiée à l'aide de *nouvelle_demande* peut contenir un caractère générique si le *modèle_demande* en contient un. La partie de la demande qui correspond au caractère générique du *modèle_demande* est inséré à la place du caractère générique de l'élément *nouvelle_demande*.

[*adresse_serveur_IP* | *nom_hôte*]

Si vous utilisez plusieurs adresses IP ou noms d'hôte, utilisez ce paramètre pour spécifier une adresse IP ou un nom d'hôte. Le serveur utilise la directive uniquement pour les demandes arrivant sur le serveur à cette adresse IP ou pour cet hôte. Pour une adresse IP, il s'agit de l'adresse de la connexion réseau du serveur et non de l'adresse du client à l'origine de la demande.

Vous pouvez spécifier une adresse IP (par exemple, 240.146.167.72) ou un nom d'hôte (par exemple, hostA.raleigh.ibm.com).

Ce paramètre est facultatif. Sans ce paramètre, le serveur utilise la directive pour toutes les demandes quel que soit le nom d'hôte de l'URL ou l'adresse IP d'où elles proviennent.

Il n'est pas possible d'indiquer de caractère générique pour une adresse IP de serveur.

Exemples

En supposant que l'URL entrante se présente de la façon suivante :

/getsomething?type=1

et que la règle MapQuery est la suivante :

MapQuery /getsomething?type=* /gettype/*

L'URL convertie sera /gettype/1 et sera utilisée dans le mappage de règles suivant.

Proxy /gettype/* http://server/gettype/*

L'URL convertie sera http://server/gettype/1.

Valeur par défaut

Aucun

MaxActiveThreads — Spécifie le nombre maximal d'unités d'exécution actives

Cette directive permet de définir le nombre maximal d'unités d'exécution pouvant être actives simultanément. Si ce nombre maximal est atteint, le serveur conserve les nouvelles demandes jusqu'à la fin d'une autre demande et jusqu'à ce que des unités d'exécution soient disponibles. Généralement, plus votre machine est puissante, plus la valeur à utiliser pour cette directive doit être élevée. Si votre machine commence à passer trop de temps sur des tâches telles que la permutation de la mémoire, essayez de réduire cette valeur.

Format

MaxActiveThreads
nombre_unités_exécution

Valeur par défaut

MaxActiveThreads 100

MaxContentLengthBuffer — Définit la taille de la mémoire tampon pour les données dynamiques

Cette directive permet de définir la taille de la mémoire tampon pour les données dynamiques générées par le serveur. Les données dynamiques proviennent des programmes CGI, des instructions côté serveur et des programmes API.

La valeur peut être spécifiée en octets (O), kilooctets (K) ou en gigaoctets (G). Vous pouvez éventuellement insérer un caractère d'espacement entre le nombre et la valeur (O, K, M, G).

Format

MaxContentLengthBuffer *taille*

Valeur par défaut

MaxContentLengthBuffer 100 K

MaxLogFileSize — Spécifie la taille maximale de chaque fichier journal

Cette directive permet de spécifier la taille maximale de chaque fichier journal. Chaque fichier journal ne pourra pas dépasser la taille définie par cette directive. Lorsqu'un fichier journal atteint la taille définie maximale, il est fermé et un nouveau fichier journal du même nom associé à l'incrément suivant est créé.

Remarques :

1. Le composant Caching Proxy est une application 32 bits qui ouvre ses fichiers journaux avec une fonction 32 bits. Etant donné cette contrainte, n'associez *pas* au paramètres de taille maximale de fichier journal une valeur supérieure à 2 Go. Le composant Caching Proxy peut geler lorsque la taille du fichier journal dépasse 2 Go, s'il tente d'écrire des données dans le fichier journal tout en traitant activement des demandes.
2. Sur les plateformes Linux et UNIX, les fichiers journaux ne sont pas créés si le groupe sous le nom duquel s'exécute le démon ibmproxy ne dispose pas des droits d'accès en écriture dans le répertoire dans lequel se trouvent les fichiers journaux. En d'autres termes, les emplacements des fichiers journaux pour les directives de consigne figurant dans le fichier ibmproxy.conf doivent être associés aux droits d'accès en écriture pour au moins le groupe défini par la directive GroupId dans le fichier ibmproxy.conf. Ce problème ne survient que lorsque l'emplacement par défaut des fichiers journaux a été modifié ou lorsque la directive UserId ou GroupId a été modifiée dans le fichier ibmproxy.conf.

La valeur recommandée pour la définition de la directive MaxLogFileSize est entre 10 Mo au moins, mais sous 200 Mo. La taille du fichier journal réel est légèrement supérieure à celle que vous définissez. Définir une valeur trop basse affecte les performances du proxy car le serveur proxy ferme et ouvre plus fréquemment le fichier journal. Sur certaines plateformes, définir une valeur trop élevée entraîne une utilisation plus importante de la mémoire pour la mise en tampon des entrées-sorties. Lorsque la taille du fichier journal s'accroît, le proxy peut ///When

the log file size becomes larger, it can cause the proxy to run out of memory or look like a memory leak, even though the I/O buffers are controlled by the operating system.

Vous pouvez spécifier la taille maximale dans l'une des unités suivantes : octets (B), kilooctets (K), mégaoctets (M) et gigaoctets (G).

Format

MaxLogFileSize *maximum* {B | K | M | G}

Valeur par défaut

MaxLogfileSize 128 M

MaxPersistRequest — Spécifie le nombre maximal de demandes à recevoir au niveau d'une connexion permanente

Cette directive permet de spécifier le nombre maximal de demandes pouvant être reçues par le serveur au niveau d'une connexion permanente. Lorsque vous déterminez ce nombre, n'oubliez pas de prendre en compte le nombre d'images utilisées dans les pages. Pour chaque image, une demande séparée est nécessaire.

Format

MaxPersistRequest *nombre*

Valeur par défaut

MaxPersistRequest 5

MaxQueueDepth — Indique le nombre maximal d'URL à placer en file d'attente

Cette directive permet d'indiquer la profondeur maximale de la file d'attente de l'agent de cache des demandes d'extraction de pages en attente. Si vous disposez d'un système de taille importante disposant d'une grande quantité de mémoire, vous pouvez définir une file d'attente de grande taille pour les demandes d'extraction de pages sans pour autant manquer de mémoire.

La file d'attente des URL à mettre en mémoire cache est déterminée au début de chaque exécution d'agent de la mémoire cache. Si vous indiquez à l'agent de la mémoire cache de suivre les liens hypertexte vers les autres URL, ces autres URL ne seront pas comptées dans la file d'attente de la mémoire cache. Une fois que la valeur spécifiée dans la directive MaxURLs est atteinte, l'agent de la mémoire cache s'arrête même s'il reste des URL dans la file d'attente.

Format

MaxQueueDepth
profondeur_maximum

Valeur par défaut

MaxQueueDepth 250

MaxRuntime — Identifie la durée maximale de l'exécution d'un agent de la mémoire cache

Cette directive permet d'indiquer la durée maximale pendant laquelle l'agent de la mémoire cache extrait les URL lors d'une exécution particulière. La valeur 0 indique que l'exécution de l'agent de la mémoire cache n'est pas interrompue.

Format

MaxRuntime {0 | *durée_maximum*}

Exemple

MaxRuntime 2 heures 10 minutes

Valeur par défaut

MaxRuntime 2 heures

MaxSocketPerServer — Spécifie le nombre maximal de sockets inactives ouvertes pour le serveur

Cette directive permet de définir le nombre maximal de sockets inactives ouvertes pour un serveur d'origine, quel qu'il soit. N'utilisez cette directive que si la valeur on est attribuée à la directive ServerConnPool.

Format

MaxSocketPerServer *numéro*

Exemple

MaxSocketPerServer 10

Valeur par défaut

MaxSocketPerServer 5

MaxUrls — Indique le nombre maximal d'URL à régénérer

Cette directive permet d'identifier le nombre maximal d'URL extraites par l'agent de la mémoire cache lors d'une exécution particulière. La valeur 0 signifie qu'il n'existe aucune limite. Lorsque vous utilisez le mode automatique de l'agent de la mémoire cache, les directives LoadURL et LoadTopCached sont prioritaires sur les directives MaxURLs.

Format

MaxURLs *nombre_maximum*

Valeur par défaut

MaxURLs 2000

Member — Spécifie un membre d'un tableau

Cette directive permet de spécifier les membres des groupes qui sont partagés par les serveurs utilisant l'accès distant à la mémoire cache.

Remarque : Lors de la configuration d'un tableau, la directive Hostname doit être configurée de la même manière pour tous les membres du tableau.

Format

```
Member nom {  
  sous-directive  
  sous-directive  
  .  
  .  
}
```

Les sous-directives suivantes sont incluses :

RCAAddr

Cette sous-directive obligatoire identifie l'adresse IP ou le nom d'hôte de la communication RCA.

RCAPort

Cette sous-directive obligatoire identifie le port pour les communications RCA. Le port doit être compris entre 1024 et 65535.

CacheSize {*n* octets | *n* Ko | *n* Mo | *n* Go }

Cette sous-directive obligatoire spécifie la taille de la mémoire cache de ce membre, qui doit être une valeur positive.

[Timeout *n* millisecondes | *n* secondes | *n* heures | *n* jours | *n* mois | *n* années | toujours]

Identifie la durée d'attente pour le membre. *n* doit être un entier positif. Le délai est facultatif ; la valeur par défaut est de 1000 millisecondes. Les valeurs du délai d'expiration sont généralement définies en secondes ou millisecondes.

[BindSpecific {on | off}]

Permet que les communications se produisent au niveau d'un sous-réseau privé, offrant une mesure de sécurité. BindSpecific est facultatif ; la valeur par défaut est On.

[ReuseAddr {on | off}]

Permet de rejoindre le tableau plus rapidement. Si la valeur du paramètre est On, tous les autres processus peuvent utiliser ce port, ce qui peut provoquer un comportement anarchique. ReuseAddr est facultatif ; la valeur par défaut est Off.

Exemple

```
Member douxamer.chocolat.ibm.com {
  RCAAddr      127.0.0.1
  RCAPort      6294
  CacheSize    25G
  Timeout      500 millisecondes
  BindSpecific On
  ReuseAddr    Off
}
```

Valeur par défaut

Aucun

Midnight — Identifie le plug-in API permettant d'archiver les fichiers journaux

Cette directive permet de définir le plug-in de l'application à exécuter à minuit pour l'archivage des journaux. La directive est initialisée lors de l'installation. Si vous ne spécifiez pas cette directive dans le fichier de configuration, l'archivage n'est pas effectué.

Format

```
Midnight
/chemin/fichier:nom_fonction
/chemin/fichier
```

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme.

Valeurs par défaut

- **Linux et UNIX** : Midnight /usr/lib/archive.so:begin
- **Windows** : Midnight C:\Program Files\IBM\edge\cp\bin\archive.dll:begin

NameTrans — Personnalise l'étape de conversion de nom

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de l'étape de conversion de nom. Ce code fournit le mécanisme de conversion du chemin virtuel dans la demande en chemin physique sur le serveur, mappant les URL vers des objets spécifiques.

Remarque : Il ne s'agit pas d'une règle de mappage de terminal. L'URL transformée doit correspondre à une des directives de règle de mappage de terminal telles que Exec, Fail, Map, Pass, Redirect et Service.

Format

```
NameTrans modèle_demande /chemin/fichier:nom_fonction  
[adresse_serveur_IP | nom_hôte]
```

modèle_demande

Spécifie un modèle pour les demandes qui déterminent ultérieurement si la fonction d'application est appelée. La spécification peut inclure le protocole, le domaine et l'hôte. Elle peut être précédée d'une barre oblique (/) et peut utiliser un astérisque (*) en tant que caractère générique. Par exemple, /front_page.html, http://www.ics.raleigh.ibm.com, /pub*, /* et * sont tous valides.

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme.

[adresse_IP_serveur | nom_hôte]

Si vous utilisez plusieurs adresses IP ou hôtes virtuels, cette directive détermine si la fonction d'application sera appelée uniquement pour les demandes provenant d'une adresse IP spécifique ou d'un hôte spécifique.

Il n'est pas possible d'indiquer de caractère générique pour une adresse IP de serveur.

Remarque : La directive doit être entrée sur une seule ligne même si elle est présentée ici sur deux lignes.

Exemple

```
NameTrans /index.html /api/bin/icsextpgm.so:trans_url
```

Valeur par défaut

Aucun

NoBG — Exécute le processus Caching Proxy en avant-plan

Sur les plateformes Linux et UNIX, cette directive permet d'empêcher le processus du serveur Caching Proxy de s'exécuter automatiquement en arrière-plan. La valeur par défaut de cette directive est off. Son format est :

```
NoBG [on | off]
```

Remarque : L'option `-nobg` dans la cas de la commande `ibmproxy` n'est pas valide sur les systèmes Windows.

Exemple

NoBG on

Valeur par défaut

NoBG off

NoCaching — Ne met pas en mémoire cache les fichiers dont l'URL correspond à un modèle

Cette directive permet d'indiquer que le serveur ne doit pas mettre en mémoire cache les fichiers dont les URL correspondent au modèle donné. Vous pouvez utiliser plusieurs occurrences de cette directive dans le fichier de configuration. Incluez une directive séparée pour chaque modèle. Le modèle d'URL doit inclure le protocole.

Si ni `CacheOnly` ni `NoCaching` n'est défini, toute URL peut être mise en mémoire cache.

Format

NoCaching *modèle_URL*

Exemple

NoCaching http://joke/*

Valeur par défaut

Aucun

NoLog — Supprime les entrées de journal pour des hôtes spécifiques ou des domaines correspondant à un modèle

Cette directive permet d'indiquer que vous ne voulez pas consigner les demandes d'accès effectuées à partir d'hôtes spécifiques ou de domaines correspondant à un modèle donné. Par exemple, vous pouvez ne pas vouloir consigner les demandes d'accès à partir des hôtes locaux.

Vous pouvez utiliser plusieurs occurrences de cette directive dans le fichier de configuration. Vous pouvez également placer plusieurs modèles au niveau de la même directive si vous les séparez par un ou plusieurs caractères d'espacement. Vous pouvez utiliser des noms d'hôte ou des adresses IP au niveau des modèles.

Remarque : Pour utiliser des modèles de nom d'hôte, vous devez attribuer la valeur `On` à la directive `DNS-Lookup`. Si la valeur `Off` est attribuée à la directive `DNS-Lookup` (valeur par défaut), vous pouvez utiliser uniquement les modèles d'adresse IP.

Format

NoLog {*nom_hôte* |
adresse_IP} [...]

Exemple

NoLog 128.0.* *.edu localhost.*

Valeur par défaut

Aucun

no_proxy — Spécifie les modèles pour la connexion directe aux domaines

Si vous utilisez la directive `http_proxy`, `ftp_proxy` ou `gopher_proxy` pour l'enchaînement de proxys, vous pouvez faire appel à cette directive pour spécifier les domaines auxquels le serveur se connecte directement sans passer par un proxy.

Spécifiez la valeur en tant que chaîne de noms de domaines ou de modèles de nom de domaine. Séparez chaque entrée de la chaîne par une virgule. Ne placez *pas* de caractères d'espacement dans la chaîne.

Le mode d'entrée des modèles de cette directive est différent de celui des autres directives. Avant tout, vous ne *pouvez pas* utiliser le caractère générique (*). Vous *pouvez* spécifier un modèle en incluant uniquement la dernière partie d'un nom de domaine. Le serveur se connecte directement aux domaines se terminant par une chaîne correspondant aux modèles spécifiés. Cette directive s'applique uniquement au chaînage de proxys et est équivalente à une ligne `@/=` directe dans le fichier de configuration de SOCKS.

