

WebSphere Application Server



# Guía de administración de Caching Proxy

*Versión 6.1*



WebSphere Application Server



# Guía de administración de Caching Proxy

*Versión 6.1*

**Nota**

Antes de utilizar esta información y el producto al que da soporte, asegúrese de leer la información general del apartado "Avisos" en la página 297.

**Primera edición (mayo de 2006)**

Esta edición se aplica a:

WebSphere Application Server, Versión 6.1

y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Realice el pedido de las publicaciones a través del representante de IBM o de la sucursal de IBM que presta servicio en su localidad.

© Copyright International Business Machines Corporation 2006. Reservados todos los derechos.

---

# Contenido

## Figuras . . . . . xi

## Acerca de este manual . . . . . xiii

A quién va dirigido este manual . . . . .	xiii
Convenios y terminología que se utilizan en este manual . . . . .	xiii
Accesibilidad . . . . .	xiv
Cómo enviar comentarios . . . . .	xiv
Información relacionada . . . . .	xiv

---

## Parte 1. Guía de iniciación con Caching Proxy . . . . . 1

### Capítulo 1. Visión general . . . . . 3

Configuraciones básicas de Caching Proxy . . . . .	3
Proxy de retorno (valor por omisión) . . . . .	3
Proxy de reenvío . . . . .	3
Soporte de nuevas características . . . . .	4

### Capítulo 2. Utilización de los formularios de Configuración y Administración . . . . 7

Requisitos del navegador . . . . .	7
Acceso a los formularios de Configuración y Administración . . . . .	8
Establecimiento de la contraseña de administrador . . . . .	9

### Capítulo 3. Utilización del Asistente de configuración . . . . . 11

### Capítulo 4. Edición manual del archivo ibmproxy.conf . . . . . 13

### Capítulo 5. Inicio y detención de Caching Proxy . . . . . 15

Arranque y cierre automático en sistemas Linux y UNIX . . . . .	15
Arranque manual en sistemas Linux y UNIX . . . . .	16
En AIX: . . . . .	16
En HP-UX: . . . . .	16
En Linux: . . . . .	16
En Solaris: . . . . .	17
Arranque como servicio Windows . . . . .	17
Arranque como aplicación Windows . . . . .	18
Utilización del menú Inicio . . . . .	18
Utilización del indicador de mandatos . . . . .	18
Inicio de varios servidores proxy . . . . .	19
Cierre manual en sistemas Linux y UNIX . . . . .	19
Limitaciones de los mandatos de cierre . . . . .	20
Cierre manual en sistemas Windows . . . . .	21
Reinicio después de los cambios de configuración . . . . .	21

---

## Parte 2. Configuración y ajuste del proceso de Caching Proxy . . . . . 23

### Capítulo 6. Definición del servidor . . . . . 25

Directivas asociadas . . . . .	26
Formularios de Configuración y Administración . . . . .	26

### Capítulo 7. Establecimiento de la propiedad de procesos. . . . . 29

Directivas asociadas . . . . .	29
Formularios de Configuración y Administración . . . . .	30

### Capítulo 8. Gestión de conexiones. . . . . 31

Directivas asociadas . . . . .	32
Formularios de Configuración y Administración . . . . .	33

### Capítulo 9. Ajuste del proceso del servidor proxy . . . . . 35

Establecimiento de las directivas relacionadas con el rendimiento . . . . .	35
Examinar el resto de aplicaciones . . . . .	35
Verifique el espacio de paginación . . . . .	36
Ajuste el sistema de archivos . . . . .	36
Ajuste de la configuración TCP/IP . . . . .	36
Ajuste el intervalo tiempo de espera de TCP para los entornos de carga alta (HP-UX, Linux, Solaris, Windows) . . . . .	36
Ajuste del kernel de Linux . . . . .	37
Ajuste las variables de ajuste de hebras de AIX . . . . .	38

---

## Parte 3. Configuración del comportamiento de Caching Proxy . . 39

### Capítulo 10. Gestionar el proceso de peticiones . . . . . 41

Habilitación de métodos HTTP/FTP . . . . .	41
Directivas asociadas . . . . .	42
Formularios de Configuración y Administración . . . . .	42
Habilitar métodos WebDAV, métodos MS Exchange y métodos definidos por el usuario . . . . .	43
Directivas asociadas . . . . .	44
Definición de normas de correlación . . . . .	44
Normas de correlación. . . . .	44
Configuración del servidor sustituto . . . . .	46
Directivas asociadas . . . . .	46
Formularios de Configuración y Administración . . . . .	46
Habilitación de la reescritura de unión (opcional). . . . .	47
Definición de la unión sin la opción JunctionPrefix . . . . .	47
Definición de la unión con la opción JunctionPrefix (método recomendado) . . . . .	48
Directivas asociadas . . . . .	49

Formularios de Configuración y Administración	49
UseCookie como alternativa a JunctionRewrite	49
Ejemplo de plug-in de transformación rápida para ampliar la funcionalidad de JunctionRewrite	50

## **Capítulo 11. Gestión del envío del contenido local . . . . . 51**

Definición de un directorio raíz de documentos	51
Directivas asociadas	51
Formularios de Configuración y Administración	51
Definición de las páginas de bienvenida por omisión	52
Directivas asociadas	53
Formularios de Configuración y Administración	53

## **Capítulo 12. Gestión de las conexiones FTP . . . . . 55**

Protección de archivos FTP	55
Gestión del inicio de sesión del servidor FTP	55
Gestión de las vías de acceso de directorios FTP	56
Gestionar el encadenamiento FTP	57

## **Capítulo 13. Personalización del proceso del servidor. . . . . 59**

Inclusiones de servidor	59
Consideraciones para las inclusiones de servidor	59
Configuración de las inclusiones de servidor	59
Formato de las inclusiones de servidor	60
Directivas de las inclusiones de servidor.	60
Personalización de los mensajes de error	67
Redirección RTSP (Real Time Streaming Protocol).	67
Acerca de la redirección RTSP	67
Limitación RTSP.	68
Mejora RTSP	68
Configuración de la redirección RTSP.	68

## **Capítulo 14. Configuración de las opciones de cabecera . . . . . 69**

Directivas asociadas	69
Formularios de Configuración y Administración	70

## **Capítulo 15. Acerca de la interfaz de programas de aplicación . . . . . 71**

Directivas asociadas	71
Formularios de Configuración y Administración	71

## **Parte 4. Configuración de la antememoria y el servidor proxy . . 73**

### **Capítulo 16. Visión general de la colocación en antememoria del servidor proxy . . . . . 75**

Almacenamiento de antememoria	75
Índice de antememoria	75
Colocación en antememoria de FTP	76
Colocación en antememoria DNS	77
Exclusiones de antememoria.	77
Gestión de la antememoria	77

### **Capítulo 17. Configuración de la colocación en antememoria básica . . . 79**

1. Habilite la colocación en antememoria	79
2. Configure el almacenamiento en antememoria	79
Personalizaciones opcionales.	81
Establecimiento de la memoria de antememoria	81
Cómo guardar y cargar la memoria de antememoria en el disco	82
Establecimiento de la colocación en antememoria de los filtros	82
Configuración de la colocación en antememoria de los resultados de las consultas y los archivos generados dinámicamente	82
Configuración de la caducidad de archivos y la recogida de basura	82
Configuración de la precarga automática	82
Configuración del compartimiento de antememoria	82
Configuración del registro cronológico	82

### **Capítulo 18. Control de los elementos colocados en antememoria . . . . . 83**

Configuración de filtros de colocación en antememoria basados en URL	83
Colocación en antememoria de respuestas de consultas	84
Requisitos adicionales para la colocación en antememoria de respuestas de consultas.	84
Colocación en antememoria de archivos servidos localmente.	85
Colocación en antememoria de los archivos mediante URL parcial	85
Directivas relacionadas del archivo de configuración	86

### **Capítulo 19. Mantenimiento del contenido de la antememoria . . . . . 87**

Caducidad de los archivos	87
Información adicional sobre la antigüedad en la antememoria	88
Acerca de las fechas en FTP	89
Configuración de la antigüedad de antememoria	90
Recogida de basura.	92
Configuración de la recogida de basura	92

### **Capítulo 20. Configuración del agente de carga para la renovación y precarga automática . . . . . 93**

Establecimiento del nombre de sistema principal del servidor	94
Precarga de la antememoria con archivos específicos	95
Precarga de la antememoria con archivos frecuentemente en antememoria	95
Profundización	96
Directivas relacionadas del archivo de configuración de proxy	98
Inicio del agente de antememoria manualmente	99

### **Capítulo 21. Utilización de una antememoria compartida . . . . . 101**

Acceso a antememoria remota . . . . .	101
Configuración del acceso a antememoria remota	102
Configuración del plug-in de Protocolo de antememoria de Internet . . . . .	102
Configuración del plug-in ICP. . . . .	102

## **Capítulo 22. Colocación en antememoria de contenidos generados dinámicamente. . . . . 105**

Configuración de IBM WebSphere Application Server para la antememoria de proxy . . . . .	106
Configuración de la colocación en antememoria dinámica en los servidores de aplicaciones . . . . .	106
Configuración del adaptador del servidor de aplicaciones . . . . .	107
Configuración de Caching Proxy para la colocación en antememoria dinámica . . . . .	107
Establecimiento de la directiva Service para habilitar el plug-in de colocación en antememoria dinámica . . . . .	107
Establecimiento de la directiva ExternalCacheManager para especificar los orígenes de archivo . . . . .	108

## **Capítulo 23. Ajuste de la antememoria del servidor proxy . . . . . 109**

Elección del soporte de almacenamiento de antememoria . . . . .	109
Optimización del rendimiento de antememoria de disco . . . . .	109
Recogida de basura de antememoria . . . . .	109
Optimizaciones específicas de la plataforma . . . . .	110
AIX. . . . .	110
HP-UX y Solaris . . . . .	110
Windows . . . . .	110

## **Parte 5. Configuración de la seguridad de Caching Proxy . . . 111**

### **Capítulo 24. Acerca de la seguridad del servidor proxy . . . . . 113**

### **Capítulo 25. Configuraciones de protección del servidor . . . . . 115**

Utilización de los formularios de Configuración y Administración para establecer la protección . . . . .	115
Utilización de las directivas del archivo de configuración para establecer la protección . . . . .	116
Valores de protección por omisión . . . . .	117

### **Capítulo 26. SSL (Secure Sockets Layer). . . . . 119**

Protocolo de enlace SSL . . . . .	119
Ajuste de rendimiento de SSL . . . . .	120
Túneles SSL . . . . .	121
Configuración de túneles SSL . . . . .	122
Configuración de la administración remota segura	123
Gestión de claves y certificados . . . . .	123

Autoridades certificadoras . . . . .	124
Utilización del programa de utilidad IBM Key Manager . . . . .	125
Creación de una nueva base de datos de claves, una contraseña y un archivo stash . . . . .	126
Recepción de un certificado de CA . . . . .	131
Almacenamiento de un certificado de CA . . . . .	131
Especificaciones de cifrado soportadas . . . . .	132

### **Capítulo 27. Habilitación del soporte de hardware criptográfico . . . . . 135**

### **Capítulo 28. Utilización del plug-in de Tivoli Access Manager . . . . . 137**

Configuración . . . . .	137
Pasos previos a la utilización del script de configuración . . . . .	137
Utilización del script de configuración . . . . .	137
Inicio de Caching Proxy y del plug-in de Access Manager . . . . .	138

### **Capítulo 29. Utilización del módulo de autorización PAC-LDAP . . . . . 139**

Visión general . . . . .	139
Autenticación . . . . .	139
Autorización . . . . .	139
Lightweight Directory Access Protocol (LDAP)	140
Instalación . . . . .	140
Requisitos y restricciones adicionales para las conexiones seguras del servidor PACD-LDAP . . . . .	141
GSKit es necesario para el paquete de cliente LDAP . . . . .	141
La variable de entorno LD_PRELOAD debe establecerse para los sistemas Linux . . . . .	141
En los sistemas Linux, el proceso PACD no se inicia al utilizar el cliente LDAP de IBM Tivoli Directory Server (ITDS) . . . . .	142
En sistemas AIX, el módulo PAC-LDAP no se puede cargar al utilizar el cliente LDAP de IBM Tivoli Directory Server (ITDS) . . . . .	142
Edición del archivo ibmproxy.conf para habilitar el módulo de autorización PAC-LDAP . . . . .	142
Edición de los archivos de configuración del módulo de autorización PAC-LDAP . . . . .	144
paccp.conf . . . . .	144
pac.conf . . . . .	144
pacpolicy.conf . . . . .	145
Creación de pac_ldap.cred . . . . .	146
Inicio y detención de pacd . . . . .	146

## **Parte 6. Supervisión de Caching Proxy . . . . . 149**

### **Capítulo 30. Configuración de las anotaciones cronológicas . . . . . 151**

Acerca de las anotaciones cronológicas . . . . .	151
Nombres de los archivos de anotaciones cronológicas y opciones básicas . . . . .	151

Filtros de las anotaciones cronológicas de acceso	152
Razones para controlar los elementos que se anotan cronológicamente	153
Configuración de las anotaciones cronológicas de acceso	153
Valores de anotaciones cronológicas por omisión	154
Mantenimiento y archivado de las anotaciones cronológicas	155
Escenario de archivo de anotaciones cronológicas	157

## Capítulo 31. Utilización del Supervisor de actividad del servidor . . . . . 159

### Apéndice A. Utilización de los mandatos de Caching Proxy . . . . . 163

Mandato cgiparse	164
Mandato cgiutils	167
Mandato htadm	169
Mandato htcformat	172
Mandato ibmproxy	174

### Apéndice B. Directivas del archivo de configuración . . . . . 177

Directivas que no se modifican durante el reinicio	177
Visión general de las directivas	177
Valores aceptables	178
Sintaxis de los registros del archivo de configuración	179
Directivas de Caching Proxy	179
AcceptAnything: servir todos los archivos	179
AccessLog: nombrar la vía de acceso del archivo de anotaciones cronológicas de acceso	179
AccessLogExcludeMethod: suprimir las entradas de anotaciones cronológicas de los archivos y directorios solicitados por un método específico	180
AccessLogExcludeMimeType: suprimir las entradas de anotaciones cronológicas de acceso al proxy para tipos MIME específicos	181
AccessLogExcludeReturnCode: suprimir las entradas de anotaciones cronológicas de códigos de retorno específicos	181
AccessLogExcludeURL: suprimir las entradas de anotaciones cronológicas de archivos o directorios específicos	182
AccessLogExcludeUserAgent: suprimir las entradas de anotaciones cronológicas de navegadores específicos	182
AddBlankIcon: especificar el URL del icono utilizado para alinear las cabeceras de los listados de directorios	183
AddDirIcon: especificar el URL de icono de los directorios en los listados de directorios	183
AddEncoding: especificar la codificación del contenido MIME de los archivos con sufijos determinados	184
AddIcon: enlazar un icono con un tipo de contenido o de codificación MIME	184
AddParentIcon: especificar el URL del icono que representa el directorio padre en los listados de directorios	185

AddType: especificar el tipo de datos de los archivos con sufijos determinados	185
AddUnknownIcon: especificar el URL de icono de los tipos de archivo desconocidos en los listados de directorios	187
AdminPort: especifica el puerto para solicitar las páginas administrativas o formularios	187
AggressiveCaching: especificar la colocación en antememoria de los archivos que no se colocan en antememoria	188
AlwaysWelcome: especificar si desea buscar los archivos de bienvenida en el directorio solicitado	188
appendCRLFtoPost: añadir CRLF a las peticiones POST	189
ArrayName: nombrar la matriz de antememoria remota	189
Authentication: personalizar el paso de autenticación	189
Authorization: personalizar el paso de autorización	190
AutoCacheRefresh: especificar si se desea utilizar la renovación de antememoria	190
BindSpecific: especificar si el servidor se enlaza a una dirección IP o a todas	191
BlockSize: especificar el tamaño de bloques de la antememoria	191
CacheAccessLog: especificar la vía de acceso de los archivos de anotaciones cronológicas de acceso a la antememoria	191
CacheAlgorithm: especificar el algoritmo de antememoria	192
CacheByIncomingUrl: especificar la base para generar los nombres de archivo de antememoria	192
CacheClean: especificar el periodo de tiempo que se deben mantener los archivos en antememoria	193
CacheDefaultExpiry: especificar el tiempo de caducidad por omisión de los archivos	193
CacheDev: especificar un dispositivo de almacenamiento para la antememoria	194
CacheExpiryCheck: especificar si el servidor devuelve los archivos caducados	194
CacheFileSizeLimit: especificar el tamaño máximo para que los archivos se almacenen en antememoria	195
CacheLastModifiedFactor: especificar el valor para determinar las fechas de caducidad	195
CacheLocalDomain: especificar si se debe colocar en antememoria el dominio local	196
CacheMatchLanguage: especificar la preferencia de idioma para el contenido de antememoria devuelto	196
CacheMaxExpiry: especificar la duración máxima de los archivos en antememoria	197
CacheMemory: especificar la memoria RAM de antememoria	198
CacheMinHold: especificar el periodo de tiempo que están disponibles los archivos	198
CacheNoConnect: especificar la modalidad de antememoria autónoma	199



CacheOnly: colocar en antememoria sólo los archivos con los URL que coinciden con una plantilla . . . . .	199
CacheQueries: especificar las respuestas de antememoria a los URL que contienen un signo de interrogación (?) . . . . .	200
CacheRefreshInterval: especificar el intervalo de tiempo para volver a validar los objetos en antememoria . . . . .	200
CacheRefreshTime: especificar cuándo se desea iniciar el agente de antememoria . . . . .	201
CacheTimeMargin: especificar la duración mínima para colocar en antememoria un archivo	201
CacheUnused: especificar el periodo de tiempo que se deben mantener los archivos en antememoria no utilizados . . . . .	201
Caching: habilitar la colocación en antememoria de proxy . . . . .	202
CompressAge: especificar cuándo comprimir las anotaciones cronológicas . . . . .	202
CompressCommand: especificar el mandato y los parámetros de compresión . . . . .	203
CompressDeleteAge: especificar cuándo suprimir las anotaciones cronológicas . . . . .	204
CompressionFilterAddContentType — Especificar el tipo de contenido de la respuesta HTTP que desea comprimir . . . . .	204
CompressionFilterEnable — Habilitar el filtro de compresión para comprimir las respuestas HTTP . . . . .	205
ConfigFile: especificar el nombre de un archivo de configuración adicional . . . . .	205
ConnThreads: especificar el número de hebras de conexión que se van a utilizar para la gestión de conexiones . . . . .	205
ContinueCaching: especificar qué cantidad de un archivo es necesaria para la colocación en antememoria . . . . .	206
DefinePicsRule: proporcionar una norma de filtrado de contenido . . . . .	206
DefProt: especificar la configuración de protección por omisión de las peticiones que coinciden con una plantilla . . . . .	206
DelayPeriod: especificar si debe haber una pausa entre peticiones . . . . .	209
DelveAcrossHosts: especificar la colocación en antememoria entre dominios . . . . .	209
DelveDepth: especificar hasta dónde se deben seguir los enlaces durante la colocación en antememoria . . . . .	209
DelveInto: especificar si el agente de antememoria debe seguir los enlaces . . . . .	210
DirBackgroundImage: especificar una imagen de fondo para los listados de directorios . . . . .	210
DirShowBytes: mostrar el recuento en bytes de los archivos pequeños en los listados de directorios . . . . .	210
DirShowCase: utilizar las mayúsculas y minúsculas al ordenar los archivos en los listados de directorios . . . . .	211

DirShowDate: mostrar la fecha de última modificación en los listados de directorios . . . . .	211
DirShowDescription: mostrar las descripciones de los archivos en los listados de directorios . . . . .	211
DirShowHidden: mostrar los archivos ocultos en los listados de directorios . . . . .	211
DirShowIcons: mostrar los iconos en los listados de directorios . . . . .	212
DirShowMaxDescrLength: especificar la longitud máxima de las descripciones en los listados de directorios . . . . .	212
DirShowMaxLength: especificar la longitud máxima de los nombres de archivos en los listados de directorios . . . . .	212
DirShowMinLength: especificar la longitud mínima de los nombres de archivos en los listados de directorios . . . . .	212
DirShowSize: mostrar el tamaño de archivo en los listados de directorios . . . . .	213
Disable: inhabilitar los métodos HTTP . . . . .	213
DisInheritEnv: especificar las variables de entorno que no heredan los programas CGI . . . . .	213
DNS-Lookup: especificar si el servidor debe buscar los nombres de nombre de sistema principal de cliente . . . . .	214
Enable: habilitar los métodos HTTP . . . . .	214
EnableTcpNodelay: habilitar la opción de socket TCP NODELAY . . . . .	215
Error: personalizar el paso de error . . . . .	215
ErrorLog: especificar el archivo donde se anotan cronológicamente los errores de servidor . . . . .	215
ErrorMessage: especificar un mensaje personalizado para una determinada condición de error . . . . .	216
Values por omisión . . . . .	218
EventLog: especificar la vía de acceso del archivo de anotaciones cronológicas de sucesos . . . . .	218
Exec: ejecutar un programa CGI para hacer coincidir las peticiones . . . . .	218
ExportCacheImageTo: exportar la memoria de antememoria al disco . . . . .	220
ExternalCacheManager: configurar Caching Proxy para la colocación en antememoria dinámica desde IBM WebSphere Application Server . . . . .	220
Fail: rechazar peticiones coincidentes . . . . .	221
FIPSEnable: cifrados aprobados por FIPS (Enable Federal Information Processing Standard) para SSLV3 y TLS . . . . .	222
flexibleSocks: habilitar la implementación de SOCKS flexibles . . . . .	222
FTPDirInfo: generar un mensaje descriptivo o de bienvenida de un directorio . . . . .	222
ftp_proxy: especificar otro servidor proxy para las peticiones FTP . . . . .	223
FTPUriPath: especificar cómo se interpretan los URL de FTP . . . . .	223
Gc: especificar la recogida de basura . . . . .	224
GCAvvisor: personalizar el proceso de recogida de basura . . . . .	224
GcHighWater: especificar cuándo empieza la recogida de basura . . . . .	224

GcLowWater: especificar cuándo termina la recogida de basura . . . . .	224
gopher_proxy: especificar otro servidor de proxy para las peticiones Gopher. . . . .	225
GroupId: especificar el ID de grupo . . . . .	225
HeaderServerName: especificar el nombre del servidor proxy devuelto en la cabecera HTTP . . . . .	226
Hostname: especificar el nombre de dominio plenamente cualificado o dirección IP del servidor . . . . .	226
http_proxy: especificar otro servidor proxy para las peticiones HTTP . . . . .	226
HTTPSCheckRoot: filtrar las peticiones HTTPS . . . . .	227
ICP_Address: especificar la dirección IP para las consultas ICP . . . . .	227
ICP_MaxThreads: especificar el número de hebras para las consultas ICP . . . . .	227
Occupier: especificar un miembro de un clúster ICP. . . . .	228
ICP_Port: especificar el número de puerto para las consultas ICP . . . . .	228
ICP_Timeout: especificar el tiempo de espera máximo para las consultas ICP . . . . .	228
IgnoreURL: especificar los URL que no se van a renovar . . . . .	229
imbeds: especificar si se va a utilizar el proceso de inclusión de la parte servidor . . . . .	229
ImportCacheImageFrom: importar la memoria de antememoria de un archivo . . . . .	230
InheritEnv: especificar qué variables de entorno heredan los programas CGI . . . . .	231
InputTimeout: especificar el tiempo de espera de la entrada . . . . .	231
JunctionReplaceUrlPrefix: sustituir el URL en lugar de insertar un prefijo cuando se utiliza con el plug-in JunctionRewrite . . . . .	231
JunctionRewrite: habilitar la reescritura de URL . . . . .	232
JunctionRewriteSetCookiePath: reescribir la opción de vía de acceso en la cabecera Set-Cookie cuando se utiliza con el plug-in JunctionRewrite . . . . .	232
JunctionSkipUrlPrefix: omitir la reescritura de los URL que ya contienen el prefijo cuando se utiliza con el plug-in JunctionRewrite . . . . .	233
KeepExpired: especificar la devolución de la copia caducada del recurso si se está actualizando el recurso en el proxy . . . . .	233
KeyRing: especificar la vía de acceso del archivo a la base de datos de conjunto de claves . . . . .	234
KeyRingStash: especificar la vía de acceso del archivo al archivo de contraseñas de la base de datos de conjunto de claves . . . . .	234
LimitRequestBody: especificar el tamaño máximo de cuerpo de las peticiones PUT o POST . . . . .	234
LimitRequestFields: especificar el número máximo de cabeceras de las peticiones de cliente . . . . .	235
LimitRequestFieldSize: especificar la longitud máxima de cabecera y de la línea de petición. . . . .	235