Format

```
no_proxy  
nom_domaine_ou_modèle[,...]
```

Exemple

```
no_proxy www.someco.com,.raleigh.ibm.com,.some.host.org:8080
```

Dans cet exemple, le serveur ne passe pas par un proxy pour les demandes suivantes :

- Toutes les demandes de domaine finissant par `www.someco.com`
- Toutes les demandes de domaine finissant par `.raleigh.ibm.com`, telles que `blugrass.raleigh.ibm.com` ou `keystone.raleigh.ibm.com`
- Toutes les demandes de port 8080 de domaines se terminant par `hôte.org`, telles que `monnom.hôte.org:8080`. (Les demandes d'autres ports du même domaine, tels que `monnom.hôte.org` pour lequel le port 80 est sous-entendu, ne sont pas incluses.)

Valeur par défaut

Aucun

NoCacheOnRange — Indique la non mise en cache pour les demandes Range

Par défaut, lors de la réception d'une demande Range des navigateurs, Caching Proxy exige une réponse complète du serveur dorsal. Caching Proxy supprime l'en-tête Range de la demande, puis achemine cette dernière jusqu'au serveur dorsal. Une fois la réponse mise en cache sur le serveur proxy les demandes suivantes portant sur les mêmes ressources sont traitées sur le même serveur proxy, que les demandes soient des demandes Range ou non. En général, l'action par défaut de Caching Proxy améliore les performances et permet des temps de réponse plus courts pour les clients. Cependant, si la réponse ne peut pas être mise en mémoire cache, ou si elle est très volumineuse, l'action par défaut réduit les performances.

Utilisez la directive `NoCacheOnRange`, qui spécifie l'absence de mise en cache pour les demandes `Range`, pour résoudre l'incident décrit lors de l'utilisation de la configuration par défaut.

Lorsque vous activez la directive globalement dans le fichier `ibmproxy.conf` ou si vous l'activez comme option de la règle de mappage `PROXY`, Caching Proxy achemine l'en-tête de demande `Range` au serveur dorsal. Toutefois, Caching Proxy ne met pas en mémoire cache la réponse 206 (contenu partiel) du serveur dorsal.

L'activation de la directive `NoCacheOnRange` peut améliorer les performances du proxy dans les cas suivants :

- Les réponses ne peuvent pas être mises en cache ou mises à jour fréquemment.
- Le temps de réponse est critique pour l'application.

Format

`NoCacheOnRange` [on | off]

Exemple

Vous pouvez également activer `NoCacheOnRange` dans une règle de mappage de proxy :

```
Proxy /not-cachable/* http://server.com/no-cachable-resources/* NoCacheOnRange
```

Valeur par défaut

`NoCacheOnRange` off

NoProxyHeader — Indique les en-têtes de client à bloquer

Cette directive permet d'indiquer les en-têtes d'URL client à bloquer. Tout en-tête HTTP envoyé par un client peut être bloqué, y compris les en-têtes requis. Soyez très vigilant lorsque vous bloquez les en-têtes. Les en-têtes communs incluent :

- **Pragma** :—Permet généralement d'indiquer aux navigateurs et aux serveurs dotés de mémoire cache d'extraire le fichier du serveur d'origine lorsque le fichier est demandé.
- **Referer** :—URL du fichier à partir duquel l'URI de demande a été obtenu.

Pour plus de détails, reportez-vous aux spécifications de protocole HTTP. Cette directive peut être spécifiée plusieurs fois.

Format

`NoProxyHeader` *en-tête*

Exemple

```
NoProxyHeader Referer:
```

Valeur par défaut

Aucun

NumClients — Indique le nombre d'unités d'exécution d'agent de la mémoire cache

Cette directive permet de spécifier le nombre d'unités d'exécution utilisées par l'agent de la mémoire cache pour l'extraction des pages se trouvant dans la file d'attente. Définissez le nombre d'unités d'exécution en fonction de la vitesse du réseau interne et de votre connexion à Internet. La plage admise est comprise entre 1 et 100.

Remarque : L'emploi de plus de six unités d'exécution peut entraîner des demandes excessivement rapides à l'intention des serveurs de contenu.

Format

NumClients *nombre*

Valeur par défaut

NumClients 4

ObjectType — Personnalise l'étape de type d'objet

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de l'étape de type d'objet. Ce code situe l'objet demandé dans le système de fichiers et spécifie son type MIME.

Format

ObjectType *modèle_demande*
/chemin/fichier:nom_fonction

modèle_demande

Spécifie un modèle pour les demandes qui déterminent ultérieurement si la fonction d'application est appelée. La spécification peut inclure le protocole, le domaine et l'hôte. Elle peut être précédée d'une barre oblique (/) et peut utiliser un astérisque (*) en tant que caractère générique. Par exemple, /front_page.html, http://www.ics.raleigh.ibm.com, /pub*, /* et * sont tous valides.

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme.

Exemple

ObjectType /index.html /api/bin/icsextpgm.so:obj_type

Valeur par défaut

Aucun

OptimizeRuleMapping — Optimise le processus de mappage de règle pour les demandes entrantes lors de l'augmentation du nombre de règles

Cette directive accélère le processus de mappage de règles pour les demandes entrantes lorsque le nombre de règles augmente.

Lorsque vous activez la directive OptimizeRuleMapping, au lieu de mapper les demandes d'URI entrantes par rapport à chaque règle une par une, le proxy mappe l'URI par rapport à un arbre de préfixes. L'arbre de préfixes aide le proxy à supprimer la ///comparaison de chaînes redondantes dans les règles de mappage. Caching Proxy obtient alors de meilleures performances lorsque le nombre de règles de votre configuration dépasse 300.

Format

OptimizeRuleMapping [on | off]

Valeur par défaut

OptimizeRuleMapping off

OutputTimeout — Spécifie le délai de sortie

Cette directive permet de définir la durée maximale pendant laquelle le serveur peut envoyer des données à un client. La limite de temps s'applique aux demandes de fichiers locaux et aux demandes pour lesquelles le serveur se comporte comme un proxy. La limite de temps ne s'applique pas aux demandes qui commencent par un programme CGI.

Si le serveur n'envoie pas de réponse complète dans le laps de temps défini par cette directive, le serveur met fin à la connexion. Spécifiez la durée en combinant des heures, des minutes (ou mn) et des secondes (ou s).

Format

OutputTimeout *durée*

Valeur par défaut

OutputTimeout 30 minutes

PacFilePath — Spécifie le répertoire contenant les fichiers PAC

Cette directive permet de spécifier le répertoire contenant les fichiers de configuration automatique du proxy générés à l'aide du formulaire de configuration de fichier PAC.

Format

PacFilePath *chemin_répertoire*

Valeurs par défaut

- **Windows** : PacFilePath c:\Program Files\IBM\edge\cp\HTML\pacfiles
- **Linux et UNIX** : PacFilePath /opt/ibm/edge/cp/racine_serveur/pub/pacfiles

Pass — Spécifie le modèle pour l'acceptation des requêtes

Cette directive permet de spécifier un modèle pour les demandes à accepter et auxquelles vous voulez répondre avec un fichier provenant de votre serveur. Une fois qu'une demande correspond à un modèle d'une directive Pass, la demande n'est pas comparée aux modèles de demande des directives suivantes.

Format

Pass *modèle_demande* [*chemin_fichier* [*adresse_IP_serveur* | *nom_hôte*]]

modèle_demande

Spécifie un modèle pour les demandes à accepter et auxquelles vous voulez répondre avec un fichier provenant de votre serveur.

Vous pouvez utiliser un astérisque (*) en tant que caractère générique dans le modèle. Le caractère tilde (~) placé juste après une barre oblique (/) doit être indiqué explicitement. Vous ne pouvez pas utiliser de caractère générique.

[*chemin_fichier*]

Indique le chemin du fichier devant être renvoyé par le serveur. Le *chemin_fichier* peut contenir un caractère générique si le *modèle_demande* en comporte un. La partie de la demande qui correspond au caractère générique du *modèle_demande* est inséré à la place du caractère générique de l'élément *nouvelle_demande*.

Ce paramètre est facultatif. Si vous ne spécifiez aucun chemin, la demande elle-même est utilisée en tant que chemin.

[*adresse_serveur_IP* | *nom_hôte*]

Si vous utilisez plusieurs adresses IP ou noms d'hôte, utilisez ce paramètre pour spécifier une adresse IP ou un nom d'hôte. Le serveur utilise la directive uniquement pour les demandes arrivant sur le serveur à cette adresse IP ou pour cet hôte. Pour une adresse IP, il s'agit de l'adresse de la connexion réseau du serveur et non de l'adresse du client à l'origine de la demande.

Vous pouvez spécifier une adresse IP (par exemple, 240.146.167.72) ou un nom d'hôte (par exemple, hostA.raleigh.ibm.com).

Ce paramètre est facultatif. Sans ce paramètre, le serveur utilise la directive pour toutes les demandes quel que soit le nom d'hôte de l'URL ou l'adresse IP d'où elles proviennent.

Il n'est pas possible d'indiquer de caractère générique pour une adresse IP de serveur.

Exemples

- Dans les exemples suivants, le serveur répond à une demande commençant par /updates/parts/ avec un fichier figurant dans le chemin indiqué, en fonction du système d'exploitation. Tout ce qui suit /updates/parts/ est également utilisé pour spécifier le fichier.

Systèmes Linux et UNIX : Pass /updates/parts/* /opt/ibm/edge/cp/racine_serveur/pub/*

Systèmes Windows : Pass /updates/parts/* c:\Program Files\IBM\edge\cp\pub*

- Dans l'exemple ci-dessus, le serveur répond à une demande commençant par /gooddoc/ avec un fichier provenant de /gooddoc. Ainsi, le serveur répond à la demande /gooddoc/volume1/issue2/newsletter4.html par le fichier /gooddoc/volume1/issue2/newsletter4.html.

Pass /gooddoc/*

- Les exemples suivants utilisent le paramètre d'adresse IP facultatif. Si le serveur reçoit des demandes commençant par /parts/, il renvoie un fichier provenant d'un répertoire différent en fonction de l'adresse IP de la connexion réseau d'où provient la demande. Pour les demandes provenant de 240.146.167.72, le serveur renvoie un fichier provenant de /customerA/catalog/. Pour les demandes provenant de toute connexion ayant une adresse de 0.83.100.45, le serveur renvoie un fichier provenant de /customerB/catalog/.

Pass /parts/* /customerA/catalog/* 240.146.167.72

Pass /parts/* /customerB/catalog/* 0.83.100.45

- Les exemples ci-après utilisent le paramètre de nom d'hôte facultatif. Si le serveur reçoit des demandes commençant par /parts/, il renvoie un fichier provenant d'un répertoire différent en fonction du nom d'hôte dans l'URL. Pour les demandes destinées à hôteA, le serveur renvoie un fichier provenant de /customerA/catalog/. Pour les demandes destinées à hôteB, le serveur renvoie un fichier provenant de /customerB/catalog/.

Systèmes AIX

Pass /Admin/* /usr/lpp/internet/server_root/Admin/*

Pass /Docs/* /usr/lpp/internet/server_root/Docs/*

Pass /errorpages/* /usr/lpp/internet/server_root/pub/errorpages/*

Pass /* /usr/lpp/internet/server_root/pub/*

Systèmes Solaris, HP-UX et Linux

```

Pass    /Admin/*    /opt/ibm/edge/cp/racine_serveur/Admin/*
Pass    /Docs/*    /opt/ibm/edge/cp/racine_serveur/Docs/*
Pass    /errorpages/* /opt/ibm/edge/cp/racine_serveur/pub/errorpages/*
Pass    /*        /opt/ibm/edge/cp/server_root/pub/*

```

Valeurs par défaut

Systèmes AIX

```

Pass    /Admin/*    /usr/lpp/internet/server_root/Admin/*
Pass    /Docs/*    /usr/lpp/internet/server_root/Docs/*
Pass    /errorpages/* /usr/lpp/internet/server_root/pub/errporpages/*
Pass    /*        /usr/lpp/internet/server_root/pub/*

```

Systèmes HP-UX, Linux et Solaris

```

Pass    /Admin/*    /opt/ibm/edge/cp/racine_serveur/Admin/*
Pass    /Docs/*    /opt/ibm/edge/cp/racine_serveur/Docs/*
Pass    /errorpages/* /opt/ibm/edge/cp/racine_serveur/pub/errorpages/*
Pass    /*        /opt/ibm/edge/cp/racine_serveur/pub/*

```

Systèmes Windows

```

Pass    /icons/*    C:\Program Files\IBM\edge\cp\icons\*
Pass    /Admin/*    C:\Program Files\IBM\edge\cp\Admin\*
Pass    /Docs/*    C:\Program Files\IBM\edge\cp\Docs\*
Pass    /erropages/* C:\Program Files\IBM\edge\cp\pub\errorpages\*
Pass    /*        C:\Program Files\IBM\edge\cp\pub\*

```

PersistTimeout — Spécifie la durée d'attente avant que le client n'envoie une autre demande

Cette directive permet de spécifier la durée pendant laquelle le serveur doit attendre entre les demandes client avant d'annuler une connexion permanente. La durée peut être exprimée selon tout incrément de durée valide, toutefois les secondes et les minutes sont les plus utilisées.

Le serveur utilise une directive de délai différente, `InputTimeout`, pour déterminer le temps d'attente pour l'envoi de la première demande du client une fois la connexion établie. Pour plus d'informations sur le délai d'entrée, voir «`InputTimeout` — Spécifie le délai d'entrée», à la page 229.

Une fois que le serveur a envoyé la première réponse, il utilise la valeur définie pour `PersistTimeout` pour déterminer la longueur de l'attente de chaque demande suivante avant d'annuler la connexion permanente.

Format

`PersistTimeout` *durée*

Valeur par défaut

`PersistTimeout` 4 secondes

PICSDBLookup — Personnalise l'étape d'extraction de libellés PICS

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur pour extraire des libellés PICS pour une URL spécifiée. La fonction peut soit créer dynamiquement un libellé PICS pour le fichier demandé, soit rechercher un libellé PICS dans une base de données ou un fichier de remplacement.

Format

`PICSDBLookup` */chemin/fichier:nom_fonction*

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme.

Exemple

PICSDBLookup /api/bin/icsext05.so:get_pics

Valeur par défaut

Aucun

PidFile (Linux et UNIX uniquement) — Définition du fichier utilisé pour stocker l'ID processus de Caching Proxy

Linux et UNIX uniquement. Utilisez cette directive pour spécifier l'emplacement du fichier qui contient l'ID processus de Caching Proxy. Lorsque le processus du serveur est lancé, il enregistre les ID processus (PID) dans un fichier. Si vous exécutez plusieurs instances du serveur sur un seul système, chaque instance doit posséder son propre fichier d'ID processus.

Format

PidFile
chemin_vers_infos_fichier_PID

Exemple

PidFile /usr/pidinfo

Valeurs par défaut

- Si une directive ServerRoot est indiquée : PidFile *racine-serveur>/ibmproxy-pid*
- Si aucune directive ServerRoot n'est indiquée : PidFile */tmp/ibmproxy-pid*

PKCS11DefaultCert, PKCS11DriverPath, PKCS11TokenPassword — Prend en charge la carte IBM 4960 PCI Cryptographic Accelerator Card (AIX uniquement)

Sur les systèmes AIX, pour prendre en charge la carte IBM 4960 PCI Cryptographic Accelerator Card, des directives supplémentaires sont fournies.

Utilisez ces trois directives pour autoriser le proxy à : charger le pilote de périphérique, ouvrir le pilote de périphérique et accéder aux certificats stockés sur le périphérique. Lors du chargement du pilote de périphérique, le serveur proxy utilise automatiquement le périphérique pour augmenter la vitesse de communication SSL.

Voir aussi «SSLCryptoCard — Spécifie la carte de chiffrement installée», à la page 282.

Format

PKCS11DefaultCert *libellé_cert_défaut*

Indiquez le label de certificat SSL par défaut stocké sur le jeton du périphérique.

PKCS11DriverPath *chemin_absolu_au_pilote_de_carte*

Indiquez le chemin d'accès absolu au pilote de périphérique pour la carte Cryptographic Accelerator Card.

PKCS11TokenPassword *mot de passe*

Indiquez le mot de passe pour ouvrir le périphérique de jeton.

Exemple

```
PKCS11DefaultCert MyDefaultCertInTheToken
PKCS11DriverPath /usr/lib/pkcs11/PKCS11_API.so
PKCS11TokenPassword MyPasswordToOpenTheToken
```

Valeur par défaut

Aucun

Directives de plug-in

Les directives mentionnées ci-dessous ont été ajoutées au fichier `ibmproxy.conf` de Caching Proxy pour activer de nouvelles fonctions et extensions. Les formulaires de configuration et d'administration ne sont pas disponibles pour modifier la plupart de ces directives. Il faut utiliser un éditeur de texte standard, comme vi ou emacs, pour les modifier manuellement. Vous trouverez dans ce chapitre, par ordre alphabétique, d'autres informations relatives à chacune de ces nouvelles directives.

- «ExternalCacheManager — Configure Caching Proxy pour la mise en mémoire cache dynamique à partir de IBM WebSphere Application Server», à la page 218
- «ICP_Address — Spécifie l'adresse IP des requêtes ICP», à la page 225
- «ICP_Port — Spécifie le numéro de port des requêtes ICP», à la page 226
- «ICP_Timeout — Spécifie le délai d'attente maximal des requêtes ICP», à la page 226
- «Occupier — Spécifie un membre de cluster ICP», à la page 225
- «ICP_MaxThreads — Spécifie le nombre maximal d'unités d'exécution pour requêtes ICP», à la page 225
- «SignificantURLTerminator — Spécifie un code d'arrêt pour les demandes d'URL», à la page 280
- «SSLCertificate — Spécifie les libellés des clés pour les certificats», à la page 281
- «SSLOnly — Désactive les unités d'exécution à l'écoute pour les demandes HTTP», à la page 283

Dans le fichier `ibmproxy.conf`, il faut entrer les directives utilisées pour configurer l'extension du Caching Proxy, au format suivant :

```
<MODULEBEGIN> nom de l'extension
subdirective1
subdirective2

<MODULEEND>
```

Chaque programme d'extension analyse le fichier `ibmproxy.conf` et lit uniquement son propre bloc de sous-directives. L'analyseur de Caching Proxy ne tient pas compte de toutes les informations qui figurent entre `<MODULEBEGIN>` et `<MODULEEND>`.

Les plug-ins de Caching Proxy et certaines nouvelles fonctions requièrent l'ajout des directives API dans le fichier `ibmproxy.conf`. Dans la mesure où le serveur proxy interagit avec les plug-ins dans l'ordre dans lequel ils sont listés, soyez prudent lorsque vous décidez de l'ordre des directives dans le fichier de configuration du proxy. En effet, des directives données à titre de prototype (sous forme de commentaires) ont été ajoutées à la section API du fichier `ibmproxy.conf`.

Ces directives API sont placées dans un ordre délibérément choisi. Lors de l'ajout de directives d'API pour permettre de nouvelles fonctionnalités et l'utilisation de plug-ins, respectez l'ordre dans lequel figurent les directives dans la section Prototypes du fichier de configuration. Vous pouvez également supprimer les marques de commentaires et modifier, si nécessaire, les directives API pour chacune des fonctionnalités ou chacun des plug-ins souhaités. Ajoutez les plug-ins générés par l'utilisateur après ceux qui sont fournis avec le produit.

Port — Spécifie le port sur lequel le serveur attend les demandes

Cette directive permet de spécifier le numéro du port sur lequel le serveur attend les demandes. Le numéro de port standard pour HTTP est 80. Les autres numéros de port inférieurs à 1024 sont réservés aux autres applications TCP/IP et ne doivent pas être utilisés. Les ports généralement utilisés pour les serveurs Web proxy sont les ports 8080 et 8008.

Lorsqu'un port différent de 80 est utilisé, les clients sont requis afin d'inclure un numéro de port spécifique pour les demandes destinées au serveur. Le numéro de port est précédé du caractère deux-points (:) et est placé après le nom d'hôte dans l'URL. Par exemple, à partir du navigateur, l'URL `http://www.turfco.com:8008/` demande la page de bienvenue par défaut provenant d'un hôte nommé `www.turfco.com` à l'écoute du port 8008.

Vous pouvez utiliser l'option **-p** dans la commande **ibmproxy** pour remplacer ce paramètre lors du démarrage du serveur.

Format

Port *numéro*

Si vous changez cette directive, vous devez arrêter le serveur puis le redémarrer pour que le changement soit effectif. La modification n'est pas prise en compte si vous redémarrez le serveur sans l'arrêter. (Voir Chapitre 5, «Démarrage et arrêt de Caching Proxy», à la page 15.)

Valeur par défaut

Port 80

PostAuth — Personnalise l'étape PostAuth

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de l'étape PostAuth. Ce code sera exécuté quels que soient les codes retour provenant des étapes précédentes ou des gestionnaires PostAuth. Vous pouvez ainsi nettoyer les ressources attribuées pour traiter la demande.

Format

PostAuth */chemin/fichier:nom_fonction*

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom de la fonction d'application au sein de votre programme.

Exemple

AuthExit */ics/api/bin/icsext05.so:post_exit*

Valeur par défaut

Aucun

PostExit — Personnalise l'étape PostExit

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de l'étape PostExit. Ce code sera exécuté quels que soient les codes retour provenant des étapes précédentes ou des gestionnaires PostExit. Vous pouvez ainsi nettoyer les ressources attribuées pour traiter la demande.

Format

`PostExit /chemin/fichier:nom_fonction`

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom de la fonction d'application au sein de votre programme.

Exemple

`PostExit /ics/api/bin/icsext05.so:post_exit`

Valeur par défaut

Aucun

PreExit — Personnalise l'étape PreExit

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de l'étape PreExit. Ce code sera exécuté après la lecture d'une demande client et avant tout autre traitement. Vous pouvez appeler le module GoServe lors de cette étape.

Format

`PreExit /chemin/fichier:nom_fonction`

/chemin/fichier

Indique le nom complet du fichier du DLL compilé, comprenant l'extension.

nom_fonction

Indique le nom de la fonction d'application au sein de votre programme.

Exemple

`PreExit /ics/api/bin/icsext05.so:pre_exit`

Valeur par défaut

Aucun

Protect — Active une configuration de protection pour les demandes correspondant à un modèle

Cette directive permet d'activer les règles de configuration de protection pour les demandes correspondant à un modèle.

Remarque : Pour que la protection fonctionne correctement, les directives DefProt et Protect doivent être placées avant les directives Pass, Exec ou Proxy dans le fichier de configuration.

La configuration de protection est définie par les sous-directives de protection. Le format de la directive diffère selon que vous voulez désigner un libellé ou un fichier contenant les sous-directives de protection ou que vous voulez inclure les sous-directives de protection dans la directive Protect.

Format

Ce paramètre peut prendre une des formes suivantes :

- La directive Protect peut être spécifiée sous la forme d'un chemin complet et d'un nom de fichier identifiant un fichier séparé contenant les sous-directives de protection. Elle peut également être définie sous la forme d'un nom de libellé de configuration de protection correspondant à un nom défini précédemment dans une directive Protection. La directive Protection contient les sous-directives de protection. Utilisez ce format :

```
Protect modèle_demande [fichier_configuration | libellé]  
      [FOR Adresse_IP_serveur | nom_hôte]
```

Remarque : La directive doit être entrée sur une seule ligne même si elle est présentée ici sur deux lignes.

- Vous pouvez spécifier les sous-directives de protection proprement dites dans la directive Protect. Les sous-directives doivent être comprises dans des accolades ({}). L'accolade de gauche doit être le dernier caractère sur la même ligne que la directive Protect. Chaque sous-directive suit sur sa propre ligne. L'accolade de droite doit être sur sa propre ligne suivant la dernière ligne de sous-directive. Vous ne pouvez pas placer de lignes de commentaire entre les accolades. Si vous voulez inclure les sous-directives de protection dans la directive Protection, le format est le suivant :

```
Protect  
modèle_demande [FOR adresse_serveur_IP |  
nom_hôte]  
    sous-directive valeur  
    sous-directive valeur  
    .  
    .  
    .  
}
```

Les paramètres suivants sont utilisés :

modèle_demande

Spécifie un modèle pour les demandes pour lesquelles la protection doit être activée. Le serveur compare les demandes client au modèle et active la protection lorsqu'une correspondance est trouvée.

[*fichier_configuration* | *libellé*]

Si vous désignez un libellé ou un fichier contenant les sous-directives de protection, ce paramètre permet d'identifier la configuration de protection à activer pour les demandes correspondant à l'élément *modèle_demande*.

Ce paramètre est facultatif. S'il est omis, la configuration de protection est définie par la protection DefProt la plus récente qui contient un modèle concordant.

[FOR *adresse_serveur_IP* | *nom_hôte*]

Si vous utilisez plusieurs adresses IP ou noms d'hôte, utilisez ce paramètre pour spécifier une adresse IP ou un nom d'hôte. Le serveur utilise la directive uniquement pour les demandes arrivant sur le serveur à cette adresse IP ou pour cet hôte. Pour une adresse IP, il s'agit de l'adresse de la connexion réseau du serveur et non de l'adresse du client à l'origine de la demande. La protection d'une adresse IP s'applique à l'adresse IP et au nom d'hôte entier

qualifié. Cependant, si le serveur est appelé à l'intérieur de son réseau avec un nom autre que le nom d'hôte entier qualifié (avec une entrée d'un fichier de noms d'hôte, par exemple), il n'est pas protégé.

Exemple :

```
Protect http://x.x.x.x PROT-ADMIN
```

A partir d'un navigateur Web :

- `http://x.x.x.x` est protégé
- `http://nomhote.exemple.com` est protégé
- `http://nomhote` n'est pas protégé

Exemple :

```
Protect http://nomhote.exemple.com PROT-ADMIN
```

A partir d'un navigateur Web :

- `http://x.x.x.x` est protégé
- `http://nomhote.exemple.com` est protégé
- `http://nomhote` n'est pas protégé

Vous pouvez spécifier une adresse IP (par exemple, FOR 240.146.167.72) ou un nom d'hôte (par exemple, FOR hostA.bcd.com).

Vous ne pouvez pas utiliser de caractères génériques pour spécifier les adresses IP.

Ce paramètre est facultatif. Sans ce paramètre, le serveur utilise la directive pour toutes les demandes quel que soit le nom d'hôte de l'URL ou l'adresse IP d'où elles proviennent.

Remarque : Le paramètre [*adresse_serveur_IP* | *nom_hôte*] est utilisé soit avec le paramètre [*fichier_configuration* | *libellé*] soit avec le paramètre *valeur sous-directive*.

- Pour utiliser [*adresse_serveur_IP* | *nom_hôte*] avec [*fichier_configuration* | *libellé*], vous devez insérer FOR, ou une autre chaîne de caractères (sans espaces) entre le paramètre [*fichier_configuration* | *libellé*] et les paramètres *adresse_serveur_IP* | *nom_hôte*.
- Pour utiliser [*adresse_serveur_IP* | *nom_hôte*] avec les paramètres *valeur sous-directive*, n'insérez pas FOR entre *adresse_IP* et *nom_hôte*.

valeur de sous-directive

Si vous voulez inclure les sous-directives de protection dans la directive Protect, utilisez ce paramètre. Pour obtenir des descriptions des sous-directives de protection, voir :

- «AuthType — Spécifie le type d'authentification», à la page 261
- «DeleteMask — Spécifie les noms utilisateur, les groupes et les adresses admises pour la suppression des fichiers», à la page 261
- «GetMask — Spécifie les noms d'utilisateur, les groupes et les adresses admis pour l'extraction des fichiers», à la page 261
- «GroupFile — Spécifie l'emplacement du fichier de groupes associé», à la page 261

- «Mask — Spécifie les noms d'utilisateur, les groupes et les adresses admises pour effectuer des demandes HTTP», à la page 262
- «PasswdFile — Spécifie l'emplacement du fichier de mots de passe associé», à la page 262
- «PostMask — Spécifie les noms utilisateur, les groupes et les adresses admis pour la transmission de fichiers», à la page 262
- «PutMask — Spécifie les noms d'utilisateur, les groupes et les adresse admis pour placer des fichiers», à la page 263
- «ServerID — Spécifie un nom à associer au fichier de mots de passe», à la page 263

Exemples

- Dans l'exemple ci-après, le serveur active la protection de la manière suivante :
 - Les demandes commençant par /secret/scoop/ activent la protection. La configuration de la protection est définie dans le fichier de configuration de protection /server/protect/setup1.acc. Etant donné que la directive Protect ne spécifie aucune configuration de protection, la configuration de protection correspondant à la directive DefProt précédente est utilisée.
 - Les demandes commençant par /secret/business/ activent la protection. La configuration de la protection est définie dans la directive Protection ayant un libellé BUS-PROT.
 - Les demandes commençant par /topsecret/ activent la protection. La configuration de la protection est incluse directement dans la directive Protect.

Ces exemples utilisent les adresses IP. Si votre serveur reçoit des demandes commençant par /secret/ ou /topsecret/, il active une configuration de protection différente en fonction de l'adresse IP de la connexion réseau d'où provient la demande.