ListenBacklog: especificar el número de conexiones de cliente del registro de reserva de escucha que puede transportar el servidor. . . . .	235
LoadInlineImages: controlar la renovación de imágenes anidadas . . . . .	236
LoadTopCached: especificar el número de páginas más solicitadas que se van a renovar. . . . .	236
LoadURL: especificar los URL que se van a renovar . . . . .	236
Log: personalizar el paso de anotación cronológica . . . . .	236
LogArchive: especificar el comportamiento del archivado de las anotaciones cronológicas . . . . .	237
LogDateFormat: especificar el formato de las anotaciones cronológicas de acceso . . . . .	238
LogToGUI (Windows sólo): visualizar las entradas de anotaciones cronológicas en la ventana del servidor . . . . .	238
LogToSyslog: especificar si se va a enviar la información de acceso a las anotaciones cronológicas del sistema (Linux y UNIX sólo) . . . . .	238
Map — Cambiar las peticiones coincidentes a una nueva serie de petición, utilizando la serie de vía de acceso de petición para cumplir la regla . . . . .	239
MapQuery — Cambiar las peticiones coincidentes a una nueva serie de petición, utilizando la serie de vía de acceso de petición y consulta para cumplir la regla. . . . .	241
MaxActiveThreads: especificar el número máximo de hebras activas . . . . .	242
MaxContentLengthBuffer: especificar el tamaño del almacenamiento intermedio para los datos dinámicos . . . . .	242
MaxLogFileSize: especificar el tamaño máximo para todos los archivos de anotaciones cronológicas. . . . .	242
MaxPersistRequest: especificar el número máximo de peticiones que se van a recibir en una conexión persistente . . . . .	243
MaxQueueDepth: especificar el número máximo de los URL que se van a colocar en cola . . . . .	244
MaxRuntime: especificar el tiempo máximo de ejecución de un agente de antememoria . . . . .	244
MaxSocketPerServer — Especificar el número máximo de sockets desocupados abiertos para el servidor . . . . .	244
MaxUrls: especificar el número máximo de los URL que se van a renovar . . . . .	245
Member: especificar un miembro de una matriz . . . . .	245
Midnight: especificar el plug-in de API utilizado para archivar las anotaciones cronológicas. . . . .	246
NameTrans: personalizar el paso de traducción de nombres . . . . .	246
NoBG: ejecutar el proceso de Caching Proxy en primer lugar. . . . .	247
NoCaching: especificar que no se coloquen en antememoria los archivos con los URL que coinciden con una plantilla. . . . .	247

NoLog: suprimir las entradas de anotaciones cronológicas de los sistemas principales o dominios específicos que coinciden con una plantilla . . . . .	248	ProxySendClientAddress: generar la cabecera Client IP Address: . . . . .	270
no_proxy: especificar las plantillas para conectarse directamente con los dominios . . . . .	248	ProxyUserAgent; modificar la serie User Agent . . . . .	270
NoCacheOnRange — Especificar sin colocación en antememoria para peticiones de rango . . . . .	249	ProxyVia: especificar el formato de la cabecera HTTP . . . . .	270
NoProxyHeader: especificar las cabeceras de cliente que se desea bloquear . . . . .	250	ProxyWAS: especificar que las peticiones se envíen a WebSphere Application Server . . . . .	271
NumClients: especificar el número de hebras del agente de antememoria que se van a utilizar . . . . .	250	PureProxy: inhabilitar un proxy dedicado . . . . .	271
ObjectType: personalizar el paso de tipo de objeto . . . . .	250	PurgeAge: especificar el límite de antigüedad para las anotaciones cronológicas. . . . .	271
OptimizeRuleMapping — Optimizar el proceso de correlación de regla para las peticiones entrantes cuando aumenta el número de reglas . . . . .	251	PurgeSize: especificar el límite del tamaño del archivador de anotaciones cronológicas. . . . .	272
OutputTimeout: especificar el tiempo de espera de la salida . . . . .	251	RCAConfigFile: especificar un alias para ConfigFile . . . . .	273
PacFilePath: especificar el directorio que contiene los archivos PAC . . . . .	252	RCAThreads: especificar el número de hebras por puerto . . . . .	273
Pass: especificar la plantilla para aceptar peticiones . . . . .	252	ReadTimeout: especificar el límite de tiempo de una conexión . . . . .	273
PersistTimeout: especificar el tiempo de espera para que el cliente envíe otra petición . . . . .	254	Redirect: especificar una plantilla para las peticiones enviadas a un servidor distinto . . . . .	273
PICSDBLookup: personalizar el paso de recuperación de etiquetas PICS . . . . .	254	RegisterCacheIdTransformer: almacenar en antememoria más de una variante de un recurso basándose en la cabecera Cookie . . . . .	275
PidFile (Linux y UNIX sólo): especificar el archivo donde se va a almacenar el ID de proceso de Caching Proxy . . . . .	255	ReversePass: interceptar las peticiones redirigidas automáticamente . . . . .	275
PKCS11DefaultCert, PKCS11DriverPath, PKCS11TokenPassword — Da soporte a la tarjeta IBM 4960 PCI Cryptographic Accelerator Card (sólo AIX). . . . .	255	RewriteSetCookieDomain: especificar el patrón de dominio que es necesario reescribir . . . . .	276
Directivas de módulos de plug-in . . . . .	256	RTSPEnable: habilitar la redirección de RTSP . . . . .	276
Port: especificar el puerto donde el servidor escucha las peticiones . . . . .	257	rtsp_proxy_server: especificar los servidores para la redirección. . . . .	277
PostAuth: personalizar el paso de PostAuth . . . . .	257	rtsp_proxy_threshold: especificar el número de peticiones antes de la redirección a una antememoria . . . . .	277
PostExit: personalizar el paso de PostExit . . . . .	257	rtsp_url_list_size: especificar el número de los URL en la memoria proxy . . . . .	277
PreExit: personalizar el paso de PreExit . . . . .	258	RuleCaseSense — Correlaciona peticiones de los URL de aplicación que no son sensibles a mayúsculas y minúsculas . . . . .	278
Protect: activar una configuración de protección de las peticiones que coinciden con una plantilla . . . . .	258	ScriptTimeout: especificar el valor de tiempo de espera de los scripts . . . . .	278
Protection: definir una configuración de protección con nombre dentro del archivo de configuración . . . . .	263	SendHTTP10Outbound: especificar la versión de protocolo para las peticiones que pasan por el proxy . . . . .	278
Subdirectivas de protección: especificar cómo proteger un conjunto de recursos. . . . .	264	SendRevProxyName: especificar el nombre de sistema principal de Caching Proxy en la cabecera HOST. . . . .	279
Proxy: especificar los protocolos de proxy o el proxy de retorno . . . . .	266	ServerConnGCRun: especificar el intervalo durante el que se ejecuta la hebra de recogida de basura. . . . .	280
ProxyAccessLog; nombrar la vía de acceso del archivo de anotaciones cronológicas de acceso al proxy . . . . .	267	ServerConnPool: especificar la agrupación de conexiones con los servidores de origen . . . . .	280
ProxyAdvisor: personalizar el servicio de las peticiones de proxy . . . . .	268	ServerConnTimeout: especificar el periodo máximo de inactividad . . . . .	280
ProxyForwardLabels: especificar el filtrado PICS . . . . .	268	ServerInit: personalizar el paso de inicialización de servidor . . . . .	281
ProxyFrom: especificar un cliente con una cabecera From: . . . . .	269	ServerRoot: especificar el directorio donde se instala el programa servidor . . . . .	281
ProxyIgnoreNoCache: ignorar una petición de recarga . . . . .	269	ServerTerm: personalizar el paso de terminación de servicio . . . . .	282
ProxyPersistence: permitir las conexiones persistentes . . . . .	269	Service: personalizar el paso de servicio . . . . .	282

SignificantURLTerminator; especificar un código de terminación para las peticiones URL . . . . .	283
SMTPServer (Windows sólo): establecer un servidor SMTP para la rutina sendmail. . . . .	283
SNMP: habilitar e inhabilitar el soporte SNMP . . . . .	284
SNMPCommunity: proporcionar una contraseña de seguridad para SNMP . . . . .	284
SSLCaching: habilitar la colocación en antememoria de una petición segura . . . . .	284
SSLCertificate — Especificar etiquetas de clave para certificados . . . . .	284
SSLCryptoCard: especificar la tarjeta criptográfica instalada . . . . .	286
SSLEnable: especificar la escucha de peticiones seguras en el puerto 443. . . . .	286
SSLForwardPort: especificar a qué puerto dirigirse para las actualizaciones HTTP SSL . . . . .	286
SSLOnly — Inhabilitar hebras de receptor para peticiones HTTP . . . . .	286
SSLPort: especificar un puerto de escucha HTTPS distinto del puerto por omisión. . . . .	287
SSLTunneling: habilitar los túneles SSL . . . . .	287
SSLVersion: especificar la versión de SSL . . . . .	288
SSLV2Timeout: especificar el tiempo de espera antes de que caduque una versión de SSLV2 . . . . .	288
SSLV3Timeout: especificar el tiempo de espera antes de que caduque una versión de SSLV3 . . . . .	288
SuffixCaseSense: especificar si las definiciones de sufijo son sensibles a las mayúsculas y minúsculas . . . . .	288

SupportVaryHeader: almacenar en antememoria más de una variante de un recurso basándose en la cabecera Vary de HTTP . . . . .	289
TLSV1Enable: habilitar el protocolo TLS (Transport Layer Secure). . . . .	290
Transmogriifier: personalizar el paso de manipulación de datos . . . . .	290
TransmogriifiedWarning: enviar un mensaje de aviso al cliente . . . . .	291
TransparentProxy — Habilitar el proxy transparente en Linux . . . . .	291
UpdateProxy: especificar el destino de antememoria . . . . .	292
UserId: especificar el ID de usuario por omisión . . . . .	292
V2CipherSpecs: enumerar las especificaciones de cifrado soportadas para SSL Versión 2 . . . . .	293
V3CipherSpecs: enumerar las especificaciones de cifrado soportadas para SSL Versión 3 . . . . .	293
WebMasterEMail: establecer una dirección de correo electrónico para recibir informes de servidor seleccionados . . . . .	294
WebMasterSocksServer (Windows sólo): establecer un servidor socks para la rutina sendmail . . . . .	295
Welcome: especificar los nombres de los archivos de bienvenida . . . . .	295

<b>Avisos . . . . .</b>	<b>297</b>
Marcas registradas. . . . .	299

---

## Figuras

1.	Profundización . . . . .	97
2.	Túneles SSL . . . . .	121



---

## Acerca de este manual

Este prefacio describe el objetivo y los usuarios de destino de esta publicación, cómo esta organizada, las características de accesibilidad, las convenciones y terminología y los documentos relacionados.

---

## A quién va dirigido este manual

El manual *Guía de administración de Caching Proxy* se ha escrito para aquellos administradores de red y de sistemas expertos que estén familiarizados con sus sistemas operativos y con el suministro de servicios de Internet. No es necesario tener conocimientos previos de Caching Proxy.

Esta publicación no está diseñada para dar soporte a releases anteriores de Caching Proxy.

---

## Convenios y terminología que se utilizan en este manual

Esta documentación utiliza los siguientes convenios tipográficos y de teclas.

Tabla 1. Convenios que se utilizan en este manual

Convenio	Significado
<b>Negrita</b>	Cuando se hace referencia a interfaces gráficas de usuario (las GUI), se indican en negrita menús, elementos de los menús, etiquetas, botones, iconos y carpetas. También puede utilizarse para enfatizar nombres de mandatos que, de lo contrario, podrían confundirse con el texto de alrededor.
<b>Monoespaciado</b>	Indica texto que es necesario entrar en un indicador de mandatos. Además, el monoespaciado indica texto que aparece en la pantalla, ejemplos de código y extractos de archivos.
<i>Cursiva</i>	Indica valores de variable que debe proporcionar el usuario (por ejemplo, el usuario facilitará el nombre de un archivo para <i>NombreArchivo</i> ). La cursiva también indica énfasis y los títulos de manuales.
<b>Control-x</b>	Donde <i>x</i> es el nombre de una tecla, indica una secuencia de Control-carácter. Por ejemplo, Control-c significa pulsar y mantener pulsada la tecla Control mientras se pulsa la tecla c.
<b>Intro</b>	Se refiere a la tecla etiquetada con la palabra Intro o con la flecha hacia la izquierda.
<b>%</b>	Representa el indicador de shell de mandatos de Linux y UNIX para un mandato que no requiere privilegios root.
<b>#</b>	Representa el indicador de shell de mandatos de Linux y UNIX de un mandato que requiere privilegios root.
<b>C:\</b>	Representa el indicador de mandatos de Windows.
<b>Entrada de mandatos</b>	Cuando se le indique que “entre” o “emita” un mandato, escriba el mandato y luego pulse Intro. Por ejemplo, la instrucción “Entre el mandato <b>ls</b> ” significa que debe escribir <b>ls</b> en un indicador de mandatos y, después, pulsar Intro.
<b>[ ]</b>	Encierran elementos opcionales en las descripciones de sintaxis.
<b>{ }</b>	Encierran listas de las que debe elegirse un elemento en las descripciones de sintaxis.
<b> </b>	Separa elementos en una lista de opciones encerradas entre los signos { } (llaves) en las descripciones de sintaxis.



Tabla 1. Convenios que se utilizan en este manual (continuación)

Convenio	Significado
...	Los puntos suspensivos que aparecen en las descripciones de sintaxis indican que es posible repetir el elemento anterior una o más veces. Los puntos suspensivos que aparecen en los ejemplos indican que se ha omitido información en el ejemplo para una mayor brevedad.

## Accesibilidad

Las características de accesibilidad ayudan al usuario que tiene discapacidades físicas, como por ejemplo una movilidad restringida o una visión limitada, a utilizar satisfactoriamente los productos de software. Éstas son las principales características de accesibilidad en WebSphere Application Server, Versión 6.1:

- Puede utilizar el software lector de pantalla y un sintetizador de voz digital para oír lo que se visualiza en la pantalla. También puede utilizar el software de reconocimiento de voz como, por ejemplo, IBM ViaVoice para entrar datos y para navegar por la interfaz de usuario.
- Puede utilizar las características con el teclado en lugar de con el ratón.
- Puede configurar y administrar las características de Application Server utilizando editores de texto estándares o interfaces de línea de mandatos en lugar de las interfaces gráficas proporcionadas. Para obtener más información sobre la accesibilidad de características específicas, consulte la documentación sobre dichas características.

## Cómo enviar comentarios

Sus comentarios son importantes para ayudarnos a proporcionar la información más precisa y de la mayor calidad posible. Si desea hacer algún comentario sobre esta publicación o cualquier otra documentación acerca de Edge Components de WebSphere Application Server:

- Envíe sus comentarios por correo electrónico a [fsdoc@us.ibm.com](mailto:fsdoc@us.ibm.com). Asegúrese de incluir el nombre de la publicación, su número de pieza, la versión de WebSphere Application Server y, si procede, la ubicación específica del texto que está comentado (por ejemplo, un número de página o de tabla).

## Información relacionada

- *Conceptos, planificación e instalación de Edge Components*, GC31-6918-00
- *Guía de programación de Edge Components*, GC31-6919-00
- *Load Balancer Administration Guide*, GC31-6921-00
- *IBM WebSphere Edge Services Architecture*
- Sitio Web de inicio de IBM: [www.ibm.com/](http://www.ibm.com/)
- Sitio Web del producto IBM WebSphere Application Server: [www.ibm.com/software/webservers/appserv/](http://www.ibm.com/software/webservers/appserv/)
- Sitio Web de la biblioteca de IBM WebSphere Application Server: [www.ibm.com/software/webservers/appserv/library.html](http://www.ibm.com/software/webservers/appserv/library.html)
- Sitio Web con soporte a IBM WebSphere Application Server: [www.ibm.com/software/webservers/appserv/support.html](http://www.ibm.com/software/webservers/appserv/support.html)
- Centro de información de IBM WebSphere Application Server: [www.ibm.com/software/webservers/appserv/infocenter.html](http://www.ibm.com/software/webservers/appserv/infocenter.html)



- Centro de información de IBM WebSphere Application Server Edge Components:  
*[www.ibm.com/software/webservers/appserv/ecinfocenter.html](http://www.ibm.com/software/webservers/appserv/ecinfocenter.html)*



---

## Parte 1. Guía de iniciación con Caching Proxy

Esta parte proporciona una visión general del componente Caching Proxy, las instrucciones para utilizar los formularios de Configuración y Administración y el Asistente de configuración, las instrucciones para editar manualmente el archivo `ibmproxy.conf` y los procedimientos para iniciar y detener el servidor proxy.

Esta parte contiene los siguientes capítulos:

Capítulo 1, “Visión general”, en la página 3

Capítulo 2, “Utilización de los formularios de Configuración y Administración”, en la página 7

Capítulo 3, “Utilización del Asistente de configuración”, en la página 11

Capítulo 4, “Edición manual del archivo `ibmproxy.conf`”, en la página 13

Capítulo 5, “Inicio y detención de Caching Proxy”, en la página 15



---

## Capítulo 1. Visión general

Actuando como proxy de retorno o como proxy de reenvío, Caching Proxy intercepta las peticiones de datos de un cliente, recupera la información solicitada de las máquinas que alojan contenidos y devuelve esos contenidos al cliente. Habitualmente, las peticiones se refieren a documentos que se almacenan en máquinas de servidor web (también llamadas servidores de origen o sistemas principales que alojan contenidos) y se entregan mediante el HTTP (Protocolo de transferencia de hipertexto). No obstante, es posible configurar Caching Proxy de forma que maneje otros protocolos, tales como FTP (Protocolo de transferencia de archivos) y Gopher.

Antes de entregarlos al peticionario, el Caching Proxy almacena en una antememoria local los contenidos que pueden colocarse en antememoria. Entre los ejemplos de contenidos que pueden colocarse en antememoria se incluyen las páginas Web estáticas y los archivos JPS (JavaServer Pages) con fragmentos que se generan dinámicamente pero que cambian con poca frecuencia. La antememoria permite a Caching Proxy satisfacer las peticiones subsiguientes que se refieren a los mismos contenidos entregándolos directamente desde la antememoria local, lo cual es mucho más rápido que recuperarlos otra vez del sistema principal que aloja contenidos.

IMPORTANTE: Caching Proxy está disponible en todas las instalaciones de Edge Components, con las excepciones siguientes:

- Caching Proxy no está disponible en instalaciones de Edge Components que se ejecuten sobre procesadores Itanium 2 o AMD Opteron de 64-bits.
- Caching Proxy no está disponible para instalaciones de Edge Components de Load Balancer para IPv4 e IPv6.

---

## Configuraciones básicas de Caching Proxy

Las configuraciones básicas de proxy son el proxy de retorno y el proxy de reenvío.

### Proxy de retorno (valor por omisión)

Por omisión, Caching Proxy se configura como un servidor de proxy de retorno. En una configuración de proxy de retorno, un servidor proxy se encuentra entre uno o más servidores de contenido e Internet. Acepta peticiones de clientes Internet para el contenido almacenado en el sitio inicial del servidor proxy. El servidor proxy aparece ante el cliente como el servidor de origen (contenido); el cliente no sabe que la petición se ha enviado a otro servidor.

### Proxy de reenvío

Como alternativa, puede configurar Caching Proxy como servidor proxy de reenvío. Sin embargo, los navegadores de cliente deben configurarse individualmente para utilizar el proxy. En una configuración de proxy de reenvío, un servidor proxy se encuentra entre el cliente e Internet. Caching Proxy reenvía la petición de un cliente a los sistemas principales de contenido situados en Internet, guarda en antememoria los datos recuperados y los entrega al cliente.

Los siguientes cambios en el archivo de configuración `ibmproxy.conf` deben realizarse para habilitar la configuración del proxy de reenvío:

- Elimine el comentario de las líneas siguientes para especificar los protocolos que Caching Proxy reenviará.

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

- Habilite el túnel SSL para que las peticiones SSL se manejen en una configuración de proxy de reenvío.

```
SSLTunneling On
```

Para obtener más información en el túnel SSL, consulte “Configuración de túneles SSL” en la página 122.

- Habilite el método CONNECT utilizando la directiva Enable:

```
Enable CONNECT OutgoingPorts All
```

o bien

```
Enable CONNECT OutgoingPorts 443
```

para obtener información sobre el formato y las opciones disponibles para el método Enable CONNECT, consulte “Configuración de túneles SSL” en la página 122.

Realizar estos cambios permite que el proxy de reenvío haga lo siguiente:

- Responder a peticiones de clientes en los protocolos Hypertext Transfer Protocol o File Transfer Protocol.
- Responder a peticiones del motor de búsqueda gopher.
- Mantener la afinidad entre un cliente y su servidor actual mientras dure una transacción.

### Proxy transparente (sólo sistemas Linux)

Una variante del Caching Proxy de reenvío es un Caching Proxy transparente. En este rol, Caching Proxy realiza la misma función que un Caching Proxy de reenvío básico, pero lo hace sin que el cliente sea consciente de su presencia. La configuración de Caching Proxy transparente sólo está soportada en sistemas Linux.

Como sucede con el Caching Proxy de reenvío normal, el Caching Proxy transparente se instala en una máquina junto a Internet o la pasarela, pero los programas de navegador de cliente no están configurados para dirigir peticiones a un Caching Proxy de reenvío. Los clientes no son conscientes de que existe un proxy en la configuración. Sin embargo, un direccionador está configurado para interceptar peticiones de cliente y dirigir las al Caching Proxy transparente.

Para obtener información sobre la directiva de esta configuración, consulte “TransparentProxy — Habilitar el proxy transparente en Linux” en la página 291.

---

## Soporte de nuevas características

La publicación *Caching Proxy Administration Guide* Versión 6.1 incluye características recién documentadas y actualizaciones correctoras.

Las nuevas características más importantes son:

- Soporte de proxy de reenvío

Para obtener información sobre la configuración de un proxy de reenvío, consulte “Proxy de reenvío” en la página 3.

- Soporte de proxy transparente sólo para sistemas Linux

Para obtener información sobre la directiva de proxy transparente (de reenvío), consulte “TransparentProxy — Habilitar el proxy transparente en Linux” en la página 291.

- Soporte de métodos WebDAV, métodos Microsoft Exchange Server y métodos definidos por el usuario

Para obtener información sobre estos métodos, consulte “Habilitar métodos WebDAV, métodos MS Exchange y métodos definidos por el usuario” en la página 43.

- Directivas de filtros de compresión HTTP

Para obtener información sobre estas directivas, consulte

“CompressionFilterAddContentType — Especificar el tipo de contenido de la respuesta HTTP que desea comprimir” en la página 204 y

“CompressionFilterEnable — Habilitar el filtro de compresión para comprimir las respuestas HTTP” en la página 205.

- Directiva de Sin colocación en antememoria en peticiones de rango

Para obtener información sobre esta directiva, consulte “NoCacheOnRange — Especificar sin colocación en antememoria para peticiones de rango” en la página 249.

- Directiva de Optimizar correlación de reglas

Para obtener información sobre esta directiva, consulte “OptimizeRuleMapping — Optimizar el proceso de correlación de regla para las peticiones entrantes cuando aumenta el número de reglas” en la página 251.

- Directiva MapQuery

MapQuery es similar a la directiva Map y utiliza la vía de acceso y la serie de consulta para cumplir la regla.

Para obtener información sobre esta directiva, consulte “MapQuery — Cambiar las peticiones coincidentes a una nueva serie de petición, utilizando la serie de vía de acceso de petición y consulta para cumplir la regla” en la página 241.

- Directiva RuleCaseSense

Para obtener información sobre esta directiva, consulte “RuleCaseSense — Correlaciona peticiones de los URL de aplicación que no son sensibles a mayúsculas y minúsculas” en la página 278.

- Para sistemas AIX, se proporcionan directivas adicional para dar soporte a la tarjeta IBM 4960 PCI Cryptographic Accelerator Card.