- Pour les demandes /secret/ provenant de 0.67.106.79, le serveur active la configuration de protection définie dans une directive Protection avec un libellé CustomerA-PROT. Pour les demandes /topsecret/ provenant de 0.67.106.79, le serveur active la configuration de protection définie en ligne au niveau de la directive Protect pour /topsecret/.
- Pour les demandes /secret/ provenant de 0.83.100.45, le serveur active la configuration de protection définie dans une directive Protection avec un libellé CustomerB-PROT. Pour les demandes /topsecret/ provenant de 0.83.100.45, le serveur active la configuration de protection définie en ligne au niveau de la directive Protect /topsecret/.

```
Protection BUS-PROT {
    UserID    busybody
    GroupID   webgroup
    AuthType   Basic
    ServerID  restricted
    PasswdFile /docs/WWW/restrict.pwd
    GroupFile  /docs/WWW/restrict.grp
    GetMask   authors
    PutMask   authors
}
DefProt /secret/* /server/protect/setup1.acc
Protect /secret/scoop/*
Protect /secret/business/*    BUS-PROT
Protect /topsecret/* {
    AuthType   Basic
    ServerID  restricted
    PasswdFile /docs/WWW/restrict.pwd
    GroupFile  /docs/WWW/restrict.grp
    GetMask   topbrass
}
```

```

    PutMask topbrass
}
Pass /secret/scoop/* /WWW/restricted/*
Pass /secret/business/* /WWW/confidential/*
Pass /topsecret/* /WWW/topsecret/*
Protect /secret/* CustomerA-PROT FOR 0.67.106.79
Protect /secret/* CustomerB-PROT FOR 0.83.100.45
Protect /topsecret/* 0.67.106.79 {
    AuthType Basic
    ServerID restricted
    PasswdFile /docs/WWW/customer-A.pwd
    GroupFile /docs/WWW/customer-A.grp
    GetMask A-brass
    PutMask A-brass
}
Protect /topsecret/* 0.83.100.45 {
    AuthType Basic
    ServerID restricted
    PasswdFile /docs/WWW/customer-B.pwd
    GroupFile /docs/WWW/customer-B.grp
    GetMask B-brass
    PutMask B-brass
}

```

- Les exemples suivants utilisent des hôtes virtuels. Si votre serveur reçoit des demandes qui commencent par /secret/ ou /topsecret/, il active une configuration de protection différente pour la demande en fonction du nom d'hôte dans l'URL.
 - Pour les demandes /secret/ destinées à hôteA.bcd.com, le serveur active la configuration de la protection définie dans une directive Protection avec un libellé CustomerA-PROT. Pour les demandes /topsecret/ destinées à hôteA.bcd.com, le serveur active la configuration de la protection définie en ligne au niveau de la directive Protect pour /topsecret/.
 - Pour les demandes /secret/ destinées à hôteB.bcd.com, le serveur active la configuration de la protection définie au niveau d'une directive Protection avec un libellé CustomerB-PROT. Pour les demandes /topsecret/ destinées à hôteB.bcd.com, le serveur active la configuration de la protection définie en ligne au niveau de la directive Protect pour /topsecret/.
 - Pour les demandes traitées par des serveurs proxy, le serveur active la configuration de la protection au niveau d'une directive Protection avec un libellé proxy-prot. Par exemple :

```

Protect http://host1/* proxy-prot
Protect /secret/* CustomerA-PROT FOR hôteA.bcd.com
Protect /secret/* CustomerB-PROT FOR hôteB.bcd.com
Protect /topsecret/* hostA.bcd.com {
    AuthType Basic
    ServerID restricted
    PasswdFile /docs/WWW/customer-A.pwd
    GroupFile /docs/WWW/customer-A.grp
    GetMask A-brass
    PutMask A-brass
}
Protect /topsecret/* hostB.bcd.com {
    AuthType Basic
    ServerID restricted
    PasswdFile /docs/WWW/customer-B.pwd
    GroupFile /docs/WWW/customer-B.grp
    GetMask B-brass
    PutMask B-brass
}

```

Valeur par défaut

Par défaut, la protection est fournie pour les formulaires de configuration et d'administration par une directive Protect avec un modèle de demande /admin-bin/*.

Protection — Définit une configuration de protection nommée dans le fichier de configuration

Cette directive permet de définir une configuration de protection dans le fichier de configuration. Vous donnez à la configuration de protection un nom et définissez le type de la protection à l'aide des sous-directives de protection.

Remarques :

1. Dans le fichier de configuration, vous devez placer les directives Protection avant les directives DefProt ou Protect les désignant.
2. Pour utiliser des noms de domaine dans les règles de protection, vous devez attribuer la valeur on à la directive DNS-Lookup.

Format

```
Protection nom_libellé {  
    sous-directive valeur  
    sous-directive valeur  
    .  
    .  
    .  
}
```

nom_libellé

Indique le nom à associer à la configuration de protection. Le nom peut ensuite être utilisé par les directives DefProt et Protect suivantes pour désigner la configuration de la protection.

valeur de sous-directive

Les sous-directives sont placées entre accolades ({}). L'accolade de gauche doit être le dernier caractère sur la même ligne que la directive *nom_libellé*. Chaque sous-directive suit sur sa propre ligne. L'accolade de droite doit être sur sa propre ligne suivant la dernière ligne de sous-directive. Vous ne pouvez pas placer de lignes de commentaire entre les accolades.

Pour obtenir des descriptions détaillées des sous-directives de protection, voir «Sous-directives de protection — Spécifie le mode de protection d'un ensemble de ressources», à la page 261.

Exemple

```
Protection NAME-ME {  
    AuthType      Basic  
    ServerID      restricted  
    PasswdFile    /WWW/password.pwd  
    GroupFile     /WWW/group.grp  
    GetMask       groupname  
    PutMask       groupname  
}
```

Valeur par défaut

```
Protect /admin-bin/* {  
    ServerId      Private_Authorization  
    AuthType      Basic  
    GetMask       A11@(*)  
    PutMask       A11@(*)
```

```

PostMask    All@(*)
Mask        All@(*)
PasswdFile  /opt/ibm/edge/cp/server_root/protect/webadmin.passwd
}

```

Sous-directives de protection — Spécifie le mode de protection d'un ensemble de ressources

Ci-dessous se trouvent des descriptions de chaque sous-directive de protection pouvant être utilisées dans une configuration de protection. Les sous-directives sont classées par ordre alphabétique.

Les configurations de protection peuvent se trouver soit dans des fichiers séparés soit dans les fichiers de configurations comme parties des directives DefProt, Protect ou Protection.

AuthType — Spécifie le type d'authentification

Cette sous-directive de protection permet de limiter l'accès en fonction des noms utilisateur et des mots de passe. Spécifiez le type d'authentification à utiliser lorsque le client envoie un mot de passe au serveur. Avec l'authentification de base (AuthType Basic), les mots de passe sont envoyés au serveur sous la forme de texte. Ils sont codés, mais non chiffrés.

Valeur par défaut :

AuthType Basic

DeleteMask — Spécifie les noms utilisateur, les groupes et les adresses admises pour la suppression des fichiers

Cette sous-directive de protection permet de spécifier des modèles de noms utilisateur, de groupes, d'adresses admis pour effectuer des demandes DELETE au niveau d'un répertoire protégé.

Exemple :

DeleteMask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*

GetMask — Spécifie les noms d'utilisateur, les groupes et les adresses admis pour l'extraction des fichiers

Cette sous-directive de protection permet de spécifier des modèles de noms utilisateur, de groupes, d'adresses admis pour effectuer des demandes GET au niveau d'un répertoire protégé.

Exemple :

GetMask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*

Valeur par défaut :

GetMask All@(*)

GroupFile — Spécifie l'emplacement du fichier de groupes associé

Cette sous-directive Protection permet de spécifier le nom et le chemin du fichier du groupe de serveurs devant être utilisé par la configuration de protection. Les groupes définis dans ce fichier de groupes de serveurs peuvent ensuite être utilisés par :

- toute directive de masque faisant partie de la configuration de protection. (Les sous-directives de masque sont DeleteMask, GetMask, Mask, PostMask et PutMask.)

- tout fichier ACL se trouvant sur un répertoire protégé par la configuration de protection.

Exemple :

GroupFile /docs/etc/WWW/restrict.group

Mask — Spécifie les noms d'utilisateur, les groupes et les adresses admises pour effectuer des demandes HTTP

Cette sous-directive permet de spécifier des modèles de noms d'utilisateur, de groupes et d'adresses admis pour effectuer des demandes HTTP non prises en charge par d'autres sous-directives de masque.

Exemples :

Mask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*

Remarque : Lorsque vous utilisez la directive Mask, vous devez garder à l'esprit que la différenciation entre les majuscules et les minuscules est effectuée. Voici un exemple d'une protection Mask pour un ID utilisateur :

MASK WEBADM,webadm

PasswdFile — Spécifie l'emplacement du fichier de mots de passe associé

Cette sous-directive de protection permet de limiter l'accès en fonction des noms utilisateur et des mots de passe. Spécifiez le nom et le chemin du fichier de mots de passe devant être utilisé par cette configuration de protection.

Etant donné que certains navigateurs mettent en mémoire cache les ID utilisateur et les mots de passe par domaine de sécurité (ID utilisateur) dans l'hôte, suivez les instructions ci-dessous lors de la spécification des ID serveur et des fichiers de mots de passe :

- Les configurations de protection qui utilisent le même fichier de mots de passe doivent utiliser le même ID serveur.
- Les configurations de protection qui utilisent différents fichiers de mots de passe doivent utiliser des ID serveur différents.

Exemple :

PasswdFile /docs/etc/WWW/restrict.password

Remarque : Si le nom ou le chemin du fichier des mots de passe contient des espaces, cet ensemble d'informations doit être placé entre guillemets ("").

PasswdFile "c:\test this\admin.pwd"

PostMask — Spécifie les noms utilisateur, les groupes et les adresses admis pour la transmission de fichiers

Pour un serveur sécurisé, cette sous-directive de protection permet de spécifier des modèles d'utilisateurs, de groupes et d'adresses admis pour effectuer des demandes POST au niveau d'un répertoire protégé.

Exemple :

PostMask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*

PutMask — Spécifie les noms d'utilisateur, les groupes et les adresse admis pour placer des fichiers

Cette sous-directive de protection permet de spécifier des modèles d'utilisateurs, de groupes, d'adresses admis pour effectuer des demandes PUT au niveau d'un répertoire protégé.

Exemple :

```
PutMask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*
```

ServerID — Spécifie un nom à associer au fichier de mots de passe

Cette sous-directive de protection permet de limiter l'accès en fonction des noms utilisateur et des mots de passe. Spécifiez un nom à associer au fichier de mots de passe en cours d'utilisation. Il n'est pas nécessaire que le nom soit un nom de machine réel.

Le nom est utilisé comme identificateur de l'élément à l'origine de la demande. Etant donné que plusieurs configurations de protection peuvent utiliser différents fichiers de mots de passe, l'association d'un nom à une protection de configuration peut aider le client lors du choix du mot de passe à envoyer. La plupart des clients affichent ce nom lorsqu'ils sont invités à entrer un nom utilisateur et un mot de passe.

Etant donné que certains navigateurs mettent en mémoire cache les ID utilisateur et les mots de passe par domaine de sécurité (ID utilisateur) dans l'hôte, suivez les instructions ci-après lors de la spécification des ID serveur et des fichiers de mots de passe :

- Les configurations de protection qui utilisent le même fichier de mots de passe doivent utiliser le même ID serveur.
- Les configurations de protection qui utilisent différents fichiers de mots de passe doivent utiliser des ID serveur différents.

Exemple :

```
ServerID restricted
```

Proxy — Identifie les protocoles de proxy ou le proxy inversé

Cette directive permet d'indiquer les protocoles que Caching Proxy doit traiter et mapper une requête à un serveur. Les protocoles valides sont http, ftp et gopher.

La directive du proxy transmet la requête à un serveur éloigné. Par exemple, avec, la directive suivante, toutes les demandes seront transmises à l'URL désignée :

```
Proxy /* http://nom.serveur.proxy/*
```

Pour un serveur proxy inversé sécurisé, utilisez la directive suivante :

```
Proxy /* https://nom.serveur.proxy/*
```

Si vous voulez que les restrictions relatives à votre serveur proxy soient moindres, supprimez les commentaires des directives ci-dessous dans votre fichier de configuration. Ces directives peuvent cependant introduire un problème de sécurité lorsque le proxy est configuré comme proxy inversé.

```
Proxy http:*  
Proxy ftp:*  
Proxy gopher:*
```

Paramètres facultatifs :

- **UseSession**
S'applique aux configurations avec proxy inversé uniquement.
Cette option demande à Caching Proxy de conserver un mappage un à un entre le socket côté client et le socket sortant. Cette option est utile pour certaines applications, comme l'authentification basée sur connexion, qui exige que le proxy conserve le socket côté client actif et qu'il réutilise le socket pour les demandes provenant du même socket côté client.
- **NoCaching**
En cas de correspondance avec la règle du proxy, cette option demande au proxy de ne pas mettre en cache les réponses correspondantes.
- **NoCacheOnRange**
En cas de correspondance avec la règle du proxy et de présence d'en-tête Range dans la demande, cette option demande au proxy de ne pas mettre en cache la réponse correspondante. Pour plus d'informations, voir «NoCacheOnRange — Indique la non mise en cache pour les demandes Range», à la page 246.
- **NoJunction**
S'applique aux configurations avec proxy inversé uniquement.
Utilisez cette option si le plug-in de réécriture de la jonction est activé. Cette option ne permet pas au proxy de réécrire les réponses correspondantes en cas de correspondance de l'URL entrante. Pour plus d'informations, voir «Activation de la réécriture de jonction (facultatif)», à la page 45 et «Définition de la jonction avec l'option JunctionPrefix (méthode recommandée)», à la page 45.
- **JunctionPrefix**
S'applique aux configurations avec proxy inversé uniquement.
Utilisez cette option si le plug-in de réécriture de la jonction est activé. Vous pouvez déclarer le préfixe de jonction dans la règle Proxy en utilisant le format ci-dessous au lieu de déduire le préfixe de jonction en fonction du premier modèle d'URL. Pour plus d'informations, voir «Activation de la réécriture de jonction (facultatif)», à la page 45 et «Définition de la jonction avec l'option JunctionPrefix (méthode recommandée)», à la page 45.

Format

Proxy *modèle demande chemin_serveur_cible* *[[ip]:port]*
[UseSession | NoCaching | NoCacheOnRange | NoJunction | JunctionPrefix:*préfixe_url*]

Exemple

Voici un exemple d'option UseSession pour la directive Proxy :

```
Proxy /abc/* http://server1/default/abc/* :80 UseSession
```

Lorsque la requête client entrante provient du port 80 et que l'URL associée correspond au modèle /abc/*, l'URL est mappée à http://server1/default/abc/*.

Valeurs par défaut

Aucun.

ProxyAccessLog — Indique le nom du chemin du fichier journal des accès au serveur proxy

Cette directive permet de spécifier le chemin et le nom du fichier dans lequel le serveur doit consigner les statistiques d'accès au serveur proxy. Par défaut, le serveur inscrit une entrée dans ce fichier journal dès qu'il se comporte en tant que proxy pour une demande client. Vous pouvez utiliser la directive NoLog si vous ne voulez pas consigner de demandes provenant de certains clients.

Le serveur démarre un nouveau fichier journal chaque jour à minuit s'il est en cours d'exécution. Sinon, le serveur démarre un nouveau fichier journal dès que vous le démarrez. Lors de la création du fichier, le serveur utilise le nom du fichier spécifié et ajoute un suffixe de date ou une extension. Le suffixe de date ou l'extension apparaît au format *Mmmjjaaaa*, où *Mmm* correspond aux trois premières lettres du mois, *jj* au jour du mois et *aaaa* à l'année.

Nous vous recommandons de supprimer les anciens fichiers journaux car ils peuvent occuper un espace disque important sur votre disque dur.

Format

ProxyAccessLog
chemin/fichier

Valeurs par défaut

- **Systèmes Linux et UNIX** : *ProxyAccessLog /opt/ibm/edge/cp/racine_serveur/logs/proxy*
- **Systèmes Windows** : *ProxyAccessLog unité:\Program Files\IBM\edge\cp\logs\proxy*

ProxyAdvisor — Personnalise le service des demandes de proxy

Cette directive permet de spécifier une application personnalisée devant être appelée par le serveur lors de la phase Proxy Advisor. Ce code doit servir la demande.

Format

ProxyAdvisor /chemin/fichier:nom_fonction

/chemin/fichier

Indique le nom complet du fichier du programme compilé.

nom_fonction

Indique le nom de la fonction d'application au sein de votre programme.

Exemple :

ProxyAdvisor /api/bin/customadvise.so:proxyadv

Valeur par défaut

Aucun

ProxyForwardLabels — Spécifie un filtrage PICS

La directive *ProxyForwardLabels* permet d'effectuer un filtrage PICS au niveau du serveur proxy, du client ou au niveau de deux proxys de la hiérarchie de proxys.

Si *ProxyForwardLabels* a la valeur *On*, le serveur proxy génère des en-têtes HTTP *PICS-Label* : pour tous les libellés PICS trouvés, y compris les libellés provenant du serveur d'origine, des bureaux de libellés, de la mémoire cache des libellés de Caching Proxy et des plug-ins du fournisseur de libellés.

Si *ProxyForwardLabels* a la valeur *Off*, les en-têtes HTTP *PICS-Label* : ne sont pas générés.

Format

ProxyForwardLabels {on | off}

Valeur par défaut

ProxyForwardLabels Off

ProxyFrom — Spécifie un client avec un en-tête "From:"

Cette directive permet de générer un en-tête "From:". Elle est généralement utilisée pour donner une adresse électronique de l'administrateur proxy.

Format

ProxyFrom
adresse_électronique

Exemple

Le paramètre ProxyFrom webmaster@proxy.ibm.com provoque les modifications d'en-tête suivantes :

En-tête d'origine

Location: http://www.ibm.com/
Last Modified: Tue 5 Nov 1997 10:05:39
GMT
Pragma: no-cache

En-tête modifié

Location: http://www.ibm.com/
Last Modified: Tue 5 Nov 1997 10:05:39
GMT
From: webmaster@proxy.ibm.com
Pragma: no-cache

Valeur par défaut

Aucun

ProxyIgnoreNoCache — Ignore les demandes de rechargement

Cette directive permet d'indiquer comment le serveur doit réagir lorsque l'utilisateur clique sur le bouton **Recharger** dans le navigateur. Si la valeur On est attribuée à ProxyIgnoreNoCache, lors des périodes de chargement important, le serveur ne demande pas la page à partir du serveur de destination et fournit la copie mise en mémoire cache du file si cette dernière est disponible. Le serveur ignore l'en-tête Pragma: no-cache envoyé par le navigateur.

Format

ProxyIgnoreNoCache {on | off}

Valeur par défaut

ProxyIgnoreNoCache off

ProxyPersistence — Autorise les connexions permanentes

Cette directive indique si une connexion permanente est conservée avec le client. Une connexion permanente réduit le temps d'attente pour les utilisateurs et réduit la charge de l'unité centrale sur le serveur proxy, mais nécessite plus de ressources. Pour une connexion permanente, des unités d'exécution supplémentaires sont requises sur le serveur et donc plus de mémoire.

Les connexions permanentes ne doivent pas être utilisées dans une configuration de serveur proxy à plusieurs niveaux si l'un des proxy n'est pas compatible HTTP 1.1.

Format

ProxyPersistence {on | off}

Valeur par défaut

ProxyPersistence on

ProxySendClientAddress — Génère l'en-tête "Client IP Address:"

Cette directive permet d'indiquer si le proxy transmet l'adresse IP du client au serveur de destination.

Format

ProxySendClientAddress {*IP_Client*: | OFF}

Exemple

La directive ProxySendClientAddress *IP_Client*: provoque les modifications d'en-tête suivantes :

En-tête d'origine

Location: http://www.ibm.com/
Last Modified: Tue 5 Nov 1997 10:05:39 GMT
Pragma: no-cache

En-tête modifié

Location: http://www.ibm.com
Last Modified: Tue 5 Nov 1997 10:05:39 GMT
IP_Client: 0.67.199.5
Pragma: no-cache

Valeur par défaut

Aucun

ProxyUserAgent — Modifie la chaîne de l'agent utilisateur

Cette directive permet de spécifier une chaîne Agent utilisateur remplaçant la chaîne envoyée par le client. Ainsi, vous renforcez le caractère anonyme lors de la visite de sites Web. Cependant, certains sites possèdent des pages personnalisées dépendant de la chaîne Agent utilisateur. Le recours à la directive ProxyUserAgent empêche l'affichage de ces pages personnalisées.

Format

ProxyUserAgent
nom_produit/version

Exemple

La directive ProxyUserAgent Caching Proxy/6.1 provoque les modifications d'en-tête suivantes :

En-tête d'origine

Location: http://www.ibm.com/
Last Modified: Tue 5 Nov 1997 10:05:39 GMT
Agent utilisateur : Mozilla/ 2.02 OS2
Pragma: no-cache

En-tête modifié

Location: http://www.ibm.com
Last Modified: Tue 5 Nov 1997 10:05:39 GMT
Agent utilisateur : Caching Proxy/6.1
Pragma: no-cache

Valeur par défaut

Aucun

ProxyVia — Spécifie le format de l'en-tête HTTP

Cette directive permet de gérer le format de l'en-tête HTTP. Elle admet quatre valeurs. Si ProxyVia prend la valeur Full, Caching Proxy ajoute un en-tête Via dans la demande ou la réponse. Si un en-tête Via est déjà dans le flux, Caching

Proxy ajoute les informations sur l'hôte à la fin. Si elle prend la valeur Set, Caching Proxy attribue les informations sur l'hôte à l'en-tête Via ; si un en-tête Via se trouve déjà dans le flux, Caching Proxy le supprime. Si la directive prend la valeur Pass, Caching Proxy transmet toutes les informations de l'en-tête telles quelles. Si elle prend la valeur Block, Caching Proxy ne transmet aucun en-tête Via.

Format

ProxyVia {Full | Set | Pass | Block}

Exemple

ProxyVia Pass

Valeur par défaut

ProxyVia Full

ProxyWAS — Spécifie que les demandes sont envoyées à WebSphere Application Server

S'applique aux configurations avec proxy inversé uniquement.

La directive de mappage ProxyWAS fonctionne de la même façon que la directive Proxy mais indique aussi à Caching Proxy que les demandes correspondantes sont dirigées vers un serveur WebSphere Application Server. Pour afficher des exemples d'utilisation de cette directive, voir «Proxy — Identifie les protocoles de proxy ou le proxy inversé», à la page 263.

Format

ProxyWAS *modèle_demande chemin_serveur_cible* [[*ip*]:*port*]
[UseSession | NoCaching | NoCacheOnRange | NoJunction | JunctionPrefix:*préfixe_url*]

Valeur par défaut

Aucun

PureProxy — Désactive un proxy dédié

Cette directive permet de spécifier si le serveur se comporte comme un proxy ou comme un serveur proxy et de contenu. Nous vous recommandons d'utiliser Caching Proxy en tant que proxy uniquement.

Format

PureProxy {on | off}

Valeur par défaut

PureProxy on

PurgeAge — Spécifie la limite d'âge pour un journal

Cette directive permet de spécifier l'âge limite d'un journal, en jours, avant qu'il ne soit purgé. Si PurgeAge a la valeur 0, le fichier journal n'est jamais supprimé.

Remarque : Le plug-in ne supprime jamais le fichier journal du jour en cours ou du jour précédent.

Format

PurgeAge *nombre*

Valeur par défaut

PurgeAge 7

Directives connexes

- «CompressAge — Indique à quel moment compresser les fichiers journaux», à la page 200
- «CompressDeleteAge — Indique à quel moment supprimer les journaux», à la page 201
- «CompressCommand — Spécifie la commande et les paramètres de compression», à la page 200
- «Midnight — Identifie le plug-in API permettant d'archiver les fichiers journaux», à la page 243
- «LogArchive — Définit le comportement de la fonction d'archivage du journal», à la page 234
- «PurgeSize — Spécifie la taille limite d'un fichier journal d'archivage»

PurgeSize — Spécifie la taille limite d'un fichier journal d'archivage

Cette directive d'indiquer la taille (en mégaoctets) pouvant être atteinte par les fichiers journaux d'archivage avant que ces derniers ne soient purgés. Si `PurgeSize` a la valeur 0, il n'y a pas de taille limite et les fichiers ne sont jamais supprimés.

Le paramètre défini pour `PurgeSize` s'applique à *tous* les journaux d'un type donné. Par exemple, si vous consignez les erreurs (une entrée `Errorlog` est présente dans le fichier de configuration) et si la valeur 10 Mo est attribuée à `PurgeSize`, `Caching Proxy` calcule la taille de tous les journaux d'erreur, additionne ces tailles, puis supprime les journaux jusqu'à ce que la taille totale soit inférieure à 10 Mo.

Remarque : Le plug-in ne supprime jamais le fichier journal du jour en cours ou du jour précédent. Lorsque vous purgez des fichiers journaux, les fichiers les plus anciens sont les premiers à être supprimés jusqu'à ce que la taille totale des fichiers journaux de chaque type soit inférieure ou égale à la valeur définie par la directive `PurgeSize` (en mégaoctets).

Format

`PurgeSize nombre_de_Mo`

Valeur par défaut

`PurgeSize 0`

Directives connexes

- «CompressAge — Indique à quel moment compresser les fichiers journaux», à la page 200
- «CompressDeleteAge — Indique à quel moment supprimer les journaux», à la page 201
- «CompressCommand — Spécifie la commande et les paramètres de compression», à la page 200
- «LogArchive — Définit le comportement de la fonction d'archivage du journal», à la page 234
- «Midnight — Identifie le plug-in API permettant d'archiver les fichiers journaux», à la page 243
- «PurgeAge — Spécifie la limite d'âge pour un journal», à la page 268

RCAConfigFile — Spécifie un alias pour ConfigFile

Cette directive permet de spécifier le nom et l'emplacement du fichier de configuration RCA (Remote Cache Access).

Remarque : Le fichier de configuration RCA a été fusionné dans le fichier `ibmproxy.conf`. Pour une compatibilité amont, la directive `RCAConfigFile` est prise en charge en tant qu'alias de `ConfigFile`.

Format

`RCAConfigFile /etc/nom_fichier`

Exemple

`RCAConfigFile /etc/user2rca.conf`

Valeur par défaut

`RCAConfigFile /etc/rca.conf`

RCAThreads — Spécifie le nombre d'unités d'exécution par port

Cette directive permet de spécifier le nombre d'unités d'exécution en cours sur un port RCA.

Format

`RCAThreads nombre_unités_exécution`

Exemple

`RCAThreads 50`

Valeur par défaut

`MaxActiveThreads x [(ArraySize -1) / (2 x ArraySize -1)]`

ReadTimeout — Spécifie la durée limite pour une connexion

Cette directive permet de spécifier la durée maximale admise sans activité réseau avant l'annulation de la connexion.

Format

`ReadTimeout durée`

Valeur par défaut

`ReadTimeout 5 minutes`

Redirect — Spécifie un modèle pour les demandes adressées à un autre serveur

Cette directive permet de spécifier un modèle pour les demandes à accepter et à envoyer à d'autres serveurs. Lorsqu'une demande correspond à un modèle de directive `Redirect`, celle-ci n'est pas comparée aux modèles des autres directives du fichier de configuration.

Format

`Redirect modèle_demande URL
[adresse_serveur_IP | nom_hôte]`

modèle_demande

Spécifie un modèle pour les demandes devant être envoyées à un autre serveur.

Vous pouvez utiliser un astérisque (*) en tant que caractère générique dans le modèle. Le caractère tilde (~) placé juste après une barre oblique (/) doit être indiqué explicitement. Vous ne pouvez pas utiliser de caractère générique.

URL

Spécifie la demande d'URL que le serveur envoie à un autre serveur. La réponse à cette demande est envoyée au demandeur d'origine sans indication précisant qu'elle provient de votre serveur.

URL doit contenir une spécification de protocole et le nom du serveur auquel envoyer la demande. Il peut également contenir un chemin ou un nom de fichier. Si *modèle-demande* utilise un caractère générique, un caractère générique peut également être utilisé pour le chemin ou le nom de fichier au niveau de l'URL. La partie de la demande d'origine qui correspond au caractère générique de l'élément *modèle-demande* est insérée à la place du caractère générique de l'URL.

[*adresse_serveur_IP* | *nom_hôte*]

Si vous utilisez plusieurs adresses IP ou noms d'hôte, utilisez ce paramètre pour spécifier une adresse IP ou un nom d'hôte. Le serveur utilise la directive uniquement pour les demandes arrivant sur le serveur à cette adresse IP ou pour cet hôte. Pour une adresse IP, il s'agit de l'adresse de la connexion réseau du serveur et non de l'adresse du client à l'origine de la demande.

Vous pouvez spécifier une adresse IP (par exemple, 240.146.167.72) ou un nom d'hôte (par exemple, hostA.bcd.com).

Ce paramètre est facultatif. Sans ce paramètre, le serveur utilise la directive pour toutes les demandes quel que soit le nom d'hôte de l'URL ou l'adresse IP d'où elles proviennent.

Il n'est pas possible d'indiquer de caractère générique pour une adresse IP de serveur.

Exemples

- Dans cet exemple, le serveur envoie les demandes commençant par /chef/truc/ au répertoire wahoo du serveur www.autre.org.

```
Redirect /chef/truc/* http://www.autre.org/wahoo/*
```

- Les exemples suivants utilisent le paramètre d'adresse IP facultatif. Si le serveur reçoit des demandes commençant par /truc/, il redirige la demande vers différents serveurs, en fonction de l'adresse IP de la connexion réseau d'où est issue la demande. Pour les demandes provenant de 240.146.167.72, le serveur envoie la demande au répertoire wahoo du serveur www.chief.org. Pour les demandes provenant de toute connexion ayant une adresse de 0.83.100.45, le serveur envoie la demande au répertoire pound du serveur www.dawg.com.

```
Redirect /truc/*  
http://www.chief.org/wahoo/*  
240.146.167.72 Redirect /truc/* http://www.dawg.com/pound/*  
0.83.100.45
```

- Les exemples suivants utilisent le paramètre d'adresse IP facultatif. Si votre serveur reçoit des demandes commençant par /truc/, il les réachemine les demandes vers des serveurs différents en fonction du nom d'hôte dans l'URL. Pour les demandes destinées à hôteA, le serveur envoie la demande au répertoire wahoo du répertoire www.chef.org. Pour les demandes destinées à hôteB, le serveur envoie la demande au répertoire pound du serveur www.dawg.com.

```
Redirect /truc/* http://www.chief.org/wahoo/* hôteA.bcd.com  
Redirect /truc/* http://www.dawg.com/pound/* hôteB.bcd.com
```

Valeur par défaut

Aucun

RegisterCacheIdTransformer — Met en cache plusieurs variantes d'une ressource sur la base de l'en-tête Cookie

Cette directive autorise Caching Proxy à mettre en cache plusieurs variantes d'une ressource (URI) sur la base de l'en-tête Cookie.

Remarque : Si les cookies sont désactivés dans les navigateurs client, les clients peuvent accéder au même objet mis en cache.

Pour plus d'informations, voir «SupportVaryHeader — Met en cache plusieurs variantes d'une ressource sur la base de l'en-tête HTTP Vary», à la page 286.

Format

RegisterCacheIdTransformer Cookie *nom-cookie*

La variable *nom-cookie* correspond au nom indiqué dans l'en-tête Cookie de la demande client.

Exemple

RegisterCacheIdTransformer Cookie Usergroup

Pour obtenir un exemple d'utilisation de cette directive en association avec SupportVaryHeader, voir «SupportVaryHeader — Met en cache plusieurs variantes d'une ressource sur la base de l'en-tête HTTP Vary», à la page 286.

Valeur par défaut

Aucun

ReversePass — Intercepte automatiquement les demandes redirigées

S'applique aux configurations avec proxy inversé uniquement.