Para obtener información sobre estas directivas, consulte “PKCS11DefaultCert, PKCS11DriverPath, PKCS11TokenPassword — Da soporte a la tarjeta IBM 4960 PCI Cryptographic Accelerator Card (sólo AIX)” en la página 255.

- Opción de expresión lógica en la directiva SSLCertificate

Para obtener información sobre la opción de expresión lógica en esta directiva, consulte “SSLCertificate — Especificar etiquetas de clave para certificados” en la página 284.

- Opciones adicionales disponibles para la regla Proxy o ProxyWAS

Caching Proxy proporciona directivas que requieren la coincidencia de patrones adicional en tiempo de ejecución. Para mejorar el rendimiento de Caching Proxy, puede utilizar estas directivas como opciones de la regla Proxy o ProxyWAS. Para obtener más información sobre estas opciones adicionales para la regla Proxy o ProxyWAS, consulte “Proxy: especificar los protocolos de proxy o el proxy de retorno” en la página 266.





---

## Capítulo 2. Utilización de los formularios de Configuración y Administración

Caching Proxy se facilita con formularios HTML que pueden servirse a los clientes que lo soliciten y utilizarse para configurar servidor proxy. Estos formularios ejecutan programas CGI que editan el archivo de configuración de servidor proxy local, `ibmproxy.conf`. Para utilizar estos formularios, el servidor proxy debe estar ejecutándose y estar configurado para pasar los formularios desde el directorio local donde residen.

Por omisión, el Caching Proxy se instala con las directivas `Pass` incluidas en el archivo `ibmproxy.conf` que permiten el acceso a los formularios de Configuración y Administración. Cuando un cliente solicita la página de inicio por omisión de este servidor proxy, se sirve `Frntpage.html`. Esta página contiene un enlace de hipertexto con la página de inicio de los formularios de Configuración y Administración, `wte.html`.

Los formularios de Configuración y Administración están protegidos y requieren la autenticación de cliente antes de que se sirvan. Para obtener las instrucciones sobre cómo establecer el ID y la contraseña del administrador, consulte “Establecimiento de la contraseña de administrador” en la página 9.

---

### Requisitos del navegador

Un navegador Web utilizado para acceder a los formularios de Configuración y Administración debe dar soporte a los siguientes elementos:

- *HTML 4.0*: todos los formularios están escritos siguiendo la especificación de HTML 4.0. El servidor Web debe dar soporte a HTML 4.0 y a los conjuntos de marcos.
- *Java 1.1 y JavaScript*: los applets se escriben siguiendo la especificación de Java 1.1. El navegador Web debe dar soporte a una máquina virtual Java que sea compatible con Java 1.1. Los applets son incompatibles con las máquinas virtuales Java que sean compatibles con la especificación de Java 2.0. Tanto JavaScript como Java deben estar habilitados.
- *256 colores*: la estación de trabajo en la que se ejecute el navegador Web debe dar soporte a 256 colores como mínimo.

Los navegadores **recomendados** son Mozilla y Firefox (para los sistemas Linux, UNIX y Windows) e Internet Explorer (para los sistemas Windows). Para obtener versiones específicas de los navegadores Mozilla, Firefox e Internet Explorer, consulte el siguiente sitio Web y siga los enlaces a la página Web del software soportado: <http://www.ibm.com/support/docview.wss?rs=180&uid=swg27006921>.

#### Notas:

1. En los sistemas PowerPC Linux de 64 bits, será imposible acceder a los formularios de Configuración y Administración con el navegador Mozilla, ya que no existe ningún SDK disponible para esta arquitectura. Como alternativa, puede acceder a los formularios de Configuración y Administración desde una máquina distinta con un navegador Web soportado.
2. Si se le solicita dos veces que inicie la sesión al iniciar la consola administrativa, es posible que el valor Java de Internet Explorer no esté establecido correctamente. Para corregir este valor en Internet Explorer,

---

## Acceso a los formularios de Configuración y Administración

Para acceder a los formularios de Configuración y Administración:

1. Asegúrese de que el servidor proxy esté en ejecución. Para obtener las instrucciones sobre cómo iniciar el servidor proxy, consulte el Capítulo 5, “Inicio y detención de Caching Proxy”, en la página 15.
2. Utilice un navegador HTTP para acceder a la página de inicio del servidor proxy (Frntpage.html) o la página de inicio de Configuración y Administración (wte.html).

**Nota:** Esta página depende de las normas de correlaciones reales del servidor proxy y puede variar con respecto a las páginas por omisión que se muestran entre paréntesis.

`http://su.nombre.servidor[:puerto]/[directorio]/[página.html]`

donde

- *su.nombre.servidor* es el nombre de vía de acceso completo del sistema principal (por ejemplo, `http://www.ibm.com/`).
  - *[:puerto]* Si el servidor proxy escucha las peticiones administrativas en un puerto distinto de 80, incluya el número de puerto después del nombre del servidor: `http://su.nombre.servidor:puerto`
  - *[/directorio]* La adición de un directorio en el URL depende de las normas de correlación.
  - *[/página.html]* Es necesario especificar la página HTML sólo si no está enumerada como una página de bienvenida. Para obtener información sobre las páginas de bienvenida, consulte “Definición de las páginas de bienvenida por omisión” en la página 52.
3. Pulse **Formularios de Configuración y Administración** para obtener los formularios de configuración del servidor. Se le solicitará que proporcione el nombre de usuario y la contraseña de administrador. Escriba un nombre de usuario y una contraseña autorizados. Se abrirá la ventana de cliente de la configuración de Caching Proxy.

**Notas:**

- a. El contenido del marco de navegación de la izquierda puede tardar varios segundos en cargarse después de que se visualice la página de inicio.
  - b. En los sistemas Windows 2003, es posible que las conexiones que requieren formularios de administración (scripts CGI) reciban una restauración antes de que se complete la conexión. Como resultado, se puede dar el caso de que los navegadores muestren mensajes de que no se ha recibido ningún dato o que no se ha visualizado la página. Para evitar este problema, aumente `MaxActiveThreads` a un valor mayor que 200 o `ConnThreads` a un valor mayor que 50 para resolver las conexiones de restauración. Consulte “`MaxActiveThreads`: especificar el número máximo de hebras activas” en la página 242 y “`ConnThreads`: especificar el número de hebras de conexión que se van a utilizar para la gestión de conexiones” en la página 205 para obtener más información sobre estas directivas.
4. El marco de navegación de la izquierda muestra las cinco categorías principales de los formularios de configuración:
    - **Configuración del proxy**

- Configuración de la antememoria
- Configuración del servidor
- Supervisor de actividad del servidor
- Configuración del plug-in

Pulse el puntero triangular que aparece a la izquierda de una cabecera para expandir la lista de formularios de configuración de esa categoría. Pulse un formulario para abrirlo. El formulario muestra los valores actuales de configuración (si los hay) en los campos de entrada; si no ha modificado la configuración desde la instalación, éstos son los valores por omisión.

- En cualquier formulario, especifique la información de configuración para esa función determinada. Todos los formularios proporcionan instrucciones para ayudarle a decidir qué modificaciones realizar. Para obtener más información, pulse el icono de ayuda, el signo de interrogación (?) que aparece en la parte superior de todos los formularios. Se facilitarán los siguientes enlaces:
  - **Ayuda para campos:** descripciones de los campos de los distintos paneles de pantalla
  - **Cómo puedo...:** pasos detallados para utilizar el formulario con el fin de realizar tareas específicas
  - **Índice:** índice de la información de ayuda
- Después de rellenar un formulario, pulse **Someter** para actualizar la configuración de servidor con los cambios realizados. El botón **Someter** está situado debajo de los campos de entrada de todos los formularios. Si no desea realizar los cambios indicados en el formulario, pulse **Restablecer** y los campos del formulario volverán a sus valores originales.
- Si pulsa **Someter** y se acepta la entrada, aparecerá el siguiente mensaje en el marco superior:  
 Los cambios de configuración solicitados se han completado satisfactoriamente  
  
 Si no se acepta la entrada, aparecerá un mensaje de error en el marco superior que indicará que no se han aceptado los valores.
- Para iniciar el servidor proxy, pulse el icono de reinicio del servidor 1) en el marco superior. Cuando el servidor proxy recibe el mandato restart, deja de aceptar peticiones de los clientes, aunque completa cualquier petición que ya esté en proceso. Después de volver a cargar el archivo de configuración, el proxy acepta peticiones de cliente de nuevo.

**Nota:** La modificación de ciertas directivas mediante los formularios de Configuración y Administración o la edición del archivo `bmproxy.conf` requiere que en lugar de reiniciar, detenga el servidor completamente y vuelva a iniciarlo de nuevo antes de que los cambios entren en vigor. Esas directivas aparecen enumeradas en la Tabla 6 en la página 177.

---

## Establecimiento de la contraseña de administrador

Después de instalar los paquetes de Caching Proxy, debe crear una identificación y contraseña del administrador para acceder a los formularios de Configuración y Administración. La configuración de servidor proxy por omisión autentica a los usuarios que soliciten los formularios de Configuración y Administración mediante el archivo de contraseñas `webadmin.passwd` situado en el directorio `/opt/ibm/edge/cp/server_root/protect/` de los sistemas Linux y UNIX o `\Archivos de programa\IBM\edge\cp\etc\` directory en los sistemas Windows. La instalación de paquetes no sobrescribe ningún archivo `webadmin.passwd` existente.

Utilice los siguientes mandatos para añadir una entrada de administrador al archivo `webadmin.passwd`:

- En sistemas Linux y UNIX:

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

Cuando se le solicite, proporcione al programa **htadm** un nombre de usuario, una contraseña y un nombre real para el administrador.

- En los sistemas Windows:

```
cd "\Archivos de programa\IBM\edge\cp\server_root\protect\"  
htadm -adduser webadmin.passwd"
```

Cuando se le solicite, proporcione al programa **htadm** un nombre de usuario, una contraseña y un nombre real para el administrador.

**Nota:** El nombre de usuario y contraseña de administrador son sensibles a las mayúsculas y minúsculas incluso si el sistema operativo no lo es. Asegúrese de entrar el nombre de usuario y contraseña exactos especificados mediante el mandato **htadm** al acceder a los formularios de Configuración y Administración.

Para obtener una descripción detallada del mandato **htadm**, consulte “Mandato **htadm**” en la página 169.

---

## Capítulo 3. Utilización del Asistente de configuración

El Asistente de configuración de Caching Proxy le permite configurar con rapidez un Caching Proxy instalado. Este programa sólo establece las directivas esenciales que son necesarias para modificar el comportamiento de Caching Proxy para actuar como sustituto. El servidor proxy puede requerir configuración adicional.

Para utilizar el Asistente de configuración de Caching Proxy:

1. Inicie el Asistente de configuración.

En los sistemas Windows: pulse **Inicio -> Programas -> IBM WebSphere -> Edge Components -> Caching Proxy -> Asistente de configuración**.

En los sistemas Linux y UNIX: especifique el mandato `/opt/ibm/edge/cp/cpwizard/cpwizard.sh`

2. Seleccione el puerto de red donde el servidor proxy va a escuchar las peticiones HTTP.
3. Escriba el nombre del servidor de contenido de destino.
4. Especifique el ID de usuario y la contraseña del administrador del servidor proxy.

### Notas:

1. El Asistente de configuración establece las siguientes directivas:

```
Port puerto
Proxy /* http://servidor de contenido
: puerto
```

2. Si el Asistente de configuración se utiliza para configurar el servidor proxy, debe crearse una norma de correlación en las peticiones de proxy recibidas mediante el puerto 443 para habilitar SSL. Para obtener más información, consulte "Definición de normas de correlación" en la página 44.

Ejemplos:

```
Proxy /* http://servidor contenido :443
```

o bien

```
Proxy /*
https://servidor contenido :443
```

**Limitaciones en los sistemas Linux:** los accesos directos del teclado no funcionan con el Asistente de configuración de Caching Proxy.



---

## Capítulo 4. Edición manual del archivo ibmproxy.conf

Caching Proxy puede configurarse manualmente, bien mediante la edición del archivo de configuración ibmproxy, bien mediante los formularios de Configuración y Administración.

- En los sistemas Linux y UNIX, el archivo ibmproxy.conf está situado en el directorio /etc/.
- En los sistemas Windows, el archivo ibmproxy.conf está situado en C:\Archivos de programa\IBM\edge\cp\etc\en\_US\.

El archivo de configuración está formado por las sentencias llamadas directivas. Para modificar la configuración, edite el archivo de configuración modificando las directivas y guarde los cambios. Puede utilizar prácticamente cualquier editor de texto como, por ejemplo, emacs y vi para editar el archivo de configuración.

**Nota:** No utilice el editor de archivos de texto que se incluye en Common Desktop Environment (CDE) de Solaris. El editor Solaris modifica en ocasiones el grupo propietario del archivo y cambia las propiedades del enlace de archivo de modo que los formularios de Configuración y Administración no pueden escribir en el archivo de configuración.

Los cambios del archivo de configuración entran en vigor al reiniciar el servidor, a menos que haya cambiado una de las directivas identificadas en la Tabla 6 en la página 177. Si ha modificado alguna de las directivas de esa lista, debe detener el servidor y volver a iniciarlo. Para obtener las instrucciones, consulte Capítulo 5, “Inicio y detención de Caching Proxy”, en la página 15.

El Apéndice B, “Directivas del archivo de configuración”, en la página 177 describe todas las directivas del archivo de configuración y proporciona información detallada sobre la sintaxis.





---

## Capítulo 5. Inicio y detención de Caching Proxy

Caching Proxy está diseñado para ejecutarse de forma continuada como un proceso en segundo plano con un mínimo de intervención por parte del operador. Generalmente, el servidor proxy se inicia durante el ciclo de arranque de la máquina y únicamente se detiene cuando el mantenimiento lo requiere. El servidor proxy puede iniciarse manualmente si es necesario. Asimismo, se puede pasar una instrucción de reinicio al servidor proxy, que detiene y reinicia el servidor proxy sin interrumpir conexiones de cliente activas.

---

### Arranque y cierre automático en sistemas Linux y UNIX

En los sistemas Linux y UNIX, se coloca un script de inicialización **ibmproxy** y los enlaces simbólicos asociados en los directorios `/etc/` adecuados cuando se instala Caching Proxy. A continuación, esos scripts se integran en las rutinas de arranque y cierre del sistema operativo. Puede modificar los valores de configuración del reinicio automático mediante la edición del script **ibmproxy** y la modificación de las opciones del mandato **ibmproxy**.

#### Nota: Límite del descriptor de archivo de Solaris

Es posible que el script de inicialización de Caching Proxy no pueda establecer satisfactoriamente el número máximo deseado de descriptors de archivo debido al límite en todo el sistema Solaris de los descriptors de archivo. Si el número máximo de todo el sistema es inferior al valor del script de inicialización de Caching Proxy, se utiliza el límite de todo el sistema. Puede modificar el límite de los descriptors de archivo para evitar problemas de rendimiento del proxy, que pueden ser el resultado de un valor demasiado bajo (inferior a 1024). Emita el mandato **ulimit** para visualizar el número de descriptors que estén disponibles en ese momento. Si el valor es inferior a 1024, aumente el límite de descriptor de archivo. Para incrementar el límite de descriptor de archivo a 1024, añada la siguiente línea al archivo `/etc/system`:

```
set rlim_fd_cur=0x400
```

#### Inhabilitación del arranque y cierre automático

Para inhabilitar el arranque y cierre automático:

- En los sistemas AIX, elimine el mandato **ibmproxy** del archivo de inicialización.
- En los sistemas HP-UX, elimine los enlaces con **ibmproxy**:
  - `/sbin/rc1.d/K154ibmproxy`
  - `/sbin/rc2.d/S880ibmproxy`
- En los sistemas Linux, elimine los enlaces simbólicos con `/etc/rc.d/init.d/ibmproxy` de los subdirectorios del nivel de ejecución.

En SUSE Linux, elimine los siguientes enlaces con **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

En Red Hat Linux, elimine los siguientes enlaces con **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

- En los sistemas Solaris, elimine el mandato **ibmproxy start** y sus dos scripts kill del siguiente modo:

- Suprimir S88ibmproxy del directorio /etc/rc2.d.

- Suprimir K54ibmproxy del directorio /etc/rc0.d.

- Suprimir K54ibmproxy del directorio /etc/rc1.d.

---

## Arranque manual en sistemas Linux y UNIX

Independientemente del método de arranque, el mandato **ibmproxy** se invoca finalmente, bien directamente desde el indicador de mandatos, bien desde dentro de un script. Para obtener una descripción detallada del mandato **ibmproxy**, consulte “Mandato ibmproxy” en la página 174. Sólo se ofrecen ejemplos de los argumentos utilizados con mayor frecuencia.

### En AIX:

- Para iniciar el servidor proxy para el entorno local por omisión mediante el mandato **startsrc**, especifique lo siguiente:

```
startsrc -s ibmproxy
```

- Para iniciar el servidor proxy para cualquier entorno local que no sea el entorno local por omisión mediante el mandato **startsrc**, especifique lo siguiente:

```
startsrc -s ibmproxy -e "LC_ALL=locale"
```

- Para iniciar el servidor proxy con los valores de tiempo de ejecución sin utilizar el mandato **startsrc**, especifique lo siguiente:

```
ibmproxy
```

### En HP-UX:

- Para iniciar el servidor proxy ejecutando el script de inicialización, especifique la siguiente información en un indicador de raíz:

```
/sbin/init.d/ibmproxy start
```

- Para iniciar el servidor proxy como un proceso en segundo plano sin ejecutar el script de inicialización, especifique la siguiente información en un indicador de raíz:

```
/usr/sbin/ibmproxy
```

- Para iniciar el servidor proxy como un proceso en primer plano sin ejecutar el script de inicialización, especifique la siguiente información en un indicador de raíz:

```
/usr/sbin/ibmproxy -nobg
```

### En Linux:

- Para iniciar el servidor proxy ejecutando el script de inicialización, especifique la siguiente información en un indicador de raíz:

```
/etc/rc.d/init.d/ibmproxy start
```

- Para iniciar el servidor proxy como un proceso en segundo plano sin ejecutar el script de inicialización, especifique la siguiente información en un indicador de raíz:

```
/usr/sbin/ibmproxy
```

- Para iniciar el servidor proxy como un proceso en primer plano sin ejecutar el script de inicialización, especifique la siguiente información en un indicador de raíz:

```
/usr/sbin/ibmproxy -nobg
```

- Para iniciar el servidor proxy mediante un archivo de configuración SQUID, *squidConfig.file*, especifique la siguiente información en un indicador de raíz:

```
squidConfig.file -r /etc/errors_icons.conf
```

donde el archivo *errors\_icons.conf* identifica qué iconos se deben utilizar para los tipos de archivo designados al examinar los directorios.

## En Solaris:

- Para iniciar el servidor proxy ejecutando el script de inicialización, especifique la siguiente información en un indicador de raíz:

```
/etc/init.d/ibmproxy start
```

- Para iniciar el servidor proxy como un proceso en segundo plano sin ejecutar el script de inicialización, especifique la siguiente información en un indicador de raíz:

```
/usr/sbin/ibmproxy
```

- Para iniciar el servidor proxy como un proceso en primer plano sin ejecutar el script de inicialización, especifique la siguiente información en un indicador de raíz:

```
/usr/sbin/ibmproxy -nobg
```

---

## Arranque como servicio Windows

Si Caching Proxy se instala como un servicio Windows, se inicia como cualquier otro servicio Windows:

1. Pulse **Inicio** → **Valores (para Windows 2000)** → **Panel de control**.
2. En la ventana **Panel de control**, efectúe una doble pulsación en **Herramientas administrativas** → **Servicios**.
3. En la ventana **Servicios**, resalte **Caching Proxy**.
4. Pulse **Inicio** para iniciar el servicio de Caching Proxy.

Si Caching Proxy se instala como servicio, puede configurarse para que se arranque automáticamente al iniciar Windows. En ese caso, no es necesario que inicie la sesión antes de que el proxy pueda servir las peticiones. Para que el proxy se inicie automáticamente:

1. Pulse **Inicio** → **Valores (para Windows 2000)** → **Panel de control**.
2. En la ventana **Panel de control**, efectúe una doble pulsación en **Herramientas administrativas** → **Servicios**.
3. En la ventana **Servicios**, resalte **Caching Proxy**.
4. Pulse el botón de selección **Automático** y, a continuación, pulse **Inicio** para iniciar el servicio de Caching Proxy automáticamente al iniciarse Windows.

### Renovación de la variable de entorno PATH

Si Caching Proxy está marcado como Iniciado en la ventana **Servicios**, pero el proxy no funciona, es posible que la máquina no se haya reiniciado después de instalar el proxy. Si el servicio de Caching Proxy está establecido para interactuar con el escritorio, un error durante el reinicio también puede provocar que aparezca el siguiente mensaje de error en un recuadro emergente: Error del catálogo de mensajes: No se puede cargar el catálogo de mensajes o no es válido

Se debe reiniciar la máquina para que el valor de la variable de entorno PATH se renueve en el registro de Windows. Si el registro no se renueva, es posible que la variable PATH muestre las vías de acceso de Caching Proxy y GSK7 correctas pero no funcione correctamente.

**Nota:** Existe un conflicto potencial para los sistemas Windows cuando Caching Proxy y otra aplicación como, por ejemplo, un sistema de archivos de red, se ejecutan como servicios. En ocasiones Caching Proxy no puede interpretar una vía de acceso que contenga una unidad remota propiedad de una aplicación del sistema de archivos que también se ejecute como un servicio.

El problema puede surgir si aparece la vía de acceso para el servicio de sistema de archivos antes de la vía de acceso del servicio de Caching Proxy en la variable de entorno PATH de Windows. La alteración de la variable PATH con el fin de situar los servicios de sistema de archivos próximos al final de la operación de establecimiento puede solucionar este problema.

Este problema no afecta a las unidades remotas controladas por las aplicaciones que no se ejecutan en servicios Windows. Por ejemplo, Caching Proxy puede acceder a las unidades compartidas en otras máquinas Windows que estén visibles mediante una red de área local (LAN).

---

## Arranque como aplicación Windows

### Utilización del menú Inicio

Al instalar Caching Proxy como una aplicación Windows, el procedimiento de instalación crea una entrada **Caching Proxy** como submenú del menú **Inicio**. Para iniciar Caching Proxy como una aplicación, pulse **Inicio -> Programas -> IBM WebSphere -> Edge Components -> Caching Proxy**.

Este proceso de arranque ejecuta el servidor proxy con los valores actuales de configuración. Si desea especificar otros valores durante el tiempo de arranque, utilice el procedimiento de arranque de mandatos (consulte el apartado siguiente).

### Utilización del indicador de mandatos

Para iniciar el servidor desde cualquier indicador de mandatos DOS o Windows, utilice el mandato **ibmproxy**. Si no ha cerrado y reiniciado Windows desde que instaló el servidor, especifique el nombre de vía de acceso completo de este mandato del siguiente modo (por omisión):

```
c:\Archivos de programa\IBM\edge\cp\bin\ibmproxy.exe
```

El mandato **ibmproxy** inicia el servidor con los valores actuales de configuración. Si no ha modificado la configuración del servidor desde la instalación, la configuración actual se basa en la información que haya especificado durante la instalación y en las opciones por omisión.

El mandato **ibmproxy** inicia el servidor como una aplicación, incluso si ha instalado Caching Proxy para que se ejecute como un servicio. Para forzar al servidor a que se ejecute como una aplicación, también puede especificar la opción de mandato **-noservice**. Las demás opciones de mandato modifican los valores de configuración durante el tiempo de ejecución.

---

## Inicio de varios servidores proxy

Se pueden ejecutar varias instancias del servidor proxy simultáneamente, pero cada instancia debe escuchar en un puerto independiente. En los sistemas AIX, sólo se puede iniciar una instancia con SRC. Se deben especificar archivos de configuración exclusivos para todas las instancias del servidor ya que el archivo de configuración identifica un número de puerto, que debe ser distinto para cada servidor en una máquina determinada. Para iniciar un instancia adicional del servidor (cuando uno como mínimo ya está en ejecución), especifique el siguiente mandato:

- En Linux y UNIX:  
`ibmproxy -r otro_archivo_configuración`
- En Windows:  
`ibmproxy -noservice -r otro_archivo_configuración`

donde *otro\_archivo\_configuración* es un archivo de configuración exclusivo.

Al iniciar varias instancias del servidor, registre el ID de proceso que se visualiza para cada instancia. Estos ID son necesarios para detener instancias específicas del servidor.

**Nota:** En los sistemas Linux que ejecuten varias instancias del servidor, el mandato **/etc/rc.d/init.d/ibmproxy stop** sólo detiene el último servidor que se haya iniciado. Las demás instancias se deben detener separadamente. Consulte “Cierre manual en sistemas Linux y UNIX” para obtener información relacionada.

---

## Cierre manual en sistemas Linux y UNIX

Para detener el servidor:

- Debe ser el usuario que ha empezado el proceso o el superusuario root.
- Debe utilizar el mismo método con el que se inició el servidor. La siguiente tabla enumera los métodos de inicio y los métodos de parada asociados.

Tabla 2. Métodos de inicio y de parada para los sistemas Linux y UNIX

Método de inicio	Método de parada
Desde /etc/inittab (en AIX)	Especifique <code>stopsrc -s ibmproxy</code>
Desde /sbin/init.d (en HP-UX)	Especifique <code>/sbin/init.d/ibmproxy stop</code>
Desde /etc/rc.d/init.d (en Linux)	Especifique <code>/etc/rc.d/init.d/ibmproxy stop</code>

Tabla 2. Métodos de inicio y de parada para los sistemas Linux y UNIX (continuación)

ibmproxy	<ol style="list-style-type: none"> <li>1. Busque el ID de proceso <b>ibmproxy</b> : en AIX, especifique <code>ps -aef   grep "ibmproxy"</code>. En Linux, especifique <code>ps -aux   grep ibmproxy   grep ID_servidor</code>. En Solaris y HP-UX, especifique <code>ps -ef   grep "ibmproxy"</code></li> <li>2. Detenga el proceso <b>ibmproxy</b>: especifique <code>kill id_proceso</code></li> </ol> <p>Para detener todos los servidores de esta máquina: especifique <code>killall ibmproxy</code></p>
ibmproxy -nobg	Especifique <code>ctrl-c</code>
ibmproxy -r -otro_archivo_configuración (en AIX)	Especifique <code>stopsrc -s ibmproxy -p id_proceso</code>
ibmproxy -r -otro_archivo_configuración (en Linux)	<ol style="list-style-type: none"> <li>1. Busque el ID de proceso <b>ibmproxy</b> : especifique <code>ps aux   grep ibmproxy   grep id_proceso</code></li> <li>2. Detenga el proceso <b>ibmproxy</b>: especifique <code>kill id_proceso</code></li> </ol>

**Nota:** Si ha iniciado el proxy transparente, descargue también la extensión de kernel de proxy transparente y las normas de cortafuegos asociadas después de detener el servidor de Caching Proxy. Como usuario root, especifique el siguiente mandato:

```
ibmproxy -unload
```

Para detener el servidor en un indicador de raíz, especifique:

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

## Limitaciones de los mandatos de cierre

Puede experimentar las siguientes limitaciones al utilizar los mandatos de cierre:

- **AIX, HP-UX y Linux**

En los sistemas AIX, HP-UX y Linux, los mandatos para detener el sistema de Caching Proxy en ocasiones sólo cierran el proceso de Caching Proxy. El mandato de AIX que ocasiona este comportamiento es el mandato **stopsrc -s ibmproxy**. El mandato de HP-UX y Linux que ocasiona este comportamiento es el mandato **ibmproxy -stop**.

Es posible que el proceso PACD, que se utiliza por el servidor LDAP, continúe en ejecución después de cerrar el servidor proxy. El proceso PACD se puede cerrar de modo seguro mediante el mandato **kill** tal como se muestra a continuación:

```
kill -15 PACD_process_ID
```

- **Solaris**

La emisión del mandato **ibmproxy -stop** en un sistema Solaris no tiene el mismo efecto que el mandato en los demás sistemas operativos. Debido a una limitación del código Solaris, no se ejecuta el paso de plug-in de terminación del servidor cuando se utiliza **ibmproxy -stop** en las plataformas Solaris.

Esta limitación tiene implicaciones para el software del servidor proxy y los plug-ins implementados por el cliente.

Es posible que el proceso PACD, que el servidor LDAP utiliza, continúe en ejecución después de que el servidor proxy se cierre. El proceso PACD se puede cerrar de modo seguro mediante el mandato **kill** tal como se muestra a continuación:

```
kill -15 PACD_process_ID
```

---

## Cierre manual en sistemas Windows

Puede detener el servidor Caching Proxy del mismo modo en que detiene los demás programas Windows.

Si el proxy se instala como un servicio:

1. Pulse **Inicio** -> **Valores (para Windows 2000)** -> **Panel de control**.
2. En la ventana **Panel de control**, efectúe una doble pulsación en **Herramientas administrativas** -> **Servicios**.
3. En la ventana **Servicios**, resalte **Caching Proxy**.
4. Pulse **Detener** para detener el servicio de Caching Proxy.

Si el proxy no está instalado como un servicio, lleve a cabo cualquiera de las acciones siguientes para detener Caching Proxy:

- Pulse el icono **x** que aparece en la esquina superior izquierda.
- Desde el menú **Archivo**, pulse **Salir**.
- Pulse **Alt + F4**.

---

## Reinicio después de los cambios de configuración

Después de modificar la configuración del servidor mediante los formularios de Configuración y Administración o la edición del archivo `ibmproxy.conf`, debe reiniciar el servidor antes de que los cambios entren en vigor. En la mayoría de los casos, puede reiniciar el servidor sin detenerlo previamente. Pero algunos valores no se renuevan mediante un simple reinicio. Para obtener más información, consulte la Tabla 6 en la página 177.

Para reiniciar el servidor sin detenerlo primero, pulse el botón **Reiniciar** en cualquier formulario de Configuración y Administración o escriba lo siguiente:  
`ibmproxy -restart`





---

## Parte 2. Configuración y ajuste del proceso de Caching Proxy

En este apartado se describe cómo el componente Caching Proxy interactúa con el sistema operativo, el hardware del sistema y la red. Asimismo, proporciona los procedimientos para configurar esta interacción. El administrador del sistema es quien gestiona generalmente estos elementos de la configuración del servidor proxy, que deben coordinarse con los recursos de red como, por ejemplo, las direcciones IP y los nombres de sistema principal, además de con los recursos del sistema, como la memoria disponible y los ciclos de la CPU.

Esta parte contiene los siguientes capítulos:

Capítulo 6, “Definición del servidor”, en la página 25

Capítulo 7, “Establecimiento de la propiedad de procesos”, en la página 29

Capítulo 8, “Gestión de conexiones”, en la página 31

Capítulo 9, “Ajuste del proceso del servidor proxy”, en la página 35



---

## Capítulo 6. Definición del servidor

Caching Proxy generalmente se ejecuta como un proceso en segundo plano en un sistema principal que esté configurado para actuar como un servidor de red. Este proceso está asociado con (*enlazado con*) una o todas las direcciones IP (Protocolo Internet) activas del sistema principal. Puede escuchar varios protocolos de Internet como, por ejemplo, FTP y HTTP en puertos específicos y realizar acciones a partir de estas peticiones de acuerdo con su configuración de comportamiento. Para obtener más información, consulte Parte 3, “Configuración del comportamiento de Caching Proxy”, en la página 39.

Por omisión, Caching Proxy adopta el nombre del sistema principal. Puede sobrescribir este comportamiento por omisión especificando deliberadamente un nombre de sistema principal para el servidor proxy. Para enlazar Caching Proxy con una dirección IP específica, el nombre de sistema principal del servidor proxy debe modificarse para que sea idéntica a esa dirección IP.

**Nota:** En el caso de que el servidor proxy intente enlazarse con una dirección IP, y se dé el caso de que ese nombre de sistema principal no esté establecido en una dirección IP disponible, el enlace no se realizará satisfactoriamente y el servidor proxy escuchará en todas las direcciones IP disponibles.

El nombre de sistema principal del servidor proxy no tiene un efecto sobre cómo se resuelve el tráfico de clientes. El servidor proxy no compara su propio nombre de sistema principal con el valor del argumento de nombre de sistema principal de la cabecera de la petición HTTP. El nombre de sistema principal del servidor proxy se incorpora ocasionalmente en las páginas de contenido local generadas dinámicamente como, por ejemplo, los mensajes de error. También se devuelve al cliente solicitado como el valor del argumento Via de la cabecera HTTP.

El servidor proxy puede configurarse para que sustituya el nombre de sistema principal del cliente que lo solicite por el nombre de sistema principal del servidor proxy antes de pasar la petición al servidor de destino. Esta acción fuerza al servidor de destino a mantener el canal de comunicación a través del servidor proxy, en lugar de establecer una conexión directa con el cliente.

Defina el proceso del servidor proxy especificando la ubicación física de los archivos del servidor proxy en el sistema principal, el nombre con el que el servidor proxy se refiere a sí mismo y los puertos en los que escucha como valores de las directivas ServerRoot, Hostname y Port. Si el sistema principal tiene varias direcciones IP, se puede enlazar el servidor proxy con una dirección específica estableciendo el valor de la directiva BindSpecific en On y el valor de la directiva Hostname igual al valor de la dirección IP.

Un puerto de administración proporciona un método de acceso a los formularios de Configuración y Administración y mantenimiento del servidor. Para proporcionar el acceso al servidor proxy mediante el puerto de administración, especifique un valor de la directiva AdminPort. Las peticiones recibidas en el puerto de administración no se colocan en cola con las peticiones recibidas en el puerto estándar. Se pueden escribir normas de correlación para permitir el acceso a los formularios de Configuración y Administración a través de este puerto.

Cuando se habilita la directiva BindSpecific, Caching Proxy se enlaza con el puerto especificado por la directiva Port junto con la dirección IP derivada del valor de la directiva Hostname. El puerto especificado por la directiva AdminPort se enlaza con todas direcciones IP disponibles en el sistema.

Para sobrescribir el nombre por omisión del servidor que se esté ejecutando, como, por ejemplo, IBM-PROXY o IBM\_HTTP\_SERVER, especifique un valor para la directiva HeaderServerName. Este valor se especifica en el campo del servidor de respuestas HTTP.

Para mejorar el rendimiento del proxy, el valor de la directiva PureProxy puede establecerse en on. Esto inhabilita completamente todas las funciones de colocación en antememoria.

---

## Directivas asociadas

Las siguientes directivas definen el proceso del servidor proxy:

- “Hostname: especificar el nombre de dominio plenamente cualificado o dirección IP del servidor” en la página 226
- “ServerRoot: especificar el directorio donde se instala el programa servidor” en la página 281
- “HeaderServerName: especificar el nombre del servidor proxy devuelto en la cabecera HTTP” en la página 226
- “BindSpecific: especificar si el servidor se enlaza a una dirección IP o a todas” en la página 191
- “Port: especificar el puerto donde el servidor escucha las peticiones” en la página 257
- “AdminPort: especifica el puerto para solicitar las páginas administrativas o formularios” en la página 187
- “PureProxy: inhabilitar un proxy dedicado” en la página 271

Para obtener más información, consulte el Capítulo 4, “Edición manual del archivo ibmproxy.conf”, en la página 13.

---

## Formularios de Configuración y Administración

Los siguientes formularios de Configuración y Administración editan los valores de las directivas asociadas:

- **Configuración de servidor → Configuración básica → Nombre de sistema principal**
- **Configuración de servidor → Configuración básica → Raíz de servidor**
- **Configuración de servidor → Configuración básica → Número de puerto por omisión**
- **Configuración de servidor → Configuración básica → Número de puerto de administrador**
- **Configuración de servidor → Configuración básica → Opciones de enlace**
- **Configuración de proxy → Rendimiento de proxy → Ejecutar como proxy puro**

**Nota:** No se pueden utilizar los formularios de Configuración y Administración para editar la directiva HeaderServerName.

Para obtener más información, consulte el Capítulo 2, “Utilización de los formularios de Configuración y Administración”, en la página 7.



---

## Capítulo 7. Establecimiento de la propiedad de procesos

Cuando un usuario distinto del superusuario root inicia Caching Proxy, aquél mantiene la propiedad de todos los procesos asociados con el servidor proxy. No obstante, si el superusuario root inicia Caching Proxy, una función de ID de usuario establecida en el servidor proxy lee las directiva UserId y GroupId del archivo ibmproxy.conf y modifica la propiedad de los procesos del usuario y grupo especificados. Esta acción se lleva a cabo para limitar el acceso a archivos y proteger el sistema. Si modifica las directivas UserId o GroupId, debe actualizar la propiedad y los permisos de los directorios de anotaciones cronológicas y otros archivos como, por ejemplo, una lista de control de acceso (ACL), que utiliza el servidor proxy.

Establezca la propiedad del proceso del servidor proxy especificando la identificación de usuario, identificación de grupo y ubicación del archivo donde el ID de proceso está registrado como valores de las directivas UserID, GroupID y PidFile.

Para forzar que proceso del servidor proxy se ejecute como un proceso en primer plano, establezca el valor de la directiva NoBG en on.

### En sistemas Linux:

En los sistemas Linux, sólo a los procesos y hebras responsables de la escucha de conexiones se les modificará la propiedad. Los procesos y hebras responsables de las demás actividades del flujo de trabajo seguirán siendo propiedad del usuario root. Todos los procesos y hebras reciben los números de ID de proceso (PID). El mandato **ps** enumera todos los ID de proceso, independientemente de si están o no asociados con un proceso o hebra.

**Nota:** En algunos kernels de Linux, es posible que Caching Proxy genere el mensaje de error siguiente en su archivo de anotaciones cronológicas de error:

```
Cannot init groups for user nobody, errno: 1
```

Puede ignorar este mensaje de error, porque no afecta a la operación normal de Caching Proxy. Además existe una solución para evitar el mensaje de error, exportando las variables de entorno siguientes antes de iniciar Caching Proxy:

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

---

## Directivas asociadas

Las siguientes directivas establecen la propiedad de procesos del servidor proxy:

- “UserId: especificar el ID de usuario por omisión” en la página 292
- “GroupId: especificar el ID de grupo” en la página 225
- “NoBG: ejecutar el proceso de Caching Proxy en primer lugar” en la página 247
- “PidFile (Linux y UNIX sólo): especificar el archivo donde se va a almacenar el ID de proceso de Caching Proxy” en la página 255

Para obtener más información, consulte el Capítulo 4, “Edición manual del archivo ibmproxy.conf”, en la página 13.

---

## Formularios de Configuración y Administración

Los siguientes formularios de Configuración y Administración editan los valores de las directivas asociadas:

- Configuración de servidor -> Configuración básica -> UserID
- Configuración de servidor -> Configuración básica -> GroupID
- Configuración de servidor -> Configuración básica -> Ubicación de archivo de ID de proceso

**Nota:** No se pueden utilizar los formularios de Configuración y Administración para editar la directiva NoBG.

Para obtener más información, consulte el Capítulo 2, “Utilización de los formularios de Configuración y Administración”, en la página 7.



---

## Capítulo 8. Gestión de conexiones

Caching Proxy genera una nueva hebra para manejar cada una de las peticiones de cliente. Si no existen hebras disponibles, el servidor proxy mantiene las peticiones hasta que están disponibles más hebras. A medida que aumenta el número de hebras activas, el servidor proxy consume más memoria. Especifique el número máximo de hebras activas como valor de la directiva `MaxActiveThreads`.

El registro de reserva de escucha es el número de peticiones pendientes para las conexiones de cliente que el servidor anota cronológicamente antes de rechazar las conexiones con nuevos clientes. Debe basar este valor en el número de peticiones que el servidor puede procesar en pocos segundos. Un servidor debe responder a una conexión de cliente antes de que caduque. Especifique el número máximo de conexiones que se pueden mantener en el registro de reserva como el valor de la directiva `ListenBacklog`.

El servidor proxy puede mantener las conexiones persistentes de cliente/servidor. Con una conexión persistente, el servidor acepta varias peticiones del cliente y envía las respuestas a través de la misma conexión TCP/IP. El uso de conexiones persistentes reduce la latencia de los clientes y la carga de CPU del servidor proxy, con un coste mínimo de un pequeño aumento de la memoria del servidor. No sólo aumenta el rendimiento global cuando el servidor no establece una conexión TCP/IP independiente para cada petición y respuesta, sino que la conexión TCP/IP puede utilizarse con mayor eficacia cuando la conexión es persistente.

La agrupación de conexiones de la parte servidor aplica las ventajas de las conexiones persistentes en la parte servidor, lo que permite la reutilización de las conexiones existentes entre un servidor proxy y los servidores de origen. Todas las conexiones reutilizadas guardan tres paquetes TCP: dos paquetes de protocolo de enlace en tres direcciones para configurar la conexión y uno para cerrarla. Las ventajas de una agrupación de conexiones de la parte servidor incluyen:

- Menos congestión de la red mediante la maximización de apertura y cierre de las conexiones
- Menos tiempo de la CPU invertido en direccionadores, clientes y servidores
- Menos memoria utilizada en los clientes y servidores
- En las faltas de coincidencia, mayor respuesta del proxy al evitar la apertura y cierre de conexiones

**Nota:** La agrupación de conexiones sólo se recomienda en un entorno controlado. Puede degradar el rendimiento en aquellos lugares donde los servidores no son compatibles con HTTP 1.1. Tenga en cuenta que es crítico que los servidores de origen estén configurados correctamente. A continuación aparece un ejemplo sencillo del archivo de configuración de Apache 1.3.19:

- `#KeepAlive`: especificar si se deben permitir las conexiones persistentes (más de una petición por conexión). Establecer en `Off` para desactivar#
- `KeepAlive On`
- `#MaxKeepAliveRequests`: número máximo de peticiones permitidas durante una conexión persistente. Establecer en `0` para permitir una cantidad ilimitada. Especificar este número alto para un máximo rendimiento#

- Max KeepAliveRequests 0
- #KeepAliveTimeout: número de segundos que se debe esperar a la siguiente petición del mismo cliente de la misma conexión#
- KeepAliveTimeout 240

Estos valores mantienen las conexiones con los servidores Web abiertas siempre y cuando se utilicen y permitan que el proxy, en lugar del servidor de origen, gestione las conexiones. Por lo tanto, las conexiones se agrupan únicamente si es necesario.

Cuando la agrupación de conexiones de la parte servidor está habilitada, se agrupan las conexiones HTTP con los servidores de origen. Las conexiones SSL también se agrupan en las configuraciones donde la directiva SSLEnable del proxy está establecida en on.

Configure cómo mantener la agrupación de conexiones especificando el número máximo de sockets desocupados que se deben conservar por servidor en cualquier momento, el periodo durante el cual el servidor espera antes de finalizar una conexión persistente desocupada y el intervalo durante el cual la recogida de basura busca conexiones caducadas (el valor por omisión es dos minutos).

Defina el periodo de tiempo durante el cual las distintas conexiones permaneces abiertas como valores de las directivas InputTimeout, OutputTimeout, PersistTimeout, ReadTimeout y ScriptTimeout.

---

## Directivas asociadas

Las siguientes directivas gestionan las conexiones con el proceso del servidor proxy:

- “MaxActiveThreads: especificar el número máximo de hebras activas” en la página 242
- “ConnThreads: especificar el número de hebras de conexión que se van a utilizar para la gestión de conexiones” en la página 205
- “ListenBacklog: especificar el número de conexiones de cliente del registro de reserva de escucha que puede transportar el servidor” en la página 235
- “ProxyPersistence: permitir las conexiones persistentes” en la página 269
- “MaxPersistRequest: especificar el número máximo de peticiones que se van a recibir en una conexión persistente” en la página 243
- “ServerConnPool: especificar la agrupación de conexiones con los servidores de origen” en la página 280
- “MaxSocketPerServer — Especificar el número máximo de sockets desocupados abiertos para el servidor” en la página 244
- “ServerConnTimeout: especificar el periodo máximo de inactividad” en la página 280
- “ServerConnGCRun: especificar el intervalo durante el que se ejecuta la hebra de recogida de basura” en la página 280
- “PersistTimeout: especificar el tiempo de espera para que el cliente envíe otra petición” en la página 254
- “InputTimeout: especificar el tiempo de espera de la entrada” en la página 231
- “ReadTimeout: especificar el límite de tiempo de una conexión” en la página 273
- “OutputTimeout: especificar el tiempo de espera de la salida” en la página 251

- “ScriptTimeout: especificar el valor de tiempo de espera de los scripts” en la página 278

Para obtener más información, consulte el Capítulo 4, “Edición manual del archivo ibmproxy.conf”, en la página 13.

---

## Formularios de Configuración y Administración

Los siguientes formularios de Configuración y Administración editan los valores de las directivas asociadas:

- Configuración de servidor → Gestión del sistema → Rendimiento → Número máximo de hebras activas
- Configuración de servidor → Gestión del sistema → Rendimiento → Tamaño de registro de reserva de escucha
- Configuración de proxy → Rendimiento de proxy → Tamaño de registro de reserva de escucha
- Configuración de servidor → Gestión del sistema → Rendimiento → Tamaño de registro de reserva de escucha
- Configuración de servidor → Gestión del sistema → Rendimiento → Tiempo de espera persistente
- Configuración de servidor → Gestión del sistema → Tiempos de espera → Tiempo de espera de entrada
- Configuración de servidor → Gestión del sistema → Tiempos de espera → Tiempo de espera de lectura
- Configuración de servidor → Gestión del sistema → Tiempos de espera → Tiempo de espera de salida
- Configuración de servidor → Gestión del sistema → Tiempos de espera → Tiempo de espera de script
- Configuración de servidor → Gestión del sistema → Tiempos de espera → Tiempo de espera persistente

### Notas:

1. No se pueden utilizar los formularios de Configuración y Administración para editar las directivas ServerConnPool, MaxsocketPerServer, ServerConnTimeout y ServerConnGCRUnl.
2. La directiva PersistTimeout puede editarse desde el formulario **Configuración de servidor → Gestión del servidor → Rendimiento** o **Configuración de servidor → Gestión del servidor → Tiempos de espera**.

Para obtener más información, consulte el Capítulo 2, “Utilización de los formularios de Configuración y Administración”, en la página 7.



---

## Capítulo 9. Ajuste del proceso del servidor proxy

Puede mejorar notablemente el rendimiento de Caching Proxy configurando y ajustando el sistema correctamente. A continuación aparecen sugerencias para mejorar la configuración y el ajuste.

---

### Establecimiento de las directivas relacionadas con el rendimiento

Las siguientes directivas afectan al rendimiento del proceso del servidor proxy significativamente.

- “PureProxy: inhabilitar un proxy dedicado” en la página 271. Esta característica mejora el rendimiento del sistema inhabilitando la colocación en antememoria completamente.
- “ProxyPersistence: permitir las conexiones persistentes” en la página 269. Esta característica permite a los clientes y servidores mantener las conexiones abiertas. Las conexiones persistentes reducen el tiempo de retardo de las peticiones de documentos del servidor proxy, aunque necesitan un aumento del ancho de banda de red además de una hebra de servidor dedicada en todas las conexiones. Evite las conexiones persistentes si la configuración limita el número de hebras disponibles.

Los campos de formularios de Configuración y Administración editan los valores de las directivas asociadas:

- **Configuración de proxy -> Rendimiento de proxy: ejecutar como proxy puro**
- **Configuración de proxy -> Rendimiento de proxy: tamaño de registro de reserva de escucha**

---

### Examinar el resto de aplicaciones

Examine los servicios o daemons que se estén ejecutando en el sistema y elimine aquellos que no sean necesarios para aumentar la memoria disponible y los ciclos de la CPU. Por ejemplo, si el sistema está ejecutando un servidor Web que únicamente sirve unas pocas páginas Web, se le recomienda que use Caching Proxy como el único servidor Web. Inhabilite los demás servidores Web del siguiente modo:

- En AIX: Examine /etc/inittab
- En Linux: Examine /etc/rc.d/rcx.d del nivel de ejecución por omisión del sistema (generalmente 2)
- En HP-UX y Solaris: Examine /etc/rcx.d del nivel de ejecución por omisión del sistema (generalmente 2).
- En sistemas Windows:
  1. Pulse **Inicio -> Configuración (para Windows 2000) -> Panel de control -> Herramientas de administración -> Servicios**.
  2. Revise los servicios que no sean necesarios pero estén establecidos en Automático.
  3. Modifique el tipo de arranque para esos servicios de Automático a Manual.