La directive de mappage ReversePass examine le flux du serveur pour détecter les demandes qui sont réécrites suite à un réacheminement automatique. En général, lorsqu'un serveur renvoie un code HTTP de la classe 3xx (par exemple, 301, moved permanently, ou 303, see other), le serveur envoie un message contenant la réponse, qui indique au client demandeur de diriger ses demandes futures vers l'URL ou l'adresse IP adéquate. Dans le cas d'une configuration de proxy inversé, un message de réacheminement issu du serveur d'origine peut amener les navigateurs clients à contourner le serveur proxy pour les demandes suivantes. Pour éviter que les clients ne contactent directement le serveur d'origine, utilisez la directive ReversePass pour intercepter les demandes destinées spécialement au serveur d'origine.

A la différence d'autres directives de mappage qui traitent le flux de demandes, ReversePass compare son modèle au flux de réponses. Le flux de réponses désigne la réponse que le serveur proxy reçoit du serveur origine et qu'il transmet au client.

Format

ReversePass *URL_modifiée* *URL_proxy* [*hôte:port*]

L'option *hôte:port* permet au proxy d'appliquer une règle ReversePass différente en fonction du nom d'hôte et du port du serveur dorsal.

Exemples

- L'exemple suivant empêche l'acheminement des demandes vers le serveur d'origine :

```
ReversePass http://backend.company.com:9080/* http://edge.company.com/*
```

Le port 9080 est le port par défaut de Application Service at the Edge. Ce type de demande peut être généré si le serveur d'applications d'origine a renvoyé un code 3xx au client.

- L'exemple suivant intercepte les demandes qui ont été réacheminées par un code 301 à partir de Edge Server.

```
ReversePass http://edge.company.com:9080/*  
http://edge.company.com/*
```

Remarque : Le contenu du modèle *URL_proxy*, jusqu'au caractère générique (*), doit correspondre exactement à la valeur envoyée par le serveur dorsal dans l'en-tête de l'emplacement ; sinon, la directive échoue.

Valeur par défaut

Aucun

RewriteSetCookieDomain — Définition du modèle de domaine à remplacer

S'applique aux configurations avec proxy inversé uniquement.

Cette directive permet d'indiquer le modèle de domaine à remplacer. La directive remplace le domaine *modèle1_domaine* par *modèle2_domaine*.

Format

```
RewriteSetCookieDomain modèle1_domaine modèle2_domaine
```

Exemple

```
RewriteSetCookieDomain .internal.com .external.com
```

Valeur par défaut

Aucun

Directives connexes

- «JunctionRewriteSetCookiePath — Réécriture de l'option dans l'en-tête Set-Cookie lors d'une utilisation avec le plug-in JunctionRewrite», à la page 230

RTSPEnable — Active le réacheminement RTSP

S'applique aux configurations avec proxy inversé uniquement.

Cette directive permet d'activer ou de désactiver le réacheminement RTSP. les valeurs admises sont on ou off.

Format

```
RTSPEnable {on | off}
```

Exemple

```
RTSPEnable on
```

Valeur par défaut

Aucun

rtsp_proxy_server - Spécifie les serveurs de réacheminement

S'applique aux configurations avec proxy inversé uniquement.

Cette directive permet d'indiquer les serveurs proxy RTSP devant recevoir les requêtes réacheminées. Plusieurs serveurs peuvent être indiqués pour différents types de flux de données. Le format de la directive est :

`rtsp_proxy_server adresse dns serveur[:port] rang par défaut [liste de types mime]`

Exemple

<code>rtsp_proxy_server</code>	<code>rproxy.mycompany.com:554</code>	<code>1</code>
<code>rtsp_proxy_server</code>	<code>fw1.mycompany.com:554</code>	<code>2</code>
<code>rtsp_proxy_server</code>	<code>fw1.mycompany.com:555</code>	<code>3</code>
<code>rtsp_proxy_server</code>	<code>fw2.mycompany.com:557</code>	<code>4</code>

Valeur par défaut

Aucun

rtsp_proxy_threshold — Spécifie le nombre de demandes avant réacheminement vers une mémoire cache

S'applique aux configurations avec proxy inversé uniquement.

Cette directive indique le nombre de requêtes devant être reçues avant qu'une requête RTSP soit réacheminée vers un serveur proxy plutôt que vers un serveur d'origine. Les serveurs proxy RealNetworks stockent en mémoire cache les flux de données dès la première demande ; cette méthode de mise en mémoire cache double la largeur de bande utilisée pour la réception d'un flux de données. La définition d'une valeur de seuil supérieure à 1 empêche la mise en mémoire cache des requêtes émises une seule fois. Le format de la directive est :

`rtsp_proxy_threshold nombre d'occurrences`

Exemple

`rtsp_proxy_threshold 5`

Valeur par défaut

Aucun

rtsp_url_list_size — Spécifie le nombre d'URL en mémoire de proxy

S'applique aux configurations avec proxy inversé uniquement.

Cette directive indique le nombre d'URL uniques conservées en mémoire en vue d'un réacheminement. Le proxy consulte cette liste pour déterminer si une URL donnée a déjà été rencontrée. Quand la liste est plus longue, le serveur proxy est mieux à même d'envoyer au même proxy une demande identique à celle qu'il a déjà reçue ; il faut toutefois savoir que chaque entrée de liste consomme environ 16 octets de mémoire.

Format

`rtsp_url_list_size taille de la liste`

Exemple

`rtsp_url_list_size 8192`

Valeur par défaut

Aucun

RuleCaseSense— Mappe les demandes à partir d'URL d'applications ne faisant pas la distinction entre les minuscules et les majuscules

Par défaut, lorsque Caching Proxy mappe des demandes par rapport à des règles définies dans le fichier `ibmproxy.conf`, le processus de correspondance fait la distinction entre les majuscules et les minuscules. Toutefois, certaines URL d'application ne font pas la distinction entre les majuscules et les minuscules. Pour gérer correctement ces demandes, la directive `RuleCaseSense` est fournie./// Lorsque la directive est définie sur `off`, le proxy fait correspondre des demandes sans distinction des majuscules/minuscules.

Remarque : Il s'agit d'une directive globale qui s'applique à toutes les règles de mappage définies.

Format

`RuleCaseSense {on | off}`

Valeur par défaut

`RuleCaseSense on`

ScriptTimeout – Spécifie le paramètre de délai pour les scripts

Cette directive permet de définir le temps alloué pour l'exécution d'un programme CGI démarré par le serveur. Lorsque le délai d'expiration est dépassé, le serveur met fin au programme. Sous Linux et UNIX, cette opération est effectuée par le signal KILL.

Entrez la durée en combinant des heures, des minutes (mn) ou des secondes (s).

Format

`ScriptTimeout délai`

Valeur par défaut

`ScriptTimeout 5 minutes`

SendHTTP10Outbound — Spécifie la version du protocole pour les demandes traitées par un proxy

Cette directive permet de spécifier que les demandes envoyées à partir de Caching Proxy vers un serveur aval doivent utiliser le protocole HTTP version 1.0. (Un serveur *aval* est un autre serveur proxy dans une chaîne de proxys ou un serveur d'origine qui va traiter la demande.)

Si cette directive est utilisée, Caching Proxy spécifie HTTP 1.0 comme protocole dans la ligne de la demande. Seules les fonctionnalités propres à HTTP 1.0 et certaines fonctions HTTP 1.1, telles que les en-têtes `cache-control` pris en charge par la plupart des serveurs HTTP 1.0, seront envoyées au serveur en aval. Cette directive doit être utilisée si un serveur aval ne traite pas correctement les demandes HTTP 1.1.

Si la directive `SendHTTP10Outbound` *n'est pas* spécifiée, Caching Proxy spécifie HTTP 1.1 comme protocole dans la ligne de la demande. Les fonctionnalités HTTP 1.1 telles que les connexions permanentes peuvent également être utilisées dans la demande.

Format

`SendHTTP10Outbound modèle_url`

Exemples

Cette directive peut être spécifiée plusieurs fois, par exemple :

```
SendHTTP10Outbound http://www.hôtea.com/*
```

```
SendHTTP10Outbound http://www.hôteb.com/*
```

Pour assurer la compatibilité amont, la syntaxe précédente de `SendHTTP10Outbound` est traitée comme suit :

- `SendHTTP10Outbound on` est traitée comme si `SendHTTP10Outbound *` était spécifié.
- `SendHTTP10Outbound off` est ignoré.

Remarque : Si `SendHTTP10Outbound off` et `SendHTTP10Outbound url_pattern` sont spécifiés, `SendHTTP10Outbound off` sera ignoré, mais un message d'avertissement sera émis.

Valeur par défaut

Aucun

SendRevProxyName — Spécifie le nom d'hôte de Caching Proxy dans l'en-tête HOST

S'applique aux configurations avec proxy inversé uniquement.

Lorsqu'il fonctionne en proxy inversé, Caching Proxy reçoit les demandes HTTP d'un client et envoie les demandes vers le serveur d'origine. Par défaut, Caching Proxy écrit le nom d'hôte du serveur d'origine dans l'en-tête HOST de la demande qu'il envoie au serveur d'origine. Si la directive `SendRevProxyName` a la valeur `yes`, Caching Proxy écrit son propre nom d'hôte dans l'en-tête HOST. Cette directive permet d'apporter une configuration spéciale au serveurs dorsaux, car la demande adressée au serveur d'origine semble toujours provenir du serveur proxy, même si elle est réacheminée d'un serveur dorsal à un autre.

Cette directive diffère de la directive de mappage `ReversePass` comme suit : La directive `ReversePass` intercepte les demandes avec une syntaxe définie et remplace différents contenus de demandes que vous spécifiez. La directive `SendRevProxyName` peut être définie uniquement pour remplacer le nom d'hôte de Caching Proxy par le nom d'hôte du serveur d'origine. Cette directive n'est pas utile pour la configuration de Application Service at the Edge.

Format

`SendRevProxyName {yes | no}`

ServerConnGCRun — Spécifie l'intervalle d'exécution de l'unité d'exécution du processus de récupération de place

Cette directive définit la fréquence à laquelle l'unité d'exécution du processus de récupération de place vérifie les connexions du serveur ayant expiré (définie avec la directive `ServerConnTimeout`). N'utilisez cette directive que si la valeur `on` est attribuée à la directive `ServerConnPool`.

Format

`ServerConnGCRun` *intervalle de temps*

Exemple

`ServerConnGCRun` 2 minutes

Valeur par défaut

`ServerConnGCRun` 2 minutes

ServerConnPool — Spécifie la mise en pool des connexions avec les serveurs d'origine

Cette directive permet au proxy de regrouper ses connexions sortantes vers les serveurs d'origine. L'activation de cette directive (en l'associant à `on`) accroît les performances et tire davantage parti des serveurs d'origine permettant des connexions permanentes. Vous pouvez également spécifier la durée du maintien d'une connexion inutilisée à l'aide de la directive `ServerConnTimeout`.

Remarque : Il est préférable d'activer cette directive dans un environnement contrôlé ; elle pourrait en effet réduire les performances avec un proxy d'acheminement ou si les serveurs d'origine ne sont pas compatibles avec HTTP 1.1.

Format

`ServerConnPool` {`on` | `off`}

Valeur par défaut

`ServerConnPool` `off`

ServerConnTimeout — Spécifie la période d'inactivité maximale

Cette directive permet de limiter la durée admise pour les activités réseau avant l'annulation de la connexion. N'utilisez cette directive que si la valeur `on` est attribuée à la directive `ServerConnPool`.

Format

`ServerConnTimeout` *time-spec*

Exemple

`ServerConnTimeout` 30 seconds

Valeur par défaut

`ServerConnTimeout` 10 seconds

ServerInit — Personnalise l'étape d'initialisation du serveur

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de ses routines d'initialisation. Ce code est exécuté avant la lecture des demandes client et à chaque redémarrage du serveur.

Si vous utilisez les modules `GoServe` au cours des étapes `PreExit` ou `Service`, vous devez appeler le module `gosclone`.

Format

`ServerInit` */chemin/fichier:nom_fonction*
[chaîne_initialisation]

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme.

chaîne_initialisation

Facultatif. Correspond à une chaîne de texte qui est transmise à la fonction de l'application.

Exemple

ServerInit /ics/api/bin/icsext05.so:svr_init

Valeur par défaut

Aucun

ServerRoot — Spécifie le répertoire dans lequel est installé le programme du serveur

Cette directive permet de spécifier le répertoire dans lequel est installé le programme du serveur (répertoire de travail en cours du serveur). Les directives de consignation utilisent ce répertoire en tant que répertoire principal par défaut lorsque des chemins relatifs sont spécifiés.

Sous Windows, le répertoire est précisé au cours de l'installation.

Format

ServerRoot
chemin_répertoire

Valeurs par défaut

- **Systèmes Linux et UNIX** : ServerRoot /opt/ibm/edge/cp/racine_serveur/
- **Systèmes Windows** : C:\Program Files\IBM\edge\cp\bin\

Remarque : Vous pouvez modifier les paramètres par défaut mais cette opération n'a aucune incidence sur la manière dont le serveur traite les demandes.

Remarque : Les règles PASS et EXEC peuvent être indépendantes de ce répertoire.

ServerTerm — Personnalise l'étape d'arrêt du serveur

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de l'étape d'arrêt. Ce code est exécuté lors d'un arrêt ou d'un redémarrage du serveur. Il permet de libérer des ressources allouées par une fonction d'application PreExit.

Format

ServerTerm */chemin/fichier:nom_fonction*

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme.

Exemple

ServerTerm /ics/api/bin/icsext05.so:shut_down

Valeur par défaut

Aucun

Service — Personnalise l'étape Service

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de l'étape Service. Ce code doit gérer la demande du client. Par exemple, il envoie le fichier ou exécute le programme CGI.

Il n'existe pas de paramètre par défaut pour cette directive. Si la demande correspond à une règle Service (fonction d'application indiquée dans une directive Service), mais que la fonction renvoie HTTP_NOACTION, le serveur génère une erreur et la demande échoue.

Format

Service

modèle_demande/chemin/fichier:nom_fonction

[*adresse_IP_serveur* |
nom_hôte]

modèle_demande

Spécifie un modèle pour les demandes qui déterminent ultérieurement si la fonction d'application est appelée. La spécification peut inclure le protocole, le domaine et l'hôte. Elle peut être précédée d'une barre oblique (/) et peut utiliser un astérisque (*) en tant que caractère générique. Par exemple, /front_page.html , http://www.ics.raleigh.ibm.com, /pub*, /* et * sont tous valides.

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme.

[*adresse_IP_serveur* | *nom_hôte*]

Si vous utilisez plusieurs adresses IP ou hôtes virtuels, ce paramètre détermine si la fonction d'application sera appelée uniquement pour les demandes provenant d'une adresse IP spécifique ou d'un hôte spécifique.

Il n'est pas possible d'indiquer de caractère générique pour une adresse IP de serveur.

Exemples

Service /index.html /ics/api/bin/icsext05.so:serve_req

Service /cgi-bin/hexcalc* /ics/api/calculator:HEXcalc*

Remarque : Pour que le chemin complet soit converti, y compris *chaîne_requête*, insérez un astérisque (*) dans *modèle_demande* et *nom_fonction*, comme indiqué dans le second exemple.

Valeur par défaut

Aucun

SignificantURLTerminator — Spécifie un code d'arrêt pour les demandes d'URL

Utilisez cette directive pour indiquer un code d'arrêt pour les demandes d'URL. En cas d'utilisation du code d'arrêt dans une demande, Caching Proxy ne tient compte que des caractères précédant le code d'arrêt lors du traitement de la demande et détermine si le fichier demandé est ou non placé en mémoire cache. Lorsque plusieurs codes d'arrêt sont utilisés, Caching Proxy compare les URL entrantes aux codes d'arrêt dans l'ordre dans lequel elles sont définies dans le fichier `ibmproxy.conf`.

Format

SignificantURLTerminator *chaîne_d'arrêt en cours*

Exemple

SignificantURLTerminator &.

Dans cet exemple, les deux demandes suivantes sont considérées comme identiques.

```
http://www.exampleURL.com/tx.asp?id=0200&. ;x=004;y=001
http://www.exampleURL.com/tx.asp?id=0200&. ;x=127;y=034
```

Valeur par défaut

Aucun

SMTPServer (Windows uniquement)— Configure un serveur SMTP pour la routine sendmail

Cette directive permet de configurer le serveur SMTP qu'utilise la routine interne `sendmail` dans le cadre de Caching Proxy pour Windows. Cette routine nécessite également la définition des directives «WebMasterEMail — Définit une adresse électronique pour la réception des rapports d'un serveur sélectionné», à la page 291 et «WebMasterSocksServer (Windows uniquement)— Configure un serveur socks pour la routine sendmail», à la page 292.

Format

SMTPServer *adresse IP ou nom d'hôte du serveur SMTP*

Exemple

SMTPServer mybox.com

Valeur par défaut

Aucun

SNMP — Active et désactive la prise en charge de SNMP

Cette directive permet d'activer ou de désactiver la prise en charge de SNMP.

Format

SNMP {on | off}

Valeur par défaut

SNMP off

SNMPCommunity — Fournit un mot de passe de sécurité pour SNMP

Cette directive permet de définir le mot de passe entre le sous-agent DPI et l'agent SNMP de Webserver. Le nom de communauté SNMP autorise un utilisateur à visualiser les variables de performances contrôlées par SNMP pour une communauté de serveurs. L'administrateur système définit les variables à l'aide desquelles les serveurs peuvent être visualisés une fois le mot de passe entré. Si vous modifiez le nom de communauté SNMP, modifiez-le également dans le fichier `/etc/snmpd.conf`.

Format

`SNMPCommunity nom`

Valeur par défaut

`SNMPCommunity public`

SSLCaching — Active la mise en mémoire cache pour une demande sécurisée

Cette directive permet de mettre des données en mémoire cache lors d'une demande sécurisée dans le cadre de l'utilisation d'un proxy inversé. Elle configure la mise en mémoire pour toutes les connexions au serveur proxy, qu'il s'agisse de connexions client ou de connexions au serveur de contenu dorsal.

Remarque : Les directives SSL ne sont pas prises en charge sous SUSE Linux.

Format

`SSLCaching {on | off}`

Valeur par défaut

`SSLCaching off`

SSLCertificate — Spécifie les libellés des clés pour les certificats

Utilisez cette directive pour préciser les libellés des clés qui permettent au proxy de déterminer le certificat à envoyer au client lorsque Caching Proxy fonctionne comme un proxy inversé pour les domaines multiples qui proposent leurs propres certificats SSL et pour indiquer au serveur proxy s'il doit ou non récupérer un certificat PKI du client en vue d'authentifier le client.

Avec la directive `SSLCertificate`, Caching Proxy peut effectuer la distinction entre un certificat émis par une autorité de certification ou un certificat d'auto-signature. Toutefois, si vous acceptez tout certificat émis par une autorité de certification (option `ClientAuthRequired`), l'utilisation de cette directive peut permettre à des utilisateurs non autorisés d'accéder au serveur proxy. Lorsque vous utilisez l'option `ClientAuthRequired` sur la directive `SSLCertificate`, vous pouvez utiliser l'option d'expression logique pour déterminer quels utilisateurs autorisés peuvent accéder au canal SSL.

Lorsqu'une expression logique supplémentaire est ajoutée dans la directive `SSLCertificate`, Caching Proxy extrait des valeurs du certificat client et calcule l'expression logique. Si l'expression `///` est satisfaite par les valeurs du certificat client, Caching Proxy accorde au client l'utilisation de la connexion SSL ; sinon, la connexion est arrêtée et fermée.

Format

`SSLCertificate serveurIP/nomhôte LibelléCertificat`
`[NoClientAuth | ClientAuthRequired logic-expression]`

serveurIP/nomhôte

Vous pouvez spécifier une adresse IP (par exemple, 204.146.167.72) ou vous pouvez spécifier un nom d'hôte (par exemple, hôteA.raleigh.ibm.com) pour le serveur vers lequel la demande SSL est acheminée.

LibelléCertificat

Le nom du certificat qui doit être utilisé si l'authentification du client est requise pour les demandes SSL acheminées à l'adresse IP ou au nom d'hôte désigné.

`[NoClientAuth | ClientAuthRequired logic-expression]`

Instructions données au serveur proxy pour qu'il récupère ou non un certificat PKI du client.

L'option d'expression logique est valide uniquement si elle est utilisée avec l'option ClientAuthRequired. Lorsqu'une expression logique supplémentaire est ajoutée dans la directive SSLCertificate, Caching Proxy extrait des valeurs du certificat client et calcule l'expression logique. Si l'expression ///est satisfaite par les valeurs du certificat client, Caching Proxy accorde au client l'utilisation de la connexion SSL ; sinon, la connexion est arrêtée et fermée.

- Le nom de l'attribut de l'expression logique peut avoir les valeurs suivantes : IST, ICN, IOU, IC, IL, IO, IE, ST, CN, OU, C, L, O, E.
 - Le nom de l'attribut est mappé aux zones suivantes du certificat client : IssuerStateOrProvince (IST) IssuerCommonName (ICN) IssuerOrgUnit (IOU) IssuerCountry (IC) IssuerLocality (IL) IssuerOrg (IO) IssuerEmail (IE) StateOrProvince (ST) CommonName (CN) OrgUnit (OU) Country (C) Locality (L) Org (O) Email (E).
- La valeur du nom de l'attribut doit être délimitée par des guillemets.
- Les opérateurs logiques autorisés sont : && (AND), || (OR), ! (NOT), = (EQUAL).

Exemples

```
SSLCertificate www.abc.com ABCCert
SSLCertificate 204.146.167.72 intABCCert
SSLCertificate www.xyz.com XYZCert ClientAuthRequired
SSLCertificate www.xyz.com XYZCert ClientAuthRequired
CN="valid.user.common.name.pattern" && (L="accepted.location.pattern" ||
C!="not.valid.country.pattern")
```

Valeur par défaut

Aucun

SSLCryptoCard — Spécifie la carte de chiffrement installée

S'applique aux configurations avec proxy inversé uniquement.

Cette directive permet d'indiquer au serveur proxy qu'une carte de chiffrement est installée et de quelle carte il s'agit.

Sous AIX, pour prendre en charge la carte IBM 4960 PCI Cryptographic Accelerator Card, voir «PKCS11DefaultCert, PKCS11DriverPath, PKCS11TokenPassword — Prend en charge la carte IBM 4960 PCI Cryptographic Accelerator Card (AIX uniquement)», à la page 252.

Format

SSLCryptoCard {rainbowcs | nciphernfast} {on | off}

Exemple

SSLCryptoCard rainbowcs on

Valeur par défaut

Aucun

SSLEnable — Indique que les demandes sécurisées sont acheminées au port 443

Cette directive permet d'indiquer que Caching Proxy est à l'écoute des demandes sécurisées sur le port 443.

Remarque : Les directives SSL ne sont pas prises en charge sous SUSE Linux.

Format

SSLEnable {on | off}

Valeur par défaut

SSLEnable off

SSLForwardPort — Spécifie le port auquel s'adresser dans le cas de mises à niveau SSL HTTP

Cette directive permet de spécifier le port auquel s'adresser dans le cas de demandes HTTP devant être mises à niveau en demandes HTTPS par Caching Proxy en implémentant le protocole SSL. Spécifiez un port différent du port HTTP principal 80 et du port SSL principal 443.

Format

SSLForwardPort *numéro de port*

Exemple

SSLForwardPort 8888

Valeur par défaut

Aucun

SSLOnly — Désactive les unités d'exécution à l'écoute pour les demandes HTTP

Cette directive permet de désactiver les unités d'exécution à l'écoute pour les demandes HTTP standard (généralement les ports 80 et 8080) lorsque le SSL (généralement le port 443) est activé.

Format

SSLOnly {on | off}

Valeur par défaut

SSLOnly off

SSLPort — Permet d'indiquer un port d'écoute HTTPS autre que celui par défaut

Utilisez cette directive pour indiquer un port d'écoute HTTPS autre que le port par défaut HTTPS (443) d'ibmproxy.

Remarque : ibmproxy prend en charge un port HTTPS pour chaque instance. Par conséquent, la directive ne doit pas être utilisée pour indiquer plusieurs ports HTTPS. Pour utiliser plusieurs ports HTTPS, vous devez lancer plusieurs instances ibmproxy avec différents fichiers `ibmproxy.conf`.

Format

SSLPort *valeur du port*

où *valeur du port* est un nombre entier supérieur à 0. La *valeur du port* doit être admise par le système d'exploitation et ne doit pas être utilisée par une autre application.

Exemple

SSLPort 8443

Valeur par défaut

443

SSLTunneling — Active l'établissement de tunnels SSL

S'applique aux configurations avec proxy d'acheminement uniquement.

Lorsque cette directive a la valeur `on`, l'établissement de tunnels SSL est autorisé sur n'importe quel port du serveur de destination. Lorsqu'elle a la valeur `off`, l'établissement de tunnels SSL est possible uniquement sur les ports définis dans les règles Proxy. S'il n'existe aucune règle Proxy pour l'établissement de tunnels SSL et que la directive SSLTunneling a la valeur `off`, cette fonction n'est pas autorisée. Si la directive SSLTunneling possède la valeur `on`, vous devez également activer la méthode CONNECT à l'aide de la directive `Enable`.

Activez cette directive si vous utilisez Caching Proxy comme proxy d'acheminement. Toutefois, lorsque vous utilisez Caching Proxy comme proxy inversé, la désactivation de cette directive (option par défaut) permet de vous protéger contre les attaques de tunnels SSL.

Pour plus d'informations, voir «Etablissement de tunnels SSL», à la page 119.

Remarque : Utilisez la directive Proxy pour activer l'établissement de tunnels SSL sur un port spécifique de l'hôte de destination.

Format

SSLTunneling {on | off}

Valeur par défaut

SSLTunneling off

SSLVersion — Spécifie la version de SSL

Cette directive permet de spécifier la version SSL à utiliser V2, V3 ou n'importe quelle version. Affectez à cette directive la valeur V2 si vous utilisez des serveurs ne prenant pas en charge SSL version 3.

Remarque : Les directives SSL ne sont pas prises en charge sous SUSE Linux.

Format

SSLVersion {SSLV2 | SSLV3 | all}

Valeur par défaut

SSLVersion SSLV3

SSLV2Timeout — Indique le délai d'inactivité au-delà duquel une session SSLV2 expire

Cette directive permet d'indiquer, en secondes, le délai d'inactivité au-delà duquel une session SSL version 3 expire.

Remarque : Les directives SSL ne sont pas prises en charge sous SUSE Linux.

Format

SSLV2Timeout *secondes*

où *secondes* est une valeur comprise entre 0 et 100.

Valeur par défaut

SSLV2Timeout 100

SSLV3Timeout — Indique le délai d'inactivité au-delà duquel une session SSLV3 expire

Cette directive permet d'indiquer, en secondes, le délai d'inactivité au-delà duquel une session SSL version 3 expire.

Remarque : Les directives SSL ne sont pas prises en charge sous SUSE Linux.

Format

SSLV3Timeout *secondes*

où *secondes* est une valeur comprise entre 1 et 86400 secondes (1 jour exprimé en secondes).

Valeur par défaut

SSLV3Timeout 100

SuffixCaseSense — Indique si les majuscules et les minuscules sont différenciées dans les définitions d'extension

Cette directive permet d'indiquer si le serveur fait une distinction entre les majuscules et les minuscules lorsqu'il compare les extensions de fichier aux modèles d'extensions dans les directives AddClient, AddCharSet, AddType, AddEncoding et AddLanguage. Par défaut, les majuscules et les minuscules ne sont pas différenciées.

Format

SuffixCaseSense {on | Off}

Valeur par défaut

SuffixCaseSense Off

SupportVaryHeader — Met en cache plusieurs variantes d'une ressource sur la base de l'en-tête HTTP Vary

Cette directive autorise Caching Proxy à mettre en cache plusieurs variantes d'une ressource (URI) sur la base de l'en-tête HTTP Vary.

Lorsque la directive SupportVaryHeader est activée, le proxy crée un ID de cache fondé sur l'URI et les valeurs d'en-tête sélectionnées dans la demande client.

Les noms des en-têtes sélectionnés sont spécifiés dans l'en-tête Vary envoyé dans une réponse précédente du serveur. Si le serveur modifie l'ensemble des noms d'en-tête sélectionnés pour une ressource, tous les objets mis en cache précédemment pour la ressource sont supprimés du cache du proxy.

Cette directive peut être utilisée en association avec la directive RegisterCacheIdTransformer («RegisterCacheIdTransformer — Met en cache plusieurs variantes d'une ressource sur la base de l'en-tête Cookie», à la page 272).

Lorsque ces deux directives sont utilisées, le proxy crée un convertisseur d'ID de cache interne fondé sur l'en-tête Vary provenant de l'en-tête de la demande du serveur et du client. Le proxy peut ainsi générer des identificateurs de cache uniques pour des paires de demande et de réponse différentes même si les URI demandés sont identiques.

Les objets mis en cache dotés du même URI ont une durée de conservation en cache par défaut différente, qui dépend des en-têtes Expire et Cache-Control dans les demandes/réponses ou d'autres paramètres de configuration. Si le plug-in Dynacache est utilisé, toutes les présentations multiples associées au même URI perdent leur validité simultanément dans la mémoire cache du proxy.

Format

SupportVaryHeader {on | off}

Exemple

Dans cet exemple, les directives suivantes sont activées et configurées dans le fichier ibmproxy.conf, comme indiqué ci-dessous :

```
SupportVaryHeader on
RegisterCacheIdTransformer Cookie UserGroup
```

L'utilisateur Guest (invité) du client accède au serveur proxy avec
URI [`<code>`] `http://www.dot.com/group.jpg` [`</code>`]

et la demande/réponse suivante :

```
GET /group.jpg HTTP/1.1
Host: www.dot.com
Cookie: UserGroup=Guest
Accept-Language: en_US
```

```
HTTP/1.1 200
Server: my-server
Vary: Accept-Language
.....
```

L'utilisateur Admin du client accède ensuite au serveur proxy avec le même URI
`http://www.dot.com/group.jpg`

et la demande/réponse suivante :

```
GET /group.jpg HTTP/1.1
Host: www.dot.com
Cookie: UserGroup=Admin
Accept-Language: fr_FR
```

```
HTTP/1.1 200
Server: my-server
Vary: Accept-Language
.....
```

Ainsi, si la réponse peut être mise en cache, le serveur proxy génère deux ID de cache différents :

1. CacheID(URI, "Guest", "en_US")
2. CacheID(URI, "Admin", "fr_FR")

Le serveur proxy enregistre en mémoire cache deux variantes différentes de la réponse du serveur. Ainsi, lorsqu'un client demande la ressource (.../group.jpg), avec n'importe quelle combinaison de valeurs de préférence de langue et de groupe utilisateur, le serveur proxy extrait du cache la variante appropriée de la ressource et l'envoie au client.

Valeur par défaut

SupportVaryHeader off

TLSV1Enable — Active le protocole Transport Layer Secure (TLS)

Cette directive permet d'activer le protocole TLS version 1 pour les connexions SSL. Une fois cette directive activée, la connexion SSL vérifie d'abord le protocole TLS, puis le protocole SSLv3 et enfin le protocole SSLv2.