---

## Verifique el espacio de paginación

Asegúrese de que el sistema tiene el suficiente espacio de paginación para que opere correctamente. El sistema necesita el doble de espacio de paginación que la memoria física. Si es posible, amplíe el espacio de paginación a varias unidades físicas. Por ejemplo, un servidor Netfinity 5000 con 512 MB de memoria y cinco unidades SCSI necesita 1 GB de espacio de paginación total con 200 MB en todas las unidades aproximadamente.

---

## Ajuste el sistema de archivos

Caching Proxy crea y destruye varios archivos durante su funcionamiento. Si el servidor proxy registra los accesos (mediante las anotaciones cronológicas de acceso, anotaciones cronológicas de acceso proxy o anotaciones cronológicas de acceso de antememoria), dirija estas anotaciones cronológicas a sus propios sistemas de archivos de modo que, si las anotaciones cronológicas crecen de forma inesperada, no utilicen el espacio diseñado para otra función (por ejemplo, la antememoria).

---

## Ajuste de la configuración TCP/IP

Caching Proxy es sensible a las modificaciones de las configuraciones TCP/IP. La reducción de los valores TCP/IP de cualquier sistema operativo puede provocar que el servidor proxy actúe de forma inesperada. Para ser más específicos, si los valores TCP/IP se establecen demasiado bajos, los clientes que se conectan al servidor proxy o los servidores de origen a los que se conecta el proxy pueden restablecer las conexiones. Esto es particularmente cierto en el caso de los clientes que se conectan al servidor proxy mediante una conexión de bajo ancho de banda (56700 bps o inferior). Proceda con cuidado si se deben reducir los parámetros TCP/IP.

---

## Ajuste el intervalo tiempo de espera de TCP para los entornos de carga alta (HP-UX, Linux, Solaris, Windows)

El intervalo de tiempo de espera de TCP especifica la duración de tiempo que un socket espera un paquete FIN del remitente antes de cerrarse a la fuerza. En los entornos de carga alta, es posible que el servidor proxy parezca atascarse si un gran número de sockets permanecen suspendidos en el estado TIME\_WAIT después de que se cierran las conexiones. La reducción del intervalo de tiempo de espera de TCP hará que descienda el número de sockets suspendidos y, en los entornos de carga alta, es posible que evite que el servidor proxy aparente atascarse. Se recomienda que este intervalo se establezca en 5 segundos.

Para establecer el intervalo de tiempo de espera de TCP en 5 segundos

- En HP-UX:

Emita el mandato siguiente:

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

Utilice el programa de utilidad "sam" para establecer el parámetro de kernel `max_thread_proc` en 2048 como mínimo.

**Nota:** Asimismo considere el ajuste de los siguientes parámetros de kernel: `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.

- En Linux:

Emita los siguientes mandatos:

```
echo "1024 61000" > /proc/sys/net/ipv4/ip_local_port_range  
echo "5" > /proc/sys/net/ipv4/tcp_fin_timeout
```

- En Solaris:

Emita el mandato siguiente:

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

Edite el archivo /etc/system para que se lea del siguiente modo:

```
set tcp:tcp_conn_hash_size=8129
```

- En Windows:

debe crearse una entrada de registro para establecer un intervalo de tiempo de espera TCP. Consulte la documentación de Windows para obtener más información.

---

## Ajuste del kernel de Linux

Varios límites del kernel de Linux son bajos y pueden modificarse. Algunos pueden modificarse mediante el sistema de archivos /proc mientras que los demás requieren la recompilación del kernel.

Nota: el sistema de archivos /proc es virtual, es decir, no existe físicamente en el disco. Por el contrario, actúa como interfaz en el kernel de Linux. Como no existe, los valores de entrada se pierden durante el reinicio. Por lo tanto, incluya los cambios que desea realizar en el sistema de archivos /proc en el archivo /etc/rc.d/rc.local de RedHat o en el archivo /etc/rc.config file de SUSE. Los cambios siempre se activan durante el reinicio.

A continuación se incluyen algunas recomendaciones:

- El valor máximo de descriptor de archivos es 4096 por omisión. Se puede modificar añadiendo la información siguiente al archivo rc.local:  

```
echo 32768 > /proc/sys/fs/file-max
```
- El valor máximo de inode es 16384 por omisión. Se puede modificar añadiendo la información siguiente al archivo rc.local:  

```
echo 65536 > /proc/sys/fs/inode-max
```
- El rango de puertos de TCP y UDP es 1024 – 4999 por omisión. Este valor se puede cambiar a 32768 – 61000 añadiendo lo siguiente al archivo rc.local:  

```
echo 32768 61000 > /proc/sys/net/ipv4/ip_local_port_range
```
- Por omisión, el número de tareas permitidas es de 512. Si se ejecutan demasiadas tareas, esto repercute en el número máximo de hebras de un proceso. Se puede incrementar este límite a 2048 modificando el valor de NR\_TASKS del archivo *YourKernelSource*/include/linux/tasks.h.
- Asimismo, cambie el valor de MIN\_TASKS\_LEFT\_FOR\_ROOT a 24. Debe recompilar el kernel para que este cambio entre en vigor.

Si decide volver a crear el kernel, habilite sólo aquellas opciones que necesite definitivamente. Si no necesita un daemon específico, no lo ejecute.

---

## Ajuste las variables de ajuste de hebras de AIX

En los sistemas AIX, el rendimiento de Caching Proxy puede mejorarse utilizando las hebras de ámbito de sistema y permitiendo que las hebras utilicen varios almacenamientos dinámicos. El rendimiento está relacionado con la capacidad de multiproceso del sistema operativo y la planificación de hebras del sistema operativo subyacente. Se puede obtener la mejora del rendimiento estableciendo las siguientes variables de ajuste de hebra del modo siguiente:

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

Puede establecer estas variables de entorno antes de iniciar `/usr/sbin/ibmproxy`, o bien puede añadirlas a `/etc/rc.ibmproxy` si utiliza **startsrc -s ibmproxy** para iniciar el servidor proxy. Después de ajustar estas variables de ajuste de hebras, la mejora del rendimiento será más evidente en los sistemas SMP. No obstante, en algunos casos, la mejora también puede ser evidente en sistemas de un solo procesador.

**Nota:** Para obtener más información, consulte la documentación del sistema operativo AIX para obtener detalles sobre las variables de ajuste de hebras.



---

## Parte 3. Configuración del comportamiento de Caching Proxy

Este apartado describe cómo el componente Caching Proxy responde a las peticiones de cliente y proporciona los procedimientos para configurar este comportamiento. Un administrador Web es quien gestiona generalmente estos elementos de la configuración de servidor proxy, que no afectan a los demás procesos del sistema principal u otros sistemas de la red.

Esta parte contiene los siguientes capítulos:

Capítulo 10, “Gestionar el proceso de peticiones”, en la página 41

Capítulo 11, “Gestión del envío del contenido local”, en la página 51

Capítulo 12, “Gestión de las conexiones FTP”, en la página 55

Capítulo 13, “Personalización del proceso del servidor”, en la página 59

Capítulo 14, “Configuración de las opciones de cabecera”, en la página 69

Capítulo 15, “Acerca de la interfaz de programas de aplicación”, en la página 71



---

## Capítulo 10. Gestionar el proceso de peticiones

Cuando Caching Proxy recibe la petición de un cliente, realiza la acción especificada en el campo de método del objeto especificado del campo URL, si se ha habilitado el método solicitado. El servidor proxy resuelve el URL de acuerdo con un conjunto de normas de correlación definidas por el administrador. Es posible que estas normas de correlación indiquen a Caching Proxy que actúe como un servidor Web y recupere el objeto del sistema de archivos local o que actúe como un servidor proxy y recupere el objeto de un servidor de origen.

En este capítulo se describe cómo habilitar los métodos, definir las normas de correlación y configurar un servidor proxy sustituto.

---

### Habilitación de métodos HTTP/FTP

Las peticiones de cliente dirigidas al servidor incluyen un campo de método que indica la acción que el servidor va a realizar en el objeto especificado.

A continuación aparece una lista de métodos a los que el servidor proxy da soporte y una descripción de cómo responde a una petición que contenga el método cuando éste está habilitado.

**Nota:** Algunos métodos son los mismos que para HTTP y para las peticiones FTP. La habilitación de estos métodos para HTTP también los habilita para FTP.

#### CONNECT

El método CONNECT permite transmitir a través del túnel las peticiones y respuestas mediante el servidor proxy. Sólo se aplica a configuraciones de proxy de reenvío.

Para obtener información sobre el formato y las opciones disponibles para el método Enable CONNECT, consulte “Configuración de túneles SSL” en la página 122.

#### DELETE

El servidor proxy suprime el objeto identificado por el URL. DELETE permite a los clientes borrar los archivos de Caching Proxy. Utilice las configuraciones de protección de servidor para definir quién puede utilizar DELETE y en qué archivos. Para obtener más detalles, consulte Capítulo 25, “Configuraciones de protección del servidor”, en la página 115.

**GET** El servidor proxy devuelve cualquier dato identificado por el URL. Si el URL hace referencia a un programa ejecutable, el proxy devuelve la salida del programa. Este método se puede manejar a través de conexiones persistentes.

#### HEAD

El servidor proxy sólo devuelve la cabecera del documento HTTP identificada por el URL sin el cuerpo del documento.

#### OPTIONS

El servidor proxy devuelve información sobre las opciones de comunicaciones de la cadena de petición-respuesta identificada por el URL.

Este método permite que un cliente determine las opciones y requisitos asociados con un objeto o las posibilidades de un servidor sin necesidad de actuar sobre el objeto o recuperarlo.

**POST** La petición contiene datos y un URL. El servidor proxy acepta los datos contenidos en la petición como un nuevo subordinado del recurso identificado en el URL, que procesa los datos. El recurso puede ser un programa que acepte datos, una pasarela de algún otro protocolo o un programa independiente que acepte anotaciones.

El método POST se designa para manejar la anotación de recursos existentes. Entre los ejemplos se incluye el envío de un mensaje a un tablón de anuncios, un grupo de noticias o lista de correo, o recursos de grupo similares; el paso de un bloque de datos, por ejemplo, de un formulario a un programa de manejo de datos, o la ampliación de una base de datos a través de una operación **añadir**. En Caching Proxy, el método POST se utiliza para procesar los formularios de Configuración y Administración.

Este método se puede manejar a través de conexiones persistentes.

**PUT** La petición contiene datos y un URL. El servidor proxy almacena los datos en el recurso identificado en el URL. Si el recurso ya existe, PUT lo sustituye con los datos contenidos en la petición. Si el recurso no existe, PUT lo crea y lo llena con los datos contenidos en la petición. Este método se puede manejar a través de conexiones persistentes.

La habilitación del método PUT permite que los archivos se escriban en Caching Proxy mediante HTTP y FTP. Como PUT permite a los clientes escribir en Caching Proxy, es necesario que utilice las configuraciones de protección de servidor para definir quién puede utilizar PUT y los archivos en los que se puede utilizar PUT. (Consulte el Capítulo 25, “Configuraciones de protección del servidor”, en la página 115.)

#### **TRACE**

El servidor proxy repite el mensaje de petición enviado al cliente. Este método permite que el cliente vea lo que se está recibiendo en el otro extremo de la cadena de petición y utilice esos datos para realizar operaciones de diagnóstico o pruebas. El tipo de contenido de la respuesta del proxy es message/http.

## **Directivas asociadas**

Las siguientes directivas habilitan los métodos HTTP/FTP:

- “Enable: habilitar los métodos HTTP” en la página 214
- “Disable: inhabilitar los métodos HTTP” en la página 213

Para obtener más información, consulte el Capítulo 4, “Edición manual del archivo ibmproxy.conf”, en la página 13.

## **Formularios de Configuración y Administración**

Los siguientes formularios de Configuración y Administración editan los valores de las directivas asociadas:

- Configuración de servidor → Métodos HTTP → GET
- Configuración de servidor → Métodos HTTP → HEAD
- Configuración de servidor → Métodos HTTP → POST
- Configuración de servidor → Métodos HTTP → PUT
- Configuración de servidor → Métodos HTTP → DELETE

- Configuración de servidor → Métodos HTTP → OPTIONS
- Configuración de servidor → Métodos HTTP → TRACE
- Configuración de servidor → Proceso de peticiones → Métodos HTTP → CONNECT

**Nota:** Si inhabilita el método POST, no puede utilizar los formularios de Configuración y Administración para configurar el Caching Proxy.

Para obtener más información, consulte el Capítulo 2, “Utilización de los formularios de Configuración y Administración”, en la página 7.

---

## Habilitar métodos WebDAV, métodos MS Exchange y métodos definidos por el usuario

Sólo se aplica a configuraciones de proxy de retorno.

Además del soporte de métodos HTTP estándar, Caching Proxy da soporte al reenvío de otros métodos definidos en los RFC o utilizados por algunas aplicaciones. Caching Proxy también da soporte a métodos definidos por el cliente y permite reenviarlos mediante el servidor proxy.

WebDAV (Web-based Distributed Authoring and Versioning) es un conjunto de extensiones del protocolo HTTP que permite editar y gestionar archivos de forma cooperativa en servidores Web remotos. Caching Proxy da soporte a los métodos WebDAV, métodos utilizados por Microsoft Exchange Server y métodos definidos por el usuario (personalizados).

Estos métodos están codificados y se gestionan con las directivas Enable y Disable. Los administradores también pueden utilizar la máscara de método definida en la directiva PROTECT para autorizar el uso de estos métodos.

Métodos WebDAV soportados (RFC 2518): PROPFIND , PROPPATCH , MKCOL, COPY, MOVE, LOCK, UNLOCK, SEARCH

Métodos de MS Exchange soportados: BMOVE, BCOPY, BDELETE, BPROPFIND, BPROPPATCH, POLL, NOTIFY, SUBSCRIBE, UNSUBSCRIBE, ACL, SUBSCRIPTIONS, X\_MS\_ENUMATTS

Cuando los métodos WebDAV o de MS Exchange Server están habilitados, Caching Proxy sólo reenvía las peticiones a los servidores de destino y no reescribe ningún enlace de recurso en el cuerpo de las peticiones.

Caching Proxy también puede reenviar métodos definidos por el usuario al servidor de fondo. Utilice la sintaxis siguientes para la directiva Enable en el archivo ibmproxy.conf a fin de habilitar un método personalizado:

```
Enable método-definido-por-usuario [WithBody | WithoutBody]
```

Establecer el valor WithBody o WithoutBody indica al proxy si el método definido por el usuario necesita un cuerpo de petición.

El siguiente ejemplo habilita un método definido por el usuario My\_METHOD e indica al proxy que el método necesita un cuerpo de petición:

```
Enable MY_METHOD WithBody
```

## Directivas asociadas

Las siguientes directivas habilitan los métodos WebDAV, métodos de MS Exchange y métodos definidos por el usuario:

- “Enable: habilitar los métodos HTTP” en la página 214
- “Disable: inhabilitar los métodos HTTP” en la página 213

Para obtener más información, consulte el Capítulo 4, “Edición manual del archivo `ibmproxy.conf`”, en la página 13.

---

## Definición de normas de correlación

Las normas de correlación son directivas de configuración que hacen que las peticiones de cliente dirigidas a Caching Proxy se procesen de algún modo, por ejemplo, se pasan a un servidor de origen (proxy), se redirigen o se rechazan. Es importante establecer las normas de correlación correctamente para el correcto funcionamiento del Caching Proxy. Las normas de correlación tienen un efecto sobre lo siguiente:

- Función del proxy básico
- Acceso a los formularios de Configuración y Administración basados en el navegador
- Habilidad de colocar en antememoria los resultados de servlet y demás contenido generado dinámicamente

Las directivas de normas de correlación utilizan el siguiente formulario:

*norma plantilla destino* [*dirección\_IP* |  
*nombre\_sistppal*]:[*puerto*]

Sólo las peticiones que coinciden con la combinación determinada de plantilla y puerto IP están sujetas a esta norma. Una plantilla puede contener comodines, por ejemplo, `https://**/*.asp`.

El orden en el que aparecen las normas en el archivo de configuración es significativo. Excepto las directivas Map, tan pronto como la petición coincide con una plantilla, aquella se procesa y no se evalúan las normas posteriores. La directiva Map sustituye el URL de la petición. Esta nueva petición continúa para ser comparada con las restantes normas de correlación.

## Normas de correlación

Las siguientes normas de correlación se aplican a las peticiones de cliente que coinciden con la plantilla determina:

- **Map, MapQuery** — reescribir la petición. Las reglas Map y MapQuery sustituyen un URL de petición (plantilla) con otra serie de URL (destino). Después de esta sustitución, la petición, que contiene la nueva serie, continúa para ser comparada con las restantes normas de correlación.
- **RuleCaseSense** — permite correlacionar peticiones de los URL de aplicación que no son sensibles a mayúsculas y minúsculas. Cuando se ajusta en off, la directiva RuleCaseSense permite al proxy correlacionar peticiones con reglas definidas en el archivo `ibmproxy.conf` sin sensibilidad a mayúsculas y minúsculas.
- **Pass, Exec**: servir la petición localmente. Las normas Pass y Exec procesan la petición en el servidor proxy. La norma Pass correlaciona un URL de petición

(plantilla) con un archivo que se sirve desde el servidor proxy (destino); la norma Exec correlaciona un URL de petición URL con un programa CGI que se ejecute en el servidor proxy.

- **Fail:** rechazar la petición. La norma Fail rechaza una petición (plantilla) en el servidor proxy. Cualquier petición que coincida con la plantilla de una norma Fail ya no se continúa procesando. Las normas Fail no tienen argumentos de destino.
- **Redirect:** enviar la petición. La norma Redirect envía una petición (plantilla) a otro servidor Web (destino). Dado que el destino de esta norma es un URL completo, incluido el protocolo de comunicación, es posible modificar el protocolo durante la redirección, por ejemplo, para añadir el cifrado SSL a una petición HTTP. Una redirección no comprueba la antememoria antes de satisfacer esta petición.
- **Proxy, ProxyWAS:** pasar por el proxy la petición. Las normas Proxy y ProxyWAS pasan las peticiones (plantillas) a otro servidor (destino). A diferencia de una simple norma Redirect, las normas Proxy permiten que el servidor proxy compruebe la antememoria para satisfacer una petición, para colocar en antememoria el contenido de los servidores de origen y para escribir las cabeceras HTTP que habilitan funciones avanzadas. Utilice la norma ProxyWAS en lugar de la norma Proxy cuando el origen de servidor sea un WebSphere Application Server.

La siguiente norma de correlación se aplica a la respuesta de servidor de origen:

- **ReversePass:** interceptar las peticiones redirigidas automáticamente. Una norma ReversePass coincide con la respuesta que va del servidor de origen a la plantilla al pasar a través del servidor proxy camino del cliente. La directiva ReversePass está diseñada para detectar todo código de estado de redirección que pudiese hacer que un cliente se pusiese en contacto directo con el servidor de origen. El cliente recibe instrucciones para contactar con el servidor definido en el argumento de destino.

Las siguientes normas de correlación se aplican a las aplicaciones API:

- **nameTrans:** acepta la petición y ejecuta una aplicación API definida por la vía de acceso del archivo de sustitución durante el paso de traducción de nombres del proceso de peticiones.
- **service:** acepta la petición y ejecuta una aplicación API, definida por la vía de acceso del archivo de sustitución, durante el paso de servicio del proceso de peticiones.

## Configuración del servidor sustituto

Para configurar un sustituto estándar:

- Establezca el puerto del servidor proxy en 80.  
Puerto 80
- Añada una norma Proxy, anterior a todas las demás, que haga pasar por el proxy todas las peticiones recibidas en el puerto 80 al servidor de origen.  
Proxy  
/\* http://nuestro.servidor.contenido.com/\* :80
- Habilite un puerto de administración en un puerto distinto de 80.  
AdminPort 8080

Esto permite que todo el tráfico HTTP del puerto 80 pase por el proxy al servidor de origen. El tráfico que entre en el puerto de administración no coincide con la norma de proxy comodín inicial y, por lo tanto, no se ve afectado. Las restantes normas de correlación se utilizan para procesar la petición.

## Directivas asociadas

Las siguientes directivas definen las normas de correlación:

- “Map — Cambiar las peticiones coincidentes a una nueva serie de petición, utilizando la serie de vía de acceso de petición para cumplir la regla” en la página 239
- “MapQuery — Cambiar las peticiones coincidentes a una nueva serie de petición, utilizando la serie de vía de acceso de petición y consulta para cumplir la regla” en la página 241
- “RuleCaseSense — Correlaciona peticiones de los URL de aplicación que no son sensibles a mayúsculas y minúsculas” en la página 278
- “Pass: especificar la plantilla para aceptar peticiones” en la página 252
- “Exec: ejecutar un programa CGI para hacer coincidir las peticiones” en la página 218
- “Redirect: especificar una plantilla para las peticiones enviadas a un servidor distinto” en la página 273
- “Proxy: especificar los protocolos de proxy o el proxy de retorno” en la página 266
- “ProxyWAS: especificar que las peticiones se envíen a WebSphere Application Server” en la página 271
- “ReversePass: interceptar las peticiones redirigidas automáticamente” en la página 275

Para obtener más información, consulte el Capítulo 4, “Edición manual del archivo ibmproxy.conf”, en la página 13.

## Formularios de Configuración y Administración

El siguiente formulario de Configuración y Administración edita los valores de las directivas asociadas:

- **Configuración de servidor -> Proceso de peticiones -> Direccionamiento de petición**

**Nota:** Los formularios de Configuración y Administración no dan soporte al argumento de número de puerto.



Para obtener más información, consulte el Capítulo 2, “Utilización de los formularios de Configuración y Administración”, en la página 7.

---

## Habilitación de la reescritura de unión (opcional)

Sólo se aplica a configuraciones de proxy de retorno.

La directiva `JunctionRewrite` habilita la rutina de reescritura de unión en `Caching Proxy` para reescribir las respuestas de los servidores de origen para garantizar que los URL relativos al servidor se correlacionen correctamente con el servidor de origen correcto cuando se utilizan uniones. El plug-in de reescritura de unión también debe habilitarse. Las uniones se definen mediante normas de correlación del proxy.

Al utilizar las normas de correlación del proxy para definir la unión, puede utilizar la directiva `Proxy` con la opción `JunctionPrefix` o sin ella.

### Definición de la unión sin la opción `JunctionPrefix`

A continuación se ofrecen ejemplos de uniones válidas sobre las que puede actuar la rutina de reescritura de unión:

- `Proxy /shop/* http://servidortienda.acme.com/*`
- `Proxy /auth/* http://servidoraautoriz.acme.com/*`

A continuación se ofrece un ejemplo de una unión válida sobre la que *no* actuará la rutina de reescritura de unión:

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

A continuación aparecen ejemplos de uniones no válidas:

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

Estas normas de correlación han creado uniones para `servidortienda`, `servidoraautoriz` y `servidorb2b`. Considere que `servidortienda` devuelve un documento HTML con los siguientes URL contenidos en los distintivos HTML apropiados:

- `/index.html` (referencia relativa al servidor)
- `/images/shop.gif` (referencia relativa al servidor)
- `buy/buy.jsp` (referencia relativa al directorio)
- `http://ebay.com` (referencia absoluta)

La rutina de reescritura de unión reescribirá las referencias relativas al servidor mediante las normas de correlación del proxy del modo siguiente:

- `/shop/index.html` (modificado)
- `/shop/images/shop.gif` (modificado)
- `buy/buy.jsp` (sin modificar)
- `http://ebay.com` (sin modificar)

## Definición de la unión con la opción JunctionPrefix (método recomendado)

Al utilizar la opción JunctionPrefix con la directiva Proxy, en lugar de inferir JunctionPrefix del primer patrón de URL de la norma Proxy, puede declarar el prefijo de unión de la norma Proxy mediante el formato siguiente:

```
Proxy url_pattern1 url_pattern2 JunctionPrefix:url_prefix
```

Al utilizar JunctionPrefix, no hay límites en cuanto al formato del primer patrón de URL. Para dar soporte a la reescritura de unión cuando *no* se utilice la opción JunctionPrefix, el URL de proxy debe tener el siguiente formato: Proxy /market/\* http://servidorautoriz/\*. Sin embargo, al utilizar JunctionPrefix, la siguiente norma Proxy es válida para la reescritura de unión:

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

La rutina de reescritura de unión afecta a los siguientes distintivos:

*Tabla 3. Distintivos afectados por la rutina de reescritura de unión*

Distintivo	Atributos
!—	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

**Nota:** La rutina de reescritura de unión no afectará a los distintivos generados por JavaScript o los plug-ins del explorador.

## Directivas asociadas

Las siguientes directivas se utilizan para habilitar el plug-in y la rutina de reescritura de unión.

- “ServerInit: personalizar el paso de inicialización de servidor” en la página 281
- “Transmogrier: personalizar el paso de manipulación de datos” en la página 290
- “JunctionRewrite: habilitar la reescritura de URL” en la página 232
- “JunctionRewriteSetCookiePath: reescribir la opción de vía de acceso en la cabecera Set-Cookie cuando se utiliza con el plug-in JunctionRewrite” en la página 232
- “JunctionReplaceUrlPrefix: sustituir el URL en lugar de insertar un prefijo cuando se utiliza con el plug-in JunctionRewrite” en la página 231
- “JunctionSkipUrlPrefix: omitir la reescritura de los URL que ya contienen el prefijo cuando se utiliza con el plug-in JunctionRewrite” en la página 233

Para obtener más información, consulte el Capítulo 4, “Edición manual del archivo ibmproxy.conf”, en la página 13.

## Formularios de Configuración y Administración

Los siguientes formularios de Configuración y Administración se pueden utilizar para habilitar el plug-ins de reescritura de unión:

- **Configuración de servidor → Proceso de peticiones → Petición de proceso de API**

**Nota:** Los formularios de Configuración y Administración no dan soporte a la directiva JunctionRewrite.

Para obtener más información, consulte el Capítulo 2, “Utilización de los formularios de Configuración y Administración”, en la página 7.

## UseCookie como alternativa a JunctionRewrite

Puede utilizar cookies para almacenar información del servidor de programa de fondo del siguiente modo: se envía una cookie al navegador de cliente. Cuando el navegador envía peticiones a los recursos de la página HTML, éste adjunta una cookie de modo que Caching Proxy envía las peticiones al servidor de programa de fondo correcto.

Para utilizar cookies como una alternativa para JunctionRewrite, efectúe las siguientes modificaciones en el archivo ibmproxy.conf:

1. Modifique **JunctionRewrite on** con **JunctionRewrite on UseCookie**.
2. Comente el plug-in JunctionRewrite.

A continuación aparece una comparación entre el plug-in JunctionRewrite y la implementación de cookies.

- plug-in JunctionRewrite
  - La página HTML se reescribe.
  - No soporta la reescritura de applets y lenguajes de script, a menos que se utilice el plug-in de transformación rápida (transmogrier). Consulte “Ejemplo de plug-in de transformación rápida para ampliar la funcionalidad de JunctionRewrite” en la página 50.
  - Rendimiento disminuido.

- Sin limitaciones en las configuraciones de servidores de programa de fondo. En una sesión el cliente puede tener acceso cruzado a servidores de programa de fondo.
- Implementación de Cookie
  - La página HTML *no* se reescribe. Se envía una cookie al cliente.
  - El navegador del cliente debe habilitar el soporte de cookie.
  - Rendimiento aumentado.
  - Alguna limitación en las configuraciones de servidores de programa de fondo. Sólo puede utilizarse cuando, en una sesión, un cliente accede a un servidor de programa de fondo.

**Nota:** No existe ningún límite al utilizar JunctionRewrite con la opción UseCookie. Traducirá incorrectamente los URL para todas las peticiones aunque la cookie se aplique únicamente a un subdirectorio del sistema principal. A continuación aparecen dos formas correctas de manejar los URL que están bajo ROOT y no necesitan ningún unión:

- Colocar las normas de proxy antes que la directiva JunctionRewrite en el archivo ibmproxy.conf. (Todas las normas de proxy que aparecen antes que la directiva JunctionRewrite no se reescribirán.)
- De forma explícita, correlacionar todos los URL, en lugar de utilizar un comodín (\*). Por ejemplo:

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

## Ejemplo de plug-in de transformación rápida para ampliar la funcionalidad de JunctionRewrite

Se proporciona código de ejemplo personalizable que reescribe y analiza los bloques de distintivos JavaScript™ (SCRIPT) y applet (APPLET) de los archivos HTML. El plug-in JunctionRewrite por sí solo puede procesar los enlaces de recursos en JavaScript o en los valores de parámetros de Java™.

Después de instalar Caching Proxy, puede compilar el mismo código y configurarlo para que se ejecute con JunctionRewrite.

Los siguientes archivos de ejemplo están situados en el subdirectorio ...samples/cp/, bajo el directorio en que ha descargado el fixpack.

- Makefile (Makefile para este plug-in de ejemplo)
- junctionRewrite2.h (interfaz para el manejador de analizador personalizable)
- junctionRewrite2.c (implementación de la interfaz anterior)
- scriptHandler.c (manejador de reescritura de JavaScript de ejemplo)
- appletHandler.c (ejemplo de descriptor de bloques de Applet)
- junctionRewrite2.def (archivo def de plug-in de Windows)
- junctionRewrite2.exp (archivo de exportación de plug-in de Linux y UNIX)

---

## Capítulo 11. Gestión del envío del contenido local

Las normas de correlación Pass y Exec se utilizan para enviar el contenido local a un cliente que lo solicite. Por omisión, una norma Pass con una plantilla comodín se coloca como la última norma de correlación. Esta norma dirige todas las peticiones que no coinciden con las plantillas anteriores para recuperar los archivos de un directorio de destino, al que generalmente se denomina directorio raíz de documentos.

Cuando se recibe un URL que no contenga un nombre de archivo, Caching Proxy satisface la petición buscando el directorio especificado, si se proporciona uno, o el directorio raíz de documentos, si no se especifica ningún directorio, del archivo que coincide con la lista de páginas de bienvenida especificada en el archivo de configuración. Si se define más de una página Web, el servidor proxy busca las páginas en el orden en que se definen. Se sirve la primera página de bienvenida que se encuentre.

La página de inicio del servidor es la página Web que el servidor envía por omisión al recibir una petición que contenga sólo el URL del servidor sin un nombre de archivo ni directorio. Como se explica previamente, la norma de correlación de comodín por omisión requiere que la página de inicio del servidor esté almacenada en el directorio raíz de documentos y que el nombre de archivo de la página de inicio coincida con una página de bienvenida definida.

**Nota:** Algunos exploradores Web utilizan el término *página de inicio* para hacer referencia a la primera página que el explorador carga al iniciarse. Este documento utiliza el término sólo para la página de inicio del servidor.

Este capítulo describe cómo definir el directorio raíz de documentos y las páginas de bienvenida.

---

### Definición de un directorio raíz de documentos

Los directorios raíz de documentos por omisión son:

- En Linux y UNIX: /opt/ibm/edge/cp/server\_root/pub/*lang*/
- En Windows: *drive*:\Archivos de programa\IBM\edge\cp\server\_root\pub\*lang*\ o el directorio especificado como el directorio HTML durante la instalación

### Directivas asociadas

La siguiente directiva define el directorio raíz de documentos:

- “Pass: especificar la plantilla para aceptar peticiones” en la página 252

Para obtener más información, consulte el Capítulo 4, “Edición manual del archivo ibmpoxy.conf”, en la página 13.

### Formularios de Configuración y Administración

Para modificar el directorio raíz de documentos de los formularios de Configuración y Administración, utilice el siguiente procedimiento:

1. Seleccione **Configuración de servidor -> Proceso de peticiones -> Direcccionamiento de petición.**

2. En la tabla de direccionamiento de peticiones, busque la fila que contiene la serie /\* (barra inclinada asterisco) en la columna **Petición Plantilla**. Esta fila representa el directorio de raíz de documentos. En el recuadro **Índice** que aparece debajo de la tabla, pulse el número que se corresponde con el número de la columna **Índice** para esa fila.
3. Pulse **Sustituir**.
4. En la lista desplegable **Acción**, pulse **Aprobar**.
5. Escriba /\* en el campo de plantillas de peticiones URL.
6. Escriba el nuevo directorio raíz de documentos en el campo **Vía de acceso de archivo de sustitución**.
7. Pulse **Someter**.
8. Después de que se acepten los cambios, pulse el icono **Reiniciar servidor** (I) en el marcho superior.

Después del reinicio, el servidor empieza a utilizar el directorio raíz de documentos.

Para obtener más información, consulte el Capítulo 2, “Utilización de los formularios de Configuración y Administración”, en la página 7.

---

## Definición de las páginas de bienvenida por omisión

El servidor busca la página de inicio en el directorio raíz de documentos, pero el archivo específico que devuelve se define mediante la lista de páginas de bienvenida.

### Acerca de las páginas de bienvenida

Cuando el servidor recibe una petición URL que no especifica un nombre de archivo, intenta satisfacer la petición de acuerdo con una lista de páginas de bienvenida establecidas en el archivo de configuración del servidor. Esta lista define los archivos que se van a utilizar como páginas principales por omisión. El servidor determina su página de inicio haciendo coincidir la lista de páginas de bienvenida con los archivos del directorio raíz de documentos. La primera coincidencia que encuentra es el archivo que se devuelve como página de inicio. Si no se encuentra ninguna coincidencia, el servidor muestra un listado de los directorios raíz de documentos.

Para que un determinado archivo se utilice como la página de inicio del servidor y se devuelva cuando una petición no especifique un directorio ni un nombre de archivo, debe incluir el archivo en el directorio raíz de documentos y asegurarse que su nombre coincida con uno de los nombres de archivo enumerados en la lista de páginas de bienvenida.

El archivo de configuración por omisión define, en el orden siguiente, estos nombres de archivo para que se utilicen como páginas de bienvenida:

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

El servidor devuelve el primer archivo que encuentra que coincide con un nombre de archivo de la lista. Hasta que cree un archivo welcome.html o index.html e incluya ese archivo en el directorio raíz de documentos, el servidor utiliza Frntpage.html como la página de inicio.

Por ejemplo, si está utilizando la configuración por omisión y el directorio raíz de documentos no contiene un archivo denominado `welcome.html`, pero contiene los archivos denominados `index.html` y `FrntPage.html`, se utiliza el archivo `index.html` como página de inicio.

Si no se encuentra ninguna página de inicio, el contenido del directorio raíz de documentos se visualiza como un directorio.

## Directivas asociadas

La siguiente directiva define las páginas de bienvenida:

- “Welcome: especificar los nombres de los archivos de bienvenida” en la página 295

Para obtener más información, consulte el Capítulo 4, “Edición manual del archivo `ibmproxy.conf`”, en la página 13.

## Formularios de Configuración y Administración

El siguiente formulario de Configuración y Administración define las páginas de bienvenida:

- **Configuración de servidor -> Directorios y página de bienvenida -> Página de bienvenida**

Para obtener más información, consulte el Capítulo 2, “Utilización de los formularios de Configuración y Administración”, en la página 7.





---

## Capítulo 12. Gestión de las conexiones FTP

Sólo se aplica a configuraciones de proxy de reenvío.

Caching Proxy pasa por el proxy todas las peticiones para los URL de FTP al servidor FTP adecuado, pero no puede utilizarse para pasar por el proxy las peticiones de un cliente FTP. Puede dar soporte sólo a aquellas peticiones FTP recibidas de un cliente HTTP (mediante el esquema de protocolo ftp://).

Sólo se da soporte a los métodos GET, PUT y DELETE para las peticiones de los archivos FTP. Sólo se da soporte al método GET para las peticiones de listados de directorio FTP. Por omisión, se inhabilitan PUT y DELETE en Caching Proxy. Para obtener más información, consulte “Habilitación de métodos HTTP/FTP” en la página 41.

Este capítulo describe cómo proteger los archivos FTP y gestionar el inicio de sesión del servidor, las vías de acceso de directorio y el encadenamiento de FTP.

---

### Protección de archivos FTP

Si ha habilitado el método PUT para la carga de archivos FTP o el método DELETE para la supresión de archivos FTP, es necesario que defina la protección del proxy FTP para las peticiones PUT y DELETE como mínimo, para evitar la actualización de archivos no autorizados en el servidor FTP.

Para proteger el paso por el proxy de las peticiones FTP, en los formularios de Configuración y Administración, seleccione **Configuración de servidor -> Protección de documentos**. Para crear una configuración de protección para las peticiones de archivos FTP, incluya ftp:// al inicio de la plantilla de petición. Por ejemplo, para proteger los archivos de un directorio llamado exams, utilice la plantilla ftp://exams/\*.

Para obtener más información sobre cómo crear configuraciones de protección, consulte el Capítulo 25, “Configuraciones de protección del servidor”, en la página 115.

---

### Gestión del inicio de sesión del servidor FTP

Si ningún ID de usuario ni contraseña se especifica en el URL de petición, Caching Proxy intenta iniciar la sesión en el servidor FTP solicitado de forma anónima (mediante el ID de usuario ANONYMOUS). Numerosos servidores FTP requieren una dirección de correo electrónico como contraseña para el FTP anónimo. Si el servidor FTP pide una contraseña para el inicio de sesión anónimo, Caching Proxy envía la dirección de correo electrónico especificada por la directiva WebmasterEmail del archivo de configuración.

Para establecer la dirección de correo electrónico del Webmaster que aparece en los formularios de Configuración y Administración, seleccione **Configuración de servidor -> Gestión del sistema -> SNMP MIB**. La dirección de correo electrónico también puede establecerse mediante la directiva WebmasterEmail; para obtener detalles, consulte el apartado de referencia: “WebMasterEMail: establecer una dirección de correo electrónico para recibir informes de servidor seleccionados” en la página 294.

Si el servidor FTP del URL de petición requiere un ID de usuario y contraseñas específicos para iniciar la sesión, los usuarios pueden especificar el ID de usuario y contraseña en el URL de petición, por ejemplo:

```
ftp://idusuario:contraseña@sistppalservidorftp/
```

Si no desea especificar la contraseña para el ID de usuario FTP en el URL de petición, los usuarios pueden especificar sólo el ID de usuario en el URL:

```
ftp://idusuario@sistppalservidorftp.
```

Caching Proxy primero intenta iniciar la sesión en el servidor FTP con el ID de usuario especificado y sin contraseña. Si el inicio de sesión no se realiza satisfactoriamente sin una contraseña, el navegador solicita la contraseña asociada al ID de usuario especificado.

Para los inicios de sesión que no sean anónimos, se debe especificar el ID de usuario como mínimo en el URL. Si no se especifica el ID de usuario, se intenta el inicio de sesión anónimo y al cliente no se le solicita el ID de usuario.

---

## Gestión de las vías de acceso de directorios FTP

Debe especificar a Caching Proxy si desea que los nombres de vía de acceso de los URL de FTP se interpreten como relativos al directorio de trabajo del usuario o relativos al directorio raíz. Por ejemplo, si un usuario que ha iniciado sesión en un servidor FTP tiene un directorio de trabajo por omisión llamado /export/home/usuario1 y desea recuperar un archivo llamado prueba1.exe de un subdirectorío llamado prueba, el proxy utiliza los siguientes URL para recuperar el archivo del servidor FTP, dependiendo de cómo se interpreten los URL de FTP:

- Si se establecen nombres de vías de acceso *absolutas*: ftp://usuario1:usuario1pw@FTPHost/export/home/usuario1/prueba/prueba1.exe
- Si se establecen nombres de vías de acceso *relativas*: ftp://usuario1:usuario1pw@FTPHost/prueba/prueba1.exe

Si se establecen las vías de acceso de URL de FTP relativas, los usuarios pueden especificar todavía un nombre de vía de acceso absoluta mediante la convención consistente en utilizar un carácter de escape %2F con el carácter de barra inclinada (/) para indicar el directorio raíz. Por ejemplo, si usuario1, cuyo directorio de trabajo es /export/home/usuario1, desea acceder a un archivo del directorio de trabajo de usuario2, /export/home/usuario2, la petición ftp://usuario1:usuario1pw@FTPHost/%2Fexport/home/usuario2/ *archivo* se interpreta correctamente como un URL relativo al directorio raíz / (es decir, un nombre de vía de acceso absoluta), incluso si se ha optado por los nombres de vías de acceso relativas de los URL de FTP.

Para especificar cómo se deben interpretar los URL de FTP, en los formularios de Configuración y Administración, seleccione **Configuración de proxy -> Rendimiento del proxy**. En la parte inferior del formulario, bajo **Las vías de acceso de URL de FTP deben ser:**, seleccione **vías de acceso absolutas** para especificar el directorio raíz del servidor o **vías de acceso relativas** para especificar el directorio de trabajo del usuario como el principio de la vía de acceso.

Este valor también puede modificarse en el archivo de configuración de proxy; para obtener más información, consulte “FTPUrlPath: especificar cómo se interpretan los URL de FTP” en la página 223.

---

## Gestionar el encadenamiento FTP

Si está encadenando varios servidores proxy Web, puede especificar que las peticiones que contengan los URL de FTP se envíen a un servidor proxy Web encadenado en lugar de al servidor FTP directamente. Para especificar un servidor proxy encadenado para las peticiones FTP, en los formularios de Configuración y Administración, seleccione **Configuración de proxy -> Encadenamiento de proxy y dominios que no son proxy**. El esquema de protocolo http:// se utiliza para especificar el URL del proxy encadenado, incluso al encadenar peticiones para un protocolo de esquema ftp://.

Para configurar el encadenamiento FTP mediante el archivo de configuración de proxy, consulte el apartado de referencia en “ftp\_proxy: especificar otro servidor proxy para las peticiones FTP” en la página 223.



---

## Capítulo 13. Personalización del proceso del servidor

Este capítulo describe cómo utilizar las inclusiones de servidor para insertar información en los programas CGI programas y documentos HTML que se envíen al cliente. Asimismo se describe la personalización de las correlaciones de recursos y mensajes de error del servidor.

---

### Inclusiones de servidor

Las inclusiones de servidor le permiten añadir información a los programas CGI y documentos HTML que el servidor envía al cliente al actuar como servidor de origen (es decir, no a objetos en antememoria o que han pasado por el proxy). La fecha actual, el tamaño de un archivo y la fecha del último cambio de un archivo son ejemplos del tipo de información que se puede enviar al cliente. Este apartado describe el formato de mandato de las inclusiones de servidor y explica cómo lograr que los mandatos include de servidor funcionen en los programas CGI y documentos HTML. Asimismo puede utilizar las inclusiones de servidor para personalizar las páginas de error.

### Consideraciones para las inclusiones de servidor

Antes de utilizar las inclusiones de servidor en el servidor, tenga en cuenta los problemas de rendimiento, seguridad y riesgo:

- El rendimiento puede verse disminuido cuando el servidor está procesando archivos mientras los está enviando.
- La seguridad puede peligrar si permite que usuarios corrientes ejecuten mandatos en el servidor. Tenga cuidado cuando decida en qué directorios va a colocar las inclusiones de servidor y en qué directorios va a colocar el mandato **exec**. Puede minimizar el riesgo de seguridad si no habilita el mandato **exec**.
- La utilización de las inclusiones de servidor puede ocasionar algunos problemas. Por ejemplo, no se puede hacer referencia a los archivos recursivamente: si está ejecutando el archivo `sleepy.html` y el archivo encuentra `<-- !#include file="sleepy.html" -->`, el servidor no detecta el error y puede fallar. La referencia a los archivos de referencia de forma no recursiva en los demás archivos no supone ningún problema.

### Configuración de las inclusiones de servidor

Para habilitar las inclusiones de servidor, seleccione **Configuración de servidor** → **Configuración básica** en los formularios de Configuración y Administración. Utilice este formulario para especificar cuál de los siguientes tipos de inclusiones de servidor son aceptables:

- Scripts CGI
- Archivos
- Todos excepto los scripts CGI que utilizan el mandato **exec**
- Ninguno

Utilice este formulario para especificar si desea realizar el proceso de inclusión de la parte servidor de los documentos de texto y HTML además de otros tipos de archivo.

Asimismo, asegúrese de que se reconozca la extensión de archivo que utilice para la inclusión. En los formularios de Configuración y Administración, seleccione **Configuración de servidor -> Tipos MIME y codificación** y utilice el formulario **Tipos MIME**. Tenga en cuenta que las extensiones shtml y htmls se reconocen por omisión.

Para configurar el servidor para las inclusiones de servidor editando las directivas del archivo de configuración de proxy, consulte los apartados de referencia de las siguientes directivas:

- “AddType: especificar el tipo de datos de los archivos con sufijos determinados” en la página 185
- “imbeds: especificar si se va a utilizar el proceso de inclusión de la parte servidor” en la página 229

## Formato de las inclusiones de servidor

Los mandatos include deben incluirse en el documento HTML o programa CGI como comentarios. Los mandatos tienen el siguiente formato:

```
<!--#directive tag=value ... -->  
o bien  
<!--#directive tag="value" ... -->
```

Las comillas que encierran los valores son opcionales, pero son necesarias para anidar espacios.

## Directivas de las inclusiones de servidor

Este apartado explica las directivas que el servidor acepta para las inclusiones de servidor. No se deben confundir estas directivas con las directivas del archivo de configuración de proxy, que aparecen documentadas en el Apéndice B, “Directivas del archivo de configuración”, en la página 177.

### config: controlar proceso de archivos

Utilice esta directiva para controlar ciertos aspectos del proceso de archivos. Los distintivos válidos son cmntmsg, errmsg, sizefmt y timefmt.

#### cmntmsg

Utilice este distintivo para especificar un mensaje que precede al inicio de los comentarios añadidos por otras directivas. Para cualquier directiva que contenga texto entre una especificación de directiva y “-->”, ese texto se trata como si fuera un comentario y se añade al archivo que el servidor envía al cliente.

Ejemplo:

```
<!--#config cmntmsg="[Esto es un comentario]" -->  
<!-- #echo var=" " texto adicional -->
```

Resultado: <!--[Esto es un comentario] texto extra -->

Valor por omisión: [Lo siguiente era adicional en la directiva]

#### errmsg

Utilice este distintivo para especificar el mensaje que se envía al cliente si ocurre un error mientras se está procesando un archivo. El mensaje se registra en las anotaciones cronológicas de errores del servidor.

Ejemplo:

```
<!-- #config
errmsg="[Se ha producido un error]" -->
```

Valor por omisión: "[Se ha producido un error al procesar esta directiva]"

### sizeofmt

Utilice este distintivo para especificar el formato en el que se visualiza el tamaño de archivo. En los siguientes ejemplos, bytes es el valor utilizado para mostrar el número de bytes, y abbrev para mostrar el número kilobytes o megabytes.

Ejemplo 1:

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

Resultado: 1024

Ejemplo 2:

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

Resultado: 1K

Valor por omisión: "abbrev"

### timefmt

Utilice este distintivo para especificar el formato utilizado para proporcionar las fechas.