Remarque : Cette directive fonctionne avec Internet Explorer et d'autres navigateurs, mais pas avec Netscape. (Il est déconseillé d'utiliser Netscape avec Caching Proxy.)

Format

TLSV1Enable {on | off}

Exemple

TLSV1Enable on

Paramètre du fichier de configuration d'origine

Aucun

Transmogrier — Personnalise l'étape de manipulation des données

Cette directive permet de spécifier une fonction d'application personnalisée devant être appelée par le serveur lors de l'étape de manipulation des données. Ce code fournit trois fonctions d'application :

- Une fonction d'*ouverture* qui effectue une initialisation avant le traitement des données
- Une fonction d'*écriture* qui traite les données
- Une fonction de *fermeture* qui effectue les opérations de nettoyage
- Une fonction d'*erreur* qui informe les utilisateurs des incidents survenus

Plusieurs directives Transmogrifier peuvent être actives dans chaque instance du serveur.

Format

Transmogrifier

/chemin/fichier:nom_fonction:nom_fonction:nom_fonction:

/chemin/fichier

Indique le nom complet du fichier du programme compilé, comprenant l'extension.

nom_fonction

Indique le nom donné à la fonction d'application au sein de votre programme. Vous devez fournir les noms des fonctions d'ouverture, d'écriture et de fermeture.

Exemple

Transmogrifier

/ics/bin/icsext05.so:open_data:write_data:close_data:error_data

Valeur par défaut

Aucun

TransmogrifiedWarning — Envoie un message d'avertissement au client

Utilisez cette directive pour envoyer au client un message relatif aux données :

Format

transmogrifiedwaning {yes|no}

Valeur par défaut

Yes

TransparentProxy — Active le proxy transparent sous Linux

S'applique aux configurations avec proxy d'acheminement uniquement.

Pour les systèmes **Linux** uniquement, utilisez cette directive pour spécifier si le serveur peut s'exécuter comme un serveur proxy transparent.

Lorsque la directive TransparentProxy est définie sur on, la directive BindSpecific est ignorée et prend par défaut la valeur off. La plupart des données HTTP étant acheminées sur le port 80, il est conseillé que ce dernier soit l'un des ports configurés.

Format

TransparentProxy {on | off}

Port 80

Valeur par défaut

TransparentProxy off

En cas d'utilisation du pare-feu IPCHAIN, l'activation de la directive suffit à configurer le proxy transparent. En cas d'utilisation du pare-feu IPTABLES, vous devez ajouter manuellement la règle du pare-feu IPTABLES.

Si vous utilisez le pare-feu IPTABLES, à l'activation de la directive TransparentProxy et **avant de démarrer le serveur proxy**, exécutez la commande suivante pour ajouter la règle de pare-feu dans IPTABLES :

```
iptables -t nat -A PREROUTING -i votre-interface-réseau -p tcp --dport 80 -j  
REDIRECT --to-port port-écoute-prox-ibm
```

En supposant que le pare-feu et le serveur proxy se trouvent dans la même ///case, cette règle demande au pare-feu IPTABLES de rediriger tout le trafic TCP indiqué pour le port 80 sur le port d'écoute du proxy local. Vous pouvez également ajouter la règle dans la configuration IPTABLES. La règle peut ainsi se charger automatiquement au redémarrage du système.

Si, après avoir démarré le proxy transparent, vous voulez arrêter le serveur Caching Proxy, vous devez également lancer la commande suivante en tant qu'utilisateur root :

```
ibmproxy -unload
```

Sous Linux, cette commande supprime les règles de pare-feu de réacheminement. Si vous ne lancez pas cette commande après l'arrêt du serveur, votre machine acceptera des demandes qui ne lui sont pas destinées.

UpdateProxy — Indique la destination de la mémoire cache

Cette directive permet d'identifier le serveur proxy que l'agent de la mémoire cache doit mettre à jour. Elle est requise lorsque l'agent de la mémoire cache doit mettre à jour un serveur proxy autre que le serveur proxy local sur lequel il est exécuté. Vous pouvez éventuellement spécifier le port.

Remarque : Sur les plateformes Linux et UNIX, cette directive est requise pour l'utilisation de l'agent de la mémoire cache. Si vous utilisez une seule machine pour le proxy, spécifiez le nom d'hôte.

S'il est capable de mettre à jour la mémoire cache sur un autre serveur, l'agent de la mémoire cache ne peut pas récupérer le journal des accès à la mémoire cache sur cette machine. Ainsi, si la directive UpdateProxy spécifie un hôte autre que l'hôte local, la directive LoadTopCached est ignorée.

Format

```
UpdateProxy  
nom_d'hôte_complet_du_serveur_proxy
```

Exemple

```
UpdateProxy proxy15.ibm.com:1080
```

Valeur par défaut

Aucun

Userld — Spécifie l'ID utilisateur par défaut

Cette directive permet de spécifier le nom ou le numéro de l'utilisateur auquel accède serveur avant d'accéder aux fichiers.

Si vous changez cette directive, vous devez arrêter manuellement le serveur puis le redémarrer pour que le changement soit effectif. La modification n'est pas prise en compte si vous redémarrez le serveur sans l'arrêter. (Voir Chapitre 5, «Démarrage et arrêt de Caching Proxy», à la page 15.)

Remarque : Si vous modifiez les paramètres par défaut du serveur pour l’ID utilisateur, l’ID groupe ou les chemins d’accès au répertoire journal, créez des répertoires et mettez à jour leurs droits d’accès et leurs propriétés. Pour que le serveur puisse enregistrer des informations dans un répertoire de consignation défini par un utilisateur, attribuez à ce répertoire des droits d’accès 755 et définissez l’ID utilisateur du serveur défini par l’utilisateur comme propriétaire. Par exemple, si l’ID utilisateur du serveur est pdupont et que le répertoire de consignation par défaut est server_root/account, le répertoire server_root/account doit posséder les droits 755 et appartenir à pdupont.

Format

UserId {*nom_ID* | *numéro*}

Valeur par défaut

AIX, Linux, Solaris : UserId nobody

HP-UX : UserId www

V2CipherSpecs — Indique les spécifications de chiffrement prises en charge par SSL version 2

Cette directive donne la liste des spécifications de chiffrement disponibles pour SSL version 2.

Remarque : Les directives SSL ne sont pas prises en charge sous SUSE Linux.

Format

V2CipherSpecs *spécification*

Toutes les associations de valeurs suivantes sont admises. Aucune ne peut être utilisée deux fois.

- 1 — RC4 US
- 2 — RC4 Export
- 3 — RC2 US
- 4 — RC2 Export
- 6 — DES 56-bit
- 7 — Triple DES US
- NULL — Les spécifications de chiffrement par défaut sont utilisées

Exemples

- Pour les Etats-Unis : V2CipherSpecs '137624'
- Pour les autres pays : V2 Cipherspecs '246'

Valeur par défaut

Aucun (SSL est désactivé par défaut.)

V3CipherSpecs — Indique les spécifications de chiffrement prises en charge par SSL version 3

Cette directive affiche la liste des spécifications de chiffrement disponibles pour SSL version 3.

Remarque : Les directives SSL ne sont pas prises en charge sous SUSE Linux.

Si la directive `FIPSEnable` a la valeur "on", la directive `V3CipherSpecs` est ignorée. Pour plus d'informations, voir «`FIPSEnable` — Codes de chiffrement conformes à la norme FIPS (Enable Federal Information Processing Standard) pour SSLV3 et TLS», à la page 220.

Format

`V3CipherSpecs` *spécification*

Les valeurs admises sont les suivantes :

- 00 — NULL NULL
- 01 — NULL MD5
- 02 — NULL SHA
- 03 — RC4 MD5 Export
- 04 — RC4 MD5 US
- 05 — RC4 SHA US
- 06 — RC2 MD5 Export
- 09 — DES SHA Export
- 0A — Triple DS SHA US
- 62 — 56-bit DES CBC SHA
- 64 — 56-bit RC4 SHA
- NULL — Les spécifications de chiffrement par défaut sont utilisées

Exemples

- Pour les Etats-Unis : `V3CipherSpecs '0A09060564620403020100'`
- Pour les autres pays : `V3Cipherspecs '0906646203020100'`

Valeur par défaut

Aucun (SSL est désactivé par défaut.)

WebMasterEMail — Définit une adresse électronique pour la réception des rapports d'un serveur sélectionné

Cette directive permet de définir une adresse électronique à laquelle recevoir des rapports d'un Caching Proxy sélectionné, tel un avertissement 30 jours avant l'expiration d'un certificat SSL. Sous Linux et UNIX, un processus `sendmail` doit être actif. Sous Windows, le processus `sendmail` est intégré à Caching Proxy, de sorte qu'aucun serveur de messagerie externe n'est requis. Deux directives supplémentaires doivent toutefois être définies : «`WebMasterSocksServer` (Windows uniquement)— Configure un serveur socks pour la routine `sendmail`», à la page 292 et «`SMTPServer` (Windows uniquement)— Configure un serveur SMTP pour la routine `sendmail`», à la page 280.

Remarque : Cette adresse électronique est également utilisée en tant que mot de passe FTP anonyme.

Format

`WebMasterEMail` *adresse_électronique_webmaster*

Exemple

`WebMasterEmail webmaster@computer.com`

Valeur par défaut

`WebMasterEmail webmaster`

WebMasterSocksServer (Windows uniquement)— Configure un serveur socks pour la routine sendmail

Cette directive permet de configurer le serveur socks qu'utilise la routine interne sendmail dans le cadre de Caching Proxy pour Windows. Cette routine nécessite également la définition des directives «WebMasterEMail — Définit une adresse électronique pour la réception des rapports d'un serveur sélectionné», à la page 291 et «SMTPServer (Windows uniquement)— Configure un serveur SMTP pour la routine sendmail», à la page 280.

Format

WebMasterSocksServer adresse IP ou nom d'hôte du serveur socks

Exemple

WebMasterSocksServer socks.mybox.com

Valeur par défaut

Aucun

Welcome — Spécifie le nom des fichiers de bienvenue

Cette directive permet de spécifier le nom d'un fichier de bienvenue que le serveur doit rechercher pour répondre à des demandes qui ne contiennent pas de nom de fichier. Vous pouvez créer une liste de fichiers de bienvenue en insérant plusieurs occurrences de cette directive dans le fichier de configuration.

Lorsque les demandes ne contiennent pas de nom de fichier ou de répertoire, le serveur recherche dans le répertoire principal des fichiers un fichier dont le nom correspond à l'un de ceux indiqués dans une directive Welcome. Si une correspondance est trouvée, le fichier est renvoyé au demandeur.

Lorsque les demandes contiennent un nom de répertoire et aucun nom de fichier, la directive AlwaysWelcome vérifie que le serveur recherche dans le répertoire un fichier de bienvenue à renvoyer. Par défaut, la directive AlwaysWelcome a pour valeur 0n. Cela signifie que le serveur recherche toujours dans le répertoire demandé un fichier correspondant au nom indiqué dans une directive Welcome. Si une correspondance est trouvée, le fichier est renvoyé au demandeur.

Si le serveur trouve plusieurs correspondances entre les noms de fichier d'un répertoire et ceux des directives Welcome, l'ordre d'apparition des directives Welcome détermine le fichier renvoyé. Le serveur utilise la première directive Welcome du fichier de configuration.

Format

Welcome nom_fichier
[adresse_IP_serveur |
nom_hôte]

nom_fichier

Indique le nom du fichier à utiliser comme fichier de bienvenue.

[adresse_serveur_IP | nom_hôte]

Si vous utilisez plusieurs adresses IP ou noms d'hôte, utilisez ce paramètre pour spécifier une adresse IP ou un nom d'hôte. Le serveur utilise la directive uniquement pour les demandes arrivant sur le serveur à cette adresse IP ou pour cet hôte. Pour une adresse IP, il s'agit de l'adresse de la connexion réseau du serveur et non de l'adresse du client à l'origine de la demande.

Vous pouvez spécifier une adresse IP (par exemple, 240.146.167.72) ou un nom d'hôte (par exemple, hostA.bcd.com).

Ce paramètre est facultatif. Sans ce paramètre, le serveur utilise la directive pour toutes les demandes, quelle que soit l'adresse IP d'où elles proviennent ou le nom d'hôte de l'URL.

Il n'est pas possible d'indiquer de caractère générique pour une adresse IP de serveur.

Exemples

- L'exemple ci-dessus définit deux pages de bienvenue et part du principe que la directive AlwaysWelcome utilise sa valeur par défaut 0n. Lorsque les demandes ne contiennent pas de nom de fichier, le serveur tente de renvoyer un fichier de bienvenue à partir du répertoire indiqué dans la demande (ou du répertoire principal des fichiers si la demande n'indique aucun nom de fichier ou de répertoire). Le serveur recherche d'abord un fichier appelé letsgo.html. Si aucun fichier ne porte ce nom dans le répertoire, le serveur recherche un fichier appelé Welcome.html.

```
Welcome letsgo.html
Welcome Welcome.html
```

- Dans l'exemple suivant, le serveur doit rechercher différents fichiers de bienvenue selon l'adresse IP de la connexion réseau d'où provient la demande. Pour les demandes venant de 0.67.106.79, le serveur cherche les fichiers de bienvenue nommés CustomerA.html. Pour les demandes venant de 0.83.100.45, le serveur cherche les fichiers de bienvenue nommés CustomerB.html. Si la demande est reçue à une autre adresse IP, le serveur recherche l'adresse par défaut.

```
Welcome CustomerA.html 0.67.106.79
Welcome CustomerB.html 0.83.100.45
```

- Dans l'exemple suivant, le serveur doit rechercher différents fichiers de bienvenue selon le nom d'hôte de l'URL. Pour les demandes venant de l'hôteA, le serveur doit rechercher les fichiers de bienvenue appelés CustomerA.html. Pour les demandes venant de l'hôteB, le serveur doit rechercher les fichiers de bienvenue appelés CustomerB.html. Si la demande est reçue pour un hôte différent, le serveur recherche le nom hôte par défaut.

```
Welcome CustomerA.html hôteA.bcd.com
Welcome CustomerB.html hôteB.bcd.com
```

Valeurs par défaut

Ces valeurs par défaut sont indiqués dans l'ordre utilisé par le fichier de configuration.

```
Welcome Welcome.html
Welcome welcome.html
Welcome index.html
Welcome Frntpage.html
```

Remarques

Première édition (mai 2006)

Les informations décrites dans ce manuel s'appliquent aux produits et services proposés aux Etats-Unis.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Corporation
Attn.: G71A/503
P.O. box 12195
3039 Cornwallis Rd.
Research Triangle Park, N.C. 27709-2195
Etats-Unis

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT". IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE VALEUR MARCHANDE OU D'ADAPTATION A VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier sans préavis les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils

contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
ATTN: Software Licensing
11 Stanwix Street
Pittsburgh, PA 15222-9183
Etats-Unis

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

Les termes qui suivent sont des marques d'IBM Corporation aux Etats-Unis et/ou dans certains autres pays :

- AIX
- IBM
- Netfinity
- RS/6000
- SecureWay
- Tivoli
- ViaVoice
- WebSphere

Java ainsi que toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT, et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Intel, Intel Inside (logos), MMX et Pentium sont des marques d'Intel Corporation aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.



GC11-2540-00



Spine information:



WebSphere Application Server

Caching Proxy - Guide d'administration

Version 6.1

GC11-2540-00