Ejemplo:

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

Resultado: "10/18/95 12:05:33"

Default: "%a, %d %b %Y %T %Z"

Los siguientes formatos strftime() son válidos con el distintivo timefmt:

Especificador	Significado
%%	Sustituir por %
%a	Sustituir por el nombre abreviado del día de la semana
%A	Sustituir por el nombre completo del día de la semana
%b	Sustituir por el nombre abreviado del mes
%B	Sustituir por el nombre completo del mes
%c	Sustituir por la fecha y hora
%C	Sustituir por el número de siglo (año dividido por 100 y truncado)
%d	Sustituir por el día del mes (01-31)
%D	Insertar la fecha como %m/%d/%y
%e	Insertar el mes del año como un número decimal (01-12) (Bajo C POSIX sólo, es un campo de 2 caracteres, justificado por la derecha, rellenado con espacios en blanco)

Especificador	Significado
%E[cCxyY]	Si el formato fecha/hora alternativo no está disponible, los descriptores %E se correlacionan con sus equivalentes no ampliados (por ejemplo, %EC se correlaciona con %C)
%Ec	Sustituir por la representación alternativa de la fecha y hora
%EC	Sustituir por el nombre del año base (periodo) de la representación alternativa
%Ex	Sustituir por la representación alternativa de la fecha
%EX	Sustituir por la representación alternativa de la hora
%Ey	Sustituir por el desplazamiento de %EC (año sólo) en la representación alternativa
%EY	Sustituir por la representación alternativa completa del año
%h	Sustituir por el nombre abreviado del mes (igual a %b)
%H	Sustituir por la hora (reloj de 23 horas) como un número decimal (00-23)
%I	Sustituir por la hora (reloj de 12 horas) como un número decimal (00-12)
%j	Sustituir por el día del año (001-366)
%m	Sustituir por el mes (01-12)
%M	Sustituir por los minutos (00-59)
%n	Sustituir por una nueva línea
%O[deHImMSUwWy]	Si el formato fecha/hora alternativo no está disponible, los descriptores %E se correlacionan con sus equivalentes no ampliados (por ejemplo, %Od se correlaciona con %d)
%Od	Sustituir por el día del mes, utilizando los símbolos numéricos alternativos, rellenos según convenga con ceros delante si existe algún símbolo alternativo para el cero, de lo contrario deben utilizarse espacios delante
%Oe	Sustituir por el día del mes, utilizando los símbolos numéricos alternativos, rellenos según convenga con espacios anteriores
%OH	Sustituir por la hora (reloj de 24), utilizando los símbolos numéricos alternativos
%OI	Sustituir por la hora (reloj de 12), utilizando los símbolos numéricos alternativos
%Om	Sustituir por el mes, utilizando los símbolos numéricos alternativos
%OM	Sustituir por los minutos, utilizando los símbolos numéricos alternativos
%OS	Sustituir por los segundos, utilizando los símbolos numéricos alternativos
%OU	Sustituir por el número de semana del año (el domingo como el primer día de la semana, normas correspondientes a %U) utilizando los símbolos numéricos alternativos
%Ow	Sustituir por el día de la semana (Domingo=0), utilizando los símbolos numéricos alternativos
%OW	Sustituir por el número de semana del año (el lunes como el primer día de la semana) utilizando los símbolos numéricos alternativos



Especificador	Significado
%Oy	Sustituir por el año (desplazamiento de %C) de la representación alternativa, utilizando los símbolos numéricos alternativos
%p	Sustituir por el equivalente local de AM o PM
%r	Sustituir por la serie equivalente a %I:%M:%S %p
%R	Sustituir por la notación de 24 horas (%H:%M)
%S	Sustituir por los segundos (00-61)
%t	Sustituir por una pestaña
%T	Sustituir por una serie equivalente a %H:%M:%S
%u	Sustituir por el día de la semana como un número decimal (1-7), con 1 igual a lunes
%U	Sustituir por el número de la semana del año (00-53), donde el domingo es el primer día de la semana
%V	Sustituir por el número de la semana del año (01-53), donde el lunes es el primer día de la semana
%w	Sustituir por el día de la semana (0-6), donde el domingo es 0
%W	Sustituir por el número de la semana del año (00-53), donde el lunes es el primer día de la semana
%x	Sustituir por la representación adecuada de la fecha
%X	Sustituir por la representación adecuada de la hora
%y	Sustituir por el número del año de dos dígitos dentro del siglo
%Y	Sustituir con el número del año de cuatro dígitos
%Z	Sustituir por el nombre del huso horario o dejar sin caracteres si se desconoce el huso horario

La configuración del sistema determina los años y nombres de mes completos y abreviados.

### **echo: visualizar valores de variable**

Utilice esta directiva para visualizar el valor de las variables de entorno especificadas con el distintivo var. Si no se encuentra una variable, se visualizará (None). Asimismo, **echo** puede mostrar un valor establecido por las directivas **set** o **global**. Las siguientes variables de entorno pueden mostrarse:

#### **DATE\_GMT**

La fecha y hora actuales en la hora media de Greenwich. El formato de esta variable se define mediante la directiva **config timefmt**.

#### **DATE\_LOCAL**

La fecha actual y hora local. El formato de esta variable se define mediante la directiva **config timefmt**.

#### **DOCUMENT\_NAME**

El nombre del documento superior. Si el HTML se ha generado mediante una CGI, esta variable contiene el nombre de la CGI.

#### **DOCUMENT\_URI**

El URL completo solicitado por el cliente, sin la serie de consulta.

**LAST\_MODIFIED**

La fecha y hora en que ha modificado el documento actual por última vez.  
El formato de esta variable se define utilizando la directiva **config timefmt**.

**QUERY\_STRING\_UNESCAPED**

La consulta de búsqueda enviada por el cliente. Ésta no está definida a menos que HTML se haya generado por una CGI.

**SSI\_DIR**

La vía de acceso del archivo actual, relativa a SSI\_ROOT. Si el archivo actual está en SSI\_ROOT, este valor es "/".

**SSI\_FILE**

El nombre de archivo del archivo actual.

**SSI\_INCLUDE**

El valor utilizado en el mandato include que ha recuperado el archivo actual. Éste no está definido para el archivo superior.

**SSI\_PARENT**

La vía de acceso y el nombre de archivo del archivo que contiene el mandato include que ha recuperado el archivo actual, relativo a SSI\_ROOT.

**SSI\_ROOT**

La vías de acceso del archivo superior. Todas las peticiones de inclusiones deben estar en este directorio o un subdirectorio de este directorio.

Ejemplo:

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

**exec: especificar programas CGI**

Utilice esta directiva para incluir la salida de un programa CGI. La directiva **exec** descarta cualquier cabecera HTTP a las que da salida la CGI *excepto* las siguientes:

**Content-type**

Determina si se va a analizar el cuerpo de la salida de otras inclusiones

**Content-encoding**

Determina si se debe realizar la traducción de EBCDIC a ASCII

**Last-modified**

Sustituye el valor de cabecera Last-modified actual a menos que el valor actual sea posterior al valor especificado

**cgi: especificar URL de programa CGI**

Utilice esta directiva para especificar el URL de un programa CGI.

En este ejemplo, **programa** es el programa CGI que se desea ejecutar y **info\_vía\_acceso** y **serie\_consulta** representan uno o más parámetros pasados al programa como variable de entorno:

```
<!--#exec  
cgi="/cgi-bin/programa/info_vía_acceso?serie_consulta" -->
```

Este ejemplo muestra la utilización de variables:

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

**flastmod: visualizar fecha y hora de la última modificación del documento**

Utilice esta directiva para visualizar la fecha y hora más recientes en las que se modificó el documento. El formato de esta variable se define mediante la directiva **config timefmt**. Los distintivos **file** y **virtual** son válidos con esta directiva y sus significados se definen del siguiente modo.

Formatos de directiva:

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

**file** Utilice este distintivo para especificar el nombre de un archivo. Para **flastmod**, **fsize** y **include**, se asume que **file** es relativo a **SSI\_ROOT** si está precedido por **'/'**. De lo contrario, es relativo a **SSI\_DIR**. El archivo especificado debe existir en **SSI\_ROOT** o en uno de sus descendientes. Por ejemplo:

```
<!--#flastmod file="/path/file" -->
```

**virtual**

Utilice este distintivo para especificar el URL de una vía de acceso virtual a un documento. Para **flastmod**, **fsize** y **include**, **virtual** siempre se pasa a través de las directivas de correlación del servidor. Por ejemplo:

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

Ejemplo:

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

Result: 12May96

#### **fsize: visualizar tamaño de archivo**

Utilice esta directiva para visualizar el tamaño del archivo especificado. La directiva **config sizefmt** define el formato de esta variable. Los distintivos **file** y **virtual** son válidos con esta directiva y sus significados son los mismos que se han definido anteriormente para la directiva **flastmod**.

Ejemplo:

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

Result: 1K

#### **global: definir variables globales**

Utilice esta directiva para definir las variables globales que se pueden repetirse posteriormente mediante este archivo o cualquier archivo incluido.

Ejemplo:

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

Por ejemplo, para hacer referencia a un documento padre **\*/a** través de los límites virtuales, es necesario que establezca una variable global **DOCUMENT\_URI**. Además es necesario que haga referencia a la variable global del documento hijo. Este ejemplo muestra el código HTML que se necesita para insertar el documento padre:

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

Este ejemplo muestra el código HTML que es necesario insertar en el documento hijo:

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

### **include: incluir un documento en la salida**

Utilice esta directiva para incluir el texto de un documento de la salida. Los distintivos **file** y **virtual** son válidos con esta directiva y sus significados son los mismos que se han definido anteriormente para la directiva **flastmod**.

### **set: establecer variables que se van a repetir**

Utilice esta directiva para establecer una variable que se pueda repetir posteriormente, pero sólo mediante este archivo.

Ejemplo:

```
<!--#set var="Variable 2"
value="AnotherValue" -->
```

Al definir una directiva, puede repetir una serie en medio de value. Por ejemplo:

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

Variables: una directiva set en la parte servidor va seguida generalmente de una directiva echo, de tal modo que busca la variable establecida, informa acerca de dónde se encuentra la variable y continúa con la función. Puede contener varias referencias a variables. Las directivas set de la parte servidor también le permiten repetir una variable ya establecida. Si no se encuentra ninguna variable set, no se visualiza nada.

Cuando una directiva set de la parte servidor encuentra una referencia de variable dentro de una directiva de inclusión de servidor, intenta resolverla en la parte *servidor*. En la segunda línea del siguiente ejemplo, la variable `&index;` de la parte servidor se utiliza con la serie var para construir el nombre de variable var1. A continuación, se asigna a la variable `&var1;` un valor indicando un carácter de escape delante del `&` de `&ecirc;` de modo que no se reconozca como una variable. En su lugar, se utiliza como una serie para crear el valor `fr&ecirc;d`, o *fred* con un acento circunflejo encima de la e. La variable `&ecirc;` es una variable de parte del servidor.

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

Los caracteres que se pueden definir de este modo (llamados variables con escape) aparecen precedidos de una barra inclinada invertida `\` e incluyen los siguientes:

Carácter	Significado
<code>\a</code>	Alerta (timbre)
<code>\b</code>	Retroceso
<code>\f</code>	Salto de página (nueva página)
<code>\n</code>	Línea nueva
<code>\r</code>	Retorno de carro
<code>\t</code>	Tabulador horizontal

Carácter	Significado
\v	Tabulador vertical
\'	Comillas simples
\"	Comillas
\?	Signo de interrogación
\\	Barra inclinada invertida
\-	Guión
\.	Punto
\&	Ampersand

---

## Personalización de los mensajes de error

Puede personalizar los mensajes de error que Caching Proxy devuelve y puede definir mensajes específicos para determinadas condiciones de error. En los formularios de Configuración y Administración, seleccione **Configuración de servidor** → **Personalización de mensajes de error**. Utilice este formulario para seleccionar una condición de error y especificar un determinado archivo HTML para utilizarlo en esa condición.

Para personalizar los mensajes de error mediante la edición de directivas en el archivo de configuración de proxy, consulte el apartado de referencia de la directiva "ErrorPage: especificar un mensaje personalizado para una determinada condición de error" en la página 216.

---

## Redirección RTSP (Real Time Streaming Protocol)

Sólo se aplica a configuraciones de proxy de retorno.

WebSphere Application Server, Versión 6.1 introduce el soporte multimedia de modalidad continua en la forma del redirector RTSP. RTSP habilita Caching Proxy para que actúe como el primer punto de contacto con los reproductores multimedia y redirija las peticiones a un servidor proxy adecuado o a un servidor de contenido que proporcione el contenido de soporte solicitado.

RTSP (Real Time Streaming Protocol) aparece definido en RFC 2326. Es un protocolo estándar de Internet para controlar la corriente de datos. Aunque no incluye la tecnología para *enviar* corrientes, es lo bastante flexible para que pueda utilizarse para controlar las corrientes de datos que no están relacionados con la reproducción de vídeo o audio.

### Acerca de la redirección RTSP

La característica de redirección RTSP permite que Caching Proxy redirija las peticiones para cualquier sesión multimedia de modalidad continua controlada por RTSP. Éstas incluyen los siguientes tipos de soporte:

- Audio grabado de RealNetworks
- Vídeo grabado de RealNetworks
- Corrientes directas RealNetworks (audio y vídeo)
- Archivos de Microsoft Media Player
- Archivos multimedia de Apple Quicktime

Cualquier reproductor que se pueda configurar para contactar con un servidor proxy en el puerto RTSP (generalmente 554) puede utilizar esta infraestructura de Caching Proxy para que el redirector RTSP maneje las peticiones.

El redirector RTSP no coloca en antememoria o pasa directamente por el proxy las representaciones multimedia. El redirector RTSP debe utilizarse junto con un servidor multimedia de modalidad continua de terceros para que proporcione una de las funciones o ambas. Caching Proxy con el redirector RTSP debe tener acceso de red a uno o más de los servidores proxy RTSP.

## Limitación RTSP

Esta característica está sujeta a la siguiente limitación:

Actualmente, sólo se da soporte a las tecnologías RealNetworks. Éstas incluyen el servidor proxy RealProxy, el servidor de origen RealServer y el reproductor multimedia RealPlayer.

## Mejora RTSP

Anteriormente, el redirector RTSP estaba sujeto a la limitación de que todas las peticiones al mismo servidor de origen de cualquier URL debían redirigirse al mismo sitio. La redirección basada en los nombres de archivo u otras partes del URL solicitado no era posible. Esta limitación ya no se aplica. Actualmente el redirector RTSP utiliza el URL completo de las peticiones recibidas junto con el valor de umbral (`rtsp_proxy_threshold`) establecido en el archivo de configuración de Caching Proxy para determinar si se debe redirigir la petición de cliente al servidor de origen o a un servidor proxy. Actualmente las peticiones al mismo servidor de origen se manejan individualmente.

## Configuración de la redirección RTSP

Las siguientes directivas de configuración de archivos se utilizan para controlar la redirección RTSP. Los valores de estas directivas no se renuevan mediante un reinicio de servidor. El servidor debe detenerse completamente y reiniciarse antes de que los cambios de estas directivas entren en vigor.

- “RTSPEnable: habilitar la redirección de RTSP” en la página 276
- “rtsp\_proxy\_server: especificar los servidores para la redirección” en la página 277
- “rtsp\_proxy\_threshold: especificar el número de peticiones antes de la redirección a una antememoria” en la página 277
- “rtsp\_url\_list\_size: especificar el número de los URL en la memoria proxy” en la página 277

---

## Capítulo 14. Configuración de las opciones de cabecera

Al solicitar documentos, los clientes Web envían cabeceras que proporcionan información adicional sobre el navegador o la petición. Las cabeceras se generan automáticamente cuando se envía una petición.

Caching Proxy permite que varias opciones para personalizar la información de cabecera la mantengan oculta del servidor de destino. Aunque la sustitución de la cabecera genérica por la cabecera real tiene la ventaja de aumentar el anonimato del cliente, tiene la desventaja de inhabilitar la personalización de páginas basada en cabeceras que se escribe en algunas páginas Web.

Las cabeceras adoptan generalmente este formato:

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

Esta cabecera incluye los siguientes campos:

- **User-Agent:** proporciona información sobre el navegador y el sistema operativo.
- **Client-IP:** proporciona la dirección IP del cliente que solicite el URL.
- **Referer:** proporciona el servidor de destino con el URL del enlace que realiza la referencia con esta página.

Los valores adecuados de configuración del proxy pueden bloquear la mayoría de las cabeceras. Sin embargo, algunos campos de cabecera son necesarios para los servidores de origen, de modo que si se bloquean, es posible que las páginas Web no se visualicen correctamente (por ejemplo, en algunos casos el bloqueo del campo de cabecera "host" puede ocasionar que los usuarios vean la página Web errónea). Para obtener información sobre los campos de cabecera, consulte la especificación HTTP Version 1.1.

---

### Directivas asociadas

Para modificar las opciones de cabecera editando el archivo de configuración de proxy, consulte los apartados de referencia de las siguientes directivas:

- "NoCacheOnRange — Especificar sin colocación en antememoria para peticiones de rango" en la página 249
- "NoProxyHeader: especificar las cabeceras de cliente que se desea bloquear" en la página 250
- "ProxyFrom: especificar un cliente con una cabecera From:" en la página 269
- "ProxyIgnoreNoCache: ignorar una petición de recarga" en la página 269
- "ProxySendClientAddress: generar la cabecera Client IP Address:" en la página 270
- "ProxyUserAgent; modificar la serie User Agent" en la página 270
- "ProxyVia: especificar el formato de la cabecera HTTP" en la página 270

Para obtener más información consulte el Capítulo 4, "Edición manual del archivo ibmproxy.conf", en la página 13.

---

## Formularios de Configuración y Administración

Puede utilizar dos formularios de Configuración y Administración para especificar las opciones de cabecera:

- Seleccione **Configuración de proxy** -> **Valores de privacidad**. En el formulario **Valores de privacidad**, establezca la siguiente información:
  - **Reenviar dirección IP del cliente al servidor de destino**  
Compruebe este recuadro si desea que la dirección IP del cliente se envíe al servidor de destino (contenido). Si no comprueba este recuadro, el servidor de destino recibe la dirección IP del servidor proxy. Si deja este recuadro deseleccionado, se incrementa el anonimato de los clientes mientras se navega por Internet.
  - **Serie del agente de usuarios**  
Escriba la serie que desea enviar en la cabecera del servidor de destino para sustituir el tipo de navegador y el sistema operativo que está utilizando el cliente. Por ejemplo: especifique que Caching Proxy 4.0 sustituye a Mozilla 2.02/OS2 en la siguiente cabecera:  

```
Content-Type:MIME  
User-Agent: Mozilla 2.02/OS2  
Referer: http://www.ics.raleigh.ibm.com/WebTrafficExpress/main.html  
Pragma:no-cache
```
  - **De:**  
Escriba la dirección de correo electrónico que el servidor lee al analizar la cabecera "De:". Es posible que desee especificar la dirección de correo electrónico del administrador de proxy ya que el administrador es la persona que debe recibir los informes de cualquier problema.
  - Pulse **Someter** para realizar los cambios en el archivo de configuración.
- Seleccione **Configuración de proxy** -> **Filtrado de cabeceras de proxy**. Utilice este formulario para enumerar las cabeceras HTTP que desea bloquear:
  1. Pulse **Añadir** o **Eliminar** e indique un posición de índice para la cabecera bloqueada.
  2. Escriba la cabecera HTTP que desea bloquear. Consulte la especificación HTTP 1.1 para obtener una lista completa y una explicación de las cabeceras.
  3. Pulse **Someter** para realizar los cambios en el archivo de configuración.

Para obtener más información, consulte el Capítulo 2, "Utilización de los formularios de Configuración y Administración", en la página 7.



---

## Capítulo 15. Acerca de la interfaz de programas de aplicación

La interfaz de programas de aplicación (API) se describe detalladamente en la publicación *Guía de programación de Edge Components*. Las directivas API del archivo de configuración habilitan las rutinas de plug-in a las que se llama durante los pasos específicos dentro del flujo de trabajo del proceso de peticiones. Estas rutinas de plug-in pueden sustituirse o ejecutarse además de las rutinas incorporadas.

---

### Directivas asociadas

A continuación se enumeran las directivas API:

- “Authentication: personalizar el paso de autenticación” en la página 189
- “Authorization: personalizar el paso de autorización” en la página 190
- “Error: personalizar el paso de error” en la página 215
- “Log: personalizar el paso de anotación cronológica” en la página 236
- “Midnight: especificar el plug-in de API utilizado para archivar las anotaciones cronológicas” en la página 246
- “NameTrans: personalizar el paso de traducción de nombres” en la página 246
- “ObjectType: personalizar el paso de tipo de objeto” en la página 250
- “PostAuth: personalizar el paso de PostAuth” en la página 257
- “PostExit: personalizar el paso de PostExit” en la página 257
- “PreExit: personalizar el paso de PreExit” en la página 258
- “ServerInit: personalizar el paso de inicialización de servidor” en la página 281
- “ServerTerm: personalizar el paso de terminación de servicio” en la página 282
- “Service: personalizar el paso de servicio” en la página 282
- “Transmogriifier: personalizar el paso de manipulación de datos” en la página 290
- “TransmogriifiedWarning: enviar un mensaje de aviso al cliente” en la página 291

Para obtener más información, consulte el Capítulo 4, “Edición manual del archivo `ibmproxy.conf`”, en la página 13.

---

### Formularios de Configuración y Administración

El siguiente formulario de Configuración y Administración edita los valores de las directivas asociadas:

- **Configuración de servidor -> Proceso de peticiones -> Petición de proceso de API**

Para obtener más información, consulte el Capítulo 2, “Utilización de los formularios de Configuración y Administración”, en la página 7.



---

## Parte 4. Configuración de la antememoria y el servidor proxy

Este apartado describe la antememoria del proxy y su configuración. La antememoria puede configurarse para almacenar archivos en la memoria (antememoria de memoria) o en uno o más dispositivos de almacenamiento (antememoria de disco). Un agente de renovación de antememoria puede configurarse para cargar previamente en la antememoria los archivos solicitados frecuentemente, y se pueden aplicar varios filtros de URL a la colocación en antememoria. En este apartado también se describe el compartimiento de antememoria mediante el uso del acceso de antememoria remota o el plug-in de Protocolo de antememoria de Internet(ICP); la eliminación de los archivos obsoletos con la recogida de basura de antememoria, y la colocación en antememoria de los archivos generados dinámicamente.

Esta parte contiene los siguientes capítulos:

- Capítulo 16, "Visión general de la colocación en antememoria del servidor proxy", en la página 75
- Capítulo 17, "Configuración de la colocación en antememoria básica", en la página 79
- Capítulo 18, "Control de los elementos colocados en antememoria", en la página 83
- Capítulo 19, "Mantenimiento del contenido de la antememoria", en la página 87
- Capítulo 20, "Configuración del agente de carga para la renovación y precarga automática", en la página 93
- Capítulo 21, "Utilización de una antememoria compartida", en la página 101
- Capítulo 22, "Colocación en antememoria de contenidos generados dinámicamente", en la página 105
- Capítulo 23, "Ajuste de la antememoria del servidor proxy", en la página 109



---

## Capítulo 16. Visión general de la colocación en antememoria del servidor proxy

La colocación en antememoria es una característica que permite que el servidor proxy guarde copias locales de los archivos que solicitan los clientes de modo que éste puede servirlos con mayor rapidez desde la antememoria cuando el mismo u otro cliente los solicita de nuevo.

Caching Proxy es compatible con HTTP 1.1 y generalmente cumple con el protocolo HTTP para colocar en antememoria los documentos y determinar la antigüedad.

Este capítulo describe algunas características de la antememoria del servidor proxy. Para esas características que pueden configurarse, la información detallada de cómo establecer los valores adecuados se incluye en capítulos posteriores.

---

### Almacenamiento de antememoria

El servidor proxy puede almacenar la antememoria en un dispositivo de almacenamiento físico o en la memoria del sistema. El tipo de almacenamiento de antememoria más adecuado para el usuario depende de las posibilidades del hardware y de si es más importante disponer de una respuesta de antememoria rápida o de un número mayor de elementos almacenados en la antememoria. El tiempo de respuesta de una antememoria de memoria generalmente es más rápido que de una antememoria de disco, pero el tamaño de una antememoria de memoria está limitado por la cantidad de RAM en la máquina del servidor proxy. El tamaño de una antememoria de disco está limitada por el tamaño de un dispositivo de almacenamiento, que generalmente es mucho mayor que la cantidad de RAM.

Para las antememorias de disco, Caching Proxy utiliza el disco sin procesar, que significa que el servidor proxy escribe directamente en el dispositivo de antememoria sin utilizar los protocolos de escritura y lectura del sistema operativo. El dispositivo de almacenamiento de una antememoria de disco debe prepararse mediante la utilización del mandato **htcformat**. La información detallada sobre **htcformat** se incluye en el apartado Capítulo 17, “Configuración de la colocación en antememoria básica”, en la página 79.

---

### Índice de antememoria

Tanto en una antememoria de memoria como de disco, Caching Proxy también utiliza el espacio de memoria del sistema para mantener un índice de la antememoria, que reduce el tiempo de proceso para buscar los archivos en antememoria.

La estructura de directorios de antememoria de Caching Proxy y sus métodos de búsqueda son distintos de los demás servidores proxy. Caching Proxy mantiene un índice en la memoria con información sobre los archivos en la antememoria. La utilización de RAM para realizar búsquedas en lugar de un disco u otro soporte da como resultado una búsqueda y recuperación de archivos más rápidas.

El índice incluye los URL, ubicaciones de antememoria e información de caducidad de los objetos en antememoria. Por esta razón, la cantidad de memoria necesaria para mantener el índice es proporcional al número de objetos en la antememoria.

Cuando se recibe una petición de un cliente, el proxy comprueba el índice de antememoria en la memoria de ese URL.

- Si el archivo no está en el índice, la petición se realiza al servidor de destino.
  - A continuación, el URL se comprueba para determinar si el archivo recuperado puede almacenarse en antememoria. Si se le permite, el servidor proxy coloca en antememoria el archivo recuperado.
  - Seguidamente, el índice de antememoria se actualiza con el URL, la ubicación y la información de caducidad para el objeto recientemente en antememoria.
- Si el archivo está en el índice:
  - Se comprueba la información de caducidad para determinar si el archivo en antememoria es nuevo.
    - Si el objeto ha caducado, se contacta con el servidor de destino y el objeto caducado se sustituye por el documento recuperado recientemente. La información de caducidad se actualiza en el índice de antememoria.
    - Si el objeto no ha caducado, el documento se sirve desde la antememoria de proxy.

---

## Colocación en antememoria de FTP

Cuando se configura el proxy para colocar en antememoria las peticiones, puede colocar en antememoria las peticiones de archivos FTP además de las peticiones de archivos HTTP. No obstante, como los archivos FTP no contienen el mismo tipo de información de cabecera que los archivos HTTP, las fechas de caducidad de los archivos FTP en antememoria se calculan de modo distinto al resto de los archivos en antememoria.

Cuando se realiza una petición al servidor FTP para que recupere un archivo, el proxy primero envía al servidor FTP una petición LIST para que el archivo obtenga la información de directorio FTP sobre el archivo. Si el servidor FTP responde a la petición LIST con una respuesta afirmativa de conclusión y con la información de directorio del archivo, el proxy crea una cabecera HTTP Last-Modified con la fecha analizada a partir de la información de directorio FTP. La función de colocación en antememoria del proxy seguidamente utiliza esta cabecera Last-Modified, junto con el valor establecido en la directiva CacheLastModifiedFactor del archivo de configuración, para determinar el periodo de tiempo que el archivo FTP permanece en la antememoria antes de caducar.

Para obtener más información sobre cómo se utilizan la cabecera Last-Modified y la directiva CacheLastModifiedFactor para determinar el periodo de tiempo que un archivo permanece en la antememoria, consulte el Capítulo 19, “Mantenimiento del contenido de la antememoria”, en la página 87.

Los archivos FTP que se recuperan para un ID de usuario específico y no mediante un inicio de sesión anónimo se consideran archivos privados y no se colocan en antememoria.

---

## Colocación en antememoria DNS

Además de la colocación en antememoria del contenido Web, el servidor proxy realiza la colocación en antememoria del servidor de nombres de dominio (DNS). Por ejemplo, cuando un cliente solicita un URL de `www.misitioWeb.com`, el proxy solicita al servidor DNS que resuelva el nombre del sistema principal de `www.misitioWeb.com` como una dirección IP. A continuación, la dirección IP se coloca en antememoria para mejorar el tiempo de respuesta para las peticiones posteriores a ese nombre de sistema principal. La colocación en antememoria DNS es automática y no puede volver a configurarse.

---

## Exclusiones de antememoria

Algunos archivos y documentos no se colocan nunca en antememoria. Éstos incluyen los elementos siguientes:

- Archivos devueltos de peticiones mediante los métodos HTTP que no sean GET como, por ejemplo POST y PUT.
- Cualquier documento que requiera la autenticación, a menos que el servidor de origen específicamente permita la colocación en antememoria.
- La salida dinámica de cualquier script CGI, ya que éste es exclusivo cada vez que se solicita. Los resultados generados dinámicamente a partir de servlets y JavaServer Pages (JSP) ejecutados por IBM WebSphere Application Server pueden colocarse en antememoria si se habilita la colocación en antememoria. Consulte el Capítulo 22, “Colocación en antememoria de contenidos generados dinámicamente”, en la página 105 para obtener información detallada.
- Cualquier información pasada a través de una conexión de túneles SSL, ya que el proxy no puede descifrar los datos que pasan a través de ella.
- Cualquier archivo devuelto desde el URL que contiene un signo de interrogación (?), a menos que se permita específicamente la colocación en antememoria de consultas. Consulte el Capítulo 18, “Control de los elementos colocados en antememoria”, en la página 83 para obtener información sobre la configuración la colocación en antememoria de los resultados de las consultas.

Es posible restringir adicionalmente los elementos colocados en antememoria mediante el establecimiento de filtros de colocación en antememoria. Por ejemplo, es posible que no desee que el servidor proxy coloque en antememoria los archivos que se sirven localmente desde el proxy. Consulte el Capítulo 18, “Control de los elementos colocados en antememoria”, en la página 83 para obtener información detallada.

---

## Gestión de la antememoria

La gestión de una antememoria implica varios factores. Como administrador del servidor, puede especificar la siguiente información:

- Qué documentos se colocan en antememoria (consulte el Capítulo 18, “Control de los elementos colocados en antememoria”, en la página 83 para obtener información detallada).
- Cuántos documentos se pueden colocar en antememoria (consulte el Capítulo 17, “Configuración de la colocación en antememoria básica”, en la página 79 para obtener información detallada).
- Durante cuánto tiempo se consideran vigentes los documentos (consulte el Capítulo 19, “Mantenimiento del contenido de la antememoria”, en la página 87 para obtener información detallada).

- Con qué frecuencia se depura la antememoria (recogida de basura) y qué tipo de archivos tienden a guardarse conservarse (consulte el Capítulo 19, “Mantenimiento del contenido de la antememoria”, en la página 87 para obtener información detallada).
- Cómo se asignan índices a los documentos en antememoria (consulte el Capítulo 17, “Configuración de la colocación en antememoria básica”, en la página 79 para obtener información detallada).
- Cuándo se renueva la antememoria (consulte el Capítulo 20, “Configuración del agente de carga para la renovación y precarga automática”, en la página 93 para obtener detalles).
- Acceso de antememoria remota (consulte el Capítulo 21, “Utilización de una antememoria compartida”, en la página 101 para obtener información detallada).
- Cómo se guardan y archivan las anotaciones cronológicas (consulte el Capítulo 17, “Configuración de la colocación en antememoria básica”, en la página 79 para obtener información detallada).

Asimismo, se pueden realizar ajustes de la configuración de antememoria para mejorar el rendimiento global de Caching Proxy. Para obtener información detallada sobre el ajuste del rendimiento, consulte el Capítulo 23, “Ajuste de la antememoria del servidor proxy”, en la página 109.



---

## Capítulo 17. Configuración de la colocación en antememoria básica

Si ha utilizado los valores por omisión del Programa de instalación del producto Edge Components para instalar Caching Proxy, la colocación en antememoria está habilitada y la antememoria se almacena en la memoria. Es posible que desee ajustar los siguientes valores de antememoria básica para personalizar la antememoria en función de las necesidades del sistema.

Si no ha utilizado programa de instalación, configure estos valores para habilitar la colocación en antememoria.

Los pasos básicos necesarios para configurar la antememoria son los siguientes:

1. Habilite la colocación en antememoria.
2. Configure el almacenamiento en antememoria.

Después de configurar los valores de antememoria básica, es posible que desee añadir o modificar los valores de las siguientes características.

- Personalice la memoria de antememoria.
- Guarde o cargue la memoria de antememoria en el disco.
- Restrinja los elementos que se colocarán en antememoria mediante los filtros URL.
- Expanda los elementos que se colocarán en antememoria mediante la habilitación de la colocación en antememoria de los resultados de las consultas o archivos generados dinámicamente.
- Configure la caducidad de archivos en antememoria y la recogida de basura.
- Configure la renovación y precarga de la antememoria dinámica.
- Configure el compartimiento de antememoria con el Acceso a antememoria remota (RCA) o el Protocolo de antememoria de Internet (ICP).
- Configure el registro cronológico.

Las instrucciones sobre cómo modificar cada uno de estos valores se facilitan en este capítulo o bien se hace referencias a ellos.

---

### 1. Habilite la colocación en antememoria

Para habilitar la colocación en antememoria, establezca la directiva Caching en on o seleccione el recuadro **Habilitar colocación en antememoria de proxy** en el formulario de configuración **Configuración de antememoria** → **Valores de antememoria**. Si no especifica un dispositivo de antememoria, la antememoria se almacenará en la memoria. Para crear una antememoria de disco, siga los pasos de “2. Configure el almacenamiento en antememoria”.

---

### 2. Configure el almacenamiento en antememoria

Las tareas para configurar el almacenamiento de antememoria dependen de si se utiliza una antememoria de memoria o una antememoria de disco.

Para utilizar la antememoria de memoria, personalice el valor Memoria de antememoria para que incluya la suficiente memoria para mantener el contenido

de una antememoria. Consulte “Establecimiento de la memoria de antememoria” en la página 81 para obtener los tamaños de memoria de antememoria recomendados.

Para utilizar una antememoria de disco, debe realizar las siguientes acciones:

1. Prepare un dispositivo de almacenamiento para mantener la antememoria.

La antememoria requiere un dispositivo especialmente formateado. Se recomienda destinar un dispositivo o partición de disco completos a la antememoria. El tamaño mínimo de una antememoria es 16392 KB.

Para formatear el dispositivo de antememoria:

- a. Elija un dispositivo para mantener la antememoria. Asegúrese de que ningún otro programa esté utilizando ese espacio de almacenamiento y que se pueda acceder al dispositivo como dispositivo original (o formateado con caracteres).
- b. Formatee el dispositivo utilizando el mandato **htcformat**. La sintaxis es la siguiente:

```
htcformat  
vía_de_acceso_dispositivo_original [-blocksize tamaño_bloque]  
[-blocks número_de_bloques]
```

Los argumentos `-blocksize` y `-blocks` son opcionales. El tamaño de bloque por omisión es de 8192 bytes. Si el número de bloques no se especifica, la partición de disco se rellenará con tantos bloques como pueda contener.

Al especificar la vía de acceso del dispositivo, asegúrese de especificar la vía de acceso del dispositivo sin procesar.

- En las plataformas AIX, la vía de acceso del dispositivo sin procesar de un volumen lógico definido como `/dev/lv02` es `/dev/rlv02`
- En las plataformas Linux, primero debe ejecutar el mandato **raw** antes de ejecutar **htcformat** para asociar la vía de acceso del dispositivo sin procesar con la unidad SCSI real `sdb1`.

```
raw /dev/raw/raw1 dev/sdb1
```

- En las plataformas HP-UX y Solaris, la vía de acceso del dispositivo sin procesar de una partición definida como `/dev/dsk/c0t0d0s0` es `/dev/rdisk/c0t0d0s0`
- En las plataformas Windows, la vía de acceso del dispositivo sin procesar de un dispositivo definido como `e:` es `\\.\e:`

Consulte el material de referencia para sistema de archivos para obtener información adicional sobre el acceso a los dispositivos sin procesar.

2. Especifique el dispositivo de antememoria mediante la directiva `CacheDev` o el formulario de configuración **Valores de antememoria**. Puede especificar más de un dispositivo.

#### PRECAUCIÓN:

En los sistemas Windows, el mandato **htcformat** no marca automáticamente el dispositivo de antememoria como de no escritura.

Si el sistema operativo intenta escribir en el dispositivo de antememoria, los datos en antememoria pueden perderse. Para evitar esto, puede utilizar el programa de utilidad Windows Disk Manager para preparar el disco antes de utilizar el mandato **htcformat**. Para preparar el disco, utilice el programa de utilidad de disco para suprimir el dispositivo y la partición que desee utilizar y, a continuación, vuelva a crearlos sin formato. Esta acción hace que el sistema considere el dispositivo no disponible para el almacenamiento del sistema.

---

## Personalizaciones opcionales

### Establecimiento de la memoria de antememoria

Establezca el valor de la directiva CacheMemory (o del campo **Memoria de antememoria** del formulario de configuración **Valores de configuración**), de acuerdo con el siguiente principio. La cantidad de memoria establecida en este valor se utiliza para el soporte de infraestructura de antememoria, incluido el índice de antememoria, y, si se configura la colocación en antememoria de la memoria, para almacenar el contenido de la antememoria.

#### Valores mínimos

Para un rendimiento óptimo de las antememorias de disco, se recomienda un valor mínimo de memoria de antememoria de 64 MB para el soporte de infraestructura de antememoria, incluido el índice de antememoria. A medida que aumenta el tamaño de antememoria, aumenta el índice de antememoria y se necesita más memoria de antememoria para almacenar el índice. Un valor de memoria de antememoria de 64 MB es lo bastante grande para proporcionar el soporte de infraestructura y almacenar un índice de antememoria para una antememoria de disco de hasta 6.4 GB aproximadamente. Para antememorias de disco de mayor tamaño, la memoria de antememoria debería ser el 1% del tamaño de antememoria.

Para las antememorias de memoria, el valor de memoria de antememoria es la cantidad de memoria reservada para el soporte de infraestructura y la misma antememoria. Se recomienda un valor mínimo de memoria de antememoria de 64 MB.

#### Valor máximo

Si se asigna demasiada memoria física a la antememoria de memoria, es posible que se produzcan operaciones no deseadas como, por ejemplo, errores de "insuficiencia de memoria" o anomalías del servidor proxy. Las limitaciones de valor para la memoria de antememoria son debidas a las limitaciones de una aplicación de 32 bits. Como Caching Proxy es una aplicación de 32 bits, puede utilizar un máximo de 2 GB de memoria.

Caching Proxy asigna la memoria definida por la directiva CacheMemory y la utiliza como la antememoria para almacenar objetos. Debe asignarse la memoria adicional, tanto si es una antememoria de memoria como una antememoria de disco sin procesar, para las estructuras de datos de la antememoria, los almacenamientos intermedios de conexiones y E/S de red, almacenamientos intermedios de sesiones y la memoria del proceso principal y todas las hebras. Asimismo, es posible que las peticiones de algunos clientes necesiten asignar un bloque de agrupaciones de memoria mayor que el valor por omisión. Por lo tanto, si la directiva CacheMemory se establece próxima a la marca de 2 GB, es posible que Caching Proxy no tenga la suficiente memoria para operar, especialmente bajo altas cargas de peticiones.

Se recomienda que el valor de la directiva CacheMemory sea inferior o igual a 1600 MB. El establecimiento del valor en más de 1600 MB interfiere con la memoria que necesita Caching Proxy para un funcionamiento normal y tiene efectos colaterales adversos. Estos efectos colaterales generalmente incluyen una mayor utilización de la CPU (posiblemente de hasta el 100 %), errores de falta de memoria y un rendimiento más lento, aunque no se limita a ellos. Si es necesario un mayor tamaño de antememoria global, utilice los dispositivo de antememoria o implemente una configuración de antememoria compartida con RCA o ICP.

## **Cómo guardar y cargar la memoria de antememoria en el disco**

Puede importar o exportar el contenido de antememoria a un archivo de vuelco y desde él. Esto es útil cuando la memoria de antememoria se pierde durante el reinicio o al desplegar la misma antememoria para varios proxies.

## **Establecimiento de la colocación en antememoria de los filtros**

Los filtros pueden restringir los elementos que se colocan en antememoria haciéndolos coincidir con el formato de la petición URL. Consulte el Capítulo 18, “Control de los elementos colocados en antememoria”, en la página 83 para obtener detalles sobre cómo establecer los filtros.

## **Configuración de la colocación en antememoria de los resultados de las consultas y los archivos generados dinámicamente**

Opcionalmente, puede configurar el servidor proxy para colocar en antememoria los resultados de las peticiones de consultas. Por omisión, los URL que contienen un signo de interrogación (?) no se colocan en antememoria. Consulte el “Colocación en antememoria de respuestas de consultas” en la página 84 para obtener información detallada.

Otra opción consiste en colocar en antememoria los resultados de la ejecución de JPS o servlets desde IBM WebSphere Application Server. Consulte el Capítulo 22, “Colocación en antememoria de contenidos generados dinámicamente”, en la página 105 para obtener información detallada.

## **Configuración de la caducidad de archivos y la recogida de basura**

Consulte el Capítulo 19, “Mantenimiento del contenido de la antememoria”, en la página 87 para obtener información sobre la configuración cuando los archivos de la antememoria caducan y sobre cómo se eliminan los archivos obsoletos.

## **Configuración de la precarga automática**

La antememoria puede configurarse para renovar automáticamente los archivos más solicitados a diario antes de que se soliciten. Consulte el Capítulo 20, “Configuración del agente de carga para la renovación y precarga automática”, en la página 93 para obtener más información.

## **Configuración del compartimiento de antememoria**

En ciertas circunstancias, la utilización de una antememoria aumenta la posibilidad de que un archivo solicitado se encuentre en la antememoria. Consulte el Capítulo 21, “Utilización de una antememoria compartida”, en la página 101 para obtener información.

## **Configuración del registro cronológico**

El mantenimiento de anotaciones cronológicas concisas y exactas es importante para gestionar Caching Proxy. Parte 6, “Supervisión de Caching Proxy”, en la página 149 contiene información sobre cómo configurar y utilizar las anotaciones cronológicas del servidor proxy.

---

## Capítulo 18. Control de los elementos colocados en antememoria

Caching Proxy ofrece varios métodos de filtrado para controlar qué archivos, documentos y demás objetos se colocan en antememoria. Éstos incluyen las características siguientes:

- Filtros de colocación en antememoria basados en URL
- Colocación en antememoria de respuestas de consultas
- Colocación en antememoria de archivos servidos localmente
- Colocación en antememoria basada en URL parcial
- Colocación en antememoria de archivos basados en parte del URL de petición
- Colocación en antememoria de archivos generados dinámicamente. Consulte el Capítulo 22, “Colocación en antememoria de contenidos generados dinámicamente”, en la página 105

**Nota:** El formulario de Configuración y Administración **Configuración de antememoria** → **Comportamiento de antememoria** contiene una opción con la etiqueta **Antememoria basada en URL entrante**. La directiva correspondiente de archivos de configuración se denomina `CacheByIncomingURL`. Esta directiva se refiere al nombre de archivo del archivo en antememoria. Compruebe este recuadro para basar el nombre de archivo del archivo en antememoria en el URL de entrada; si no está seleccionado el recuadro, el nombre de archivo se basa en el URL de salida.

---

### Configuración de filtros de colocación en antememoria basados en URL

El servidor proxy puede configurarse para comparar peticiones con una plantilla de URL para determinar si un archivo se ha colocado en antememoria. Esta característica se configura mediante el establecimiento de plantillas para las peticiones cuyos archivos *siempre* están colocados en antememoria y de plantillas independientes para las peticiones cuyos archivos *nunca* deben colocarse en antememoria. Se pueden utilizar varias plantillas.

Un sistema similar se utiliza para habilitar la colocación en antememoria de respuestas de consultas. Consulte “Colocación en antememoria de respuestas de consultas” en la página 84 para obtener información.

Para establecer los filtros de colocación en antememoria de URL mediante la edición del archivo `ibmproxy.conf`, consulte “CacheOnly: colocar en antememoria sólo los archivos con los URL que coinciden con una plantilla” en la página 199 y “NoCaching: especificar que no se coloquen en antememoria los archivos con los URL que coinciden con una plantilla” en la página 247.

Para establecer los filtros de colocación en antememoria de URL en los formularios de Configuración y Administración, utilice el campo **Configuración de antememoria** → **Comportamiento de antememoria: Filtrado de antememoria por URL**. Utilice este apartado para especificar los URL cuyos archivos siempre se colocan en antememoria o para especificar los URL cuyos archivos nunca se colocan en antememoria. Para especificar dos listas, una de archivos que siempre

se vayan a almacenar en antememoria y otra de los archivos que nunca se vayan a colocar en antememoria, cree una lista y, a continuación, pulse **Someter** antes de crear la otra lista.

---

## Colocación en antememoria de respuestas de consultas

Las respuestas devueltas de consultas (peticiones URL que contienen un signo de interrogación) se pueden almacenar en antememoria mediante filtros de colocación en antememoria. Esta característica puede ser útil en los escenarios de proxy de retorno (sustituto) si numerosos clientes realizan la misma petición de consulta.

La colocación en antememoria de consultas puede configurarse mediante la edición de la directiva `CacheQueries` en el archivo de configuración `ibmproxy.conf`. La directiva `CacheQueries` presenta las siguientes opciones:

- **Always:** todas las respuestas de consultas de los sistemas principales que coincidan con la plantilla se colocarán en antememoria, si se pueden colocar en antememoria mediante los estándares HTTP 1.1.
- **Public:** las respuestas de consultas de los sistemas principales que coincidan con la plantilla se colocarán en antememoria si contienen la cabecera "Cache-control: public" o la cabecera de revalidación forzada y se pueden colocar en antememoria mediante los estándares HTTP 1.1.

Encontrará información adicional sobre estas opciones en "CacheQueries: especificar las respuestas de antememoria a los URL que contienen un signo de interrogación (?)" en la página 200.

Para configurar la colocación en antememoria de respuestas de consultas en los formularios de Configuración y Administración, utilice el campo **Configuración de antememoria** → **Comportamiento de antememoria: Colocar en antememoria filtrado de respuestas de consulta por URL**. Para especificar dos listas, cree una lista y, a continuación, pulse **Someter** antes de crear la otra lista.

## Requisitos adicionales para la colocación en antememoria de respuestas de consultas

Asimismo, para configurar el valor de colocación en antememoria de consultas, asegúrese de que los siguientes valores se configuran correctamente para permitir que las respuestas de consultas se coloquen en antememoria. Consulte "Configuración de la antigüedad de antememoria" en la página 90 para obtener información sobre cómo establecer estas opciones mediante los formularios de Configuración y Administración.

- **CacheTimeMargin:** esta directiva especifica un tiempo de caducidad mínimo, de modo que los archivos con tiempos de caducidad inferiores a este mínimo no se colocan en antememoria. Como las respuestas de consultas tienen en ocasiones tiempos de caducidad muy breves, el establecimiento de esta directiva en un valor inferior permite que se coloquen en antememoria más respuestas de consultas. Consulte "CacheTimeMargin: especificar la duración mínima para colocar en antememoria un archivo" en la página 201 o utilice el formulario **Valores de caducidad de antememoria**, que se describe en "Configuración de la antigüedad de antememoria" en la página 90.
- **CacheDefaultExpiry:** esta directiva especifica el tiempo de caducidad de los archivos que no tengan una fecha de caducidad explícita o una fecha modificada por última vez en función de la cual se va a calcular el tiempo de caducidad. El aumento de este valor de las peticiones HTTP del valor por omisión de 0 permite que se coloquen en antememoria más respuestas de consultas. No obstante, la modificación del valor de este modo también incrementa el riesgo de



que el contenido que no es actual se sirva desde esa antememoria. Consulte “CacheDefaultExpiry: especificar el tiempo de caducidad por omisión de los archivos” en la página 193 o utilice el formulario **Valores de caducidad de antememoria**, que se describe en “Configuración de la antigüedad de antememoria” en la página 90.

- CacheLastModifiedFactor: esta directiva se utiliza para calcular una fecha de caducidad para los archivos que tienen una fecha modificada por última vez pero no tienen una fecha de caducidad explícita. El establecimiento del factor para los archivos HTTP en un valor mayor incrementa periodo de tiempo que un archivo HTTP reside en la antememoria sin que se vuelva a validar. La modificación del valor de este modo también incrementa el riesgo de que el contenido que no es actual se sirva desde esa antememoria. Consulte “CacheLastModifiedFactor: especificar el valor para determinar las fechas de caducidad” en la página 195 o el formulario **Factor de última modificación**, que se describe en “Configuración de la antigüedad de antememoria” en la página 90.
- Opcionalmente, establezca las directivas SignificantUrlTerminator y AggressiveCaching. Consulte “SignificantURLTerminator; especificar un código de terminación para las peticiones URL” en la página 283 o “AggressiveCaching: especificar la colocación en antememoria de los archivos que no se colocan en antememoria” en la página 188.

---

## Colocación en antememoria de archivos servidos localmente

Como generalmente no resulta eficaz colocar en antememoria los archivos que se sirven desde el servidor proxy, los archivos que se originan en el dominio local del servidor no se colocan en antememoria por omisión. Para colocar en antememoria los objetos que se originan en el dominio local del servidor, seleccione el recuadro **Almacenar en antememoria archivos de dominio locales** del formulario de Configuración y Administración **Configuración de antememoria** → **Comportamiento de antememoria**. Alternativamente, establezca la directiva CacheLocalDomain del archivo de configuración de proxy en on.

---

## Colocación en antememoria de los archivos mediante URL parcial

Los elementos sólo pueden colocarse en antememoria basándose sólo en una parte (significativa) especificada del URL de entrada, en lugar del URL completo. Esto resulta útil en los servicios Web del modelo de transacciones o en la colocación en antememoria dinámica, ya que la misma respuesta se devuelve a menudo para diversas peticiones de entrada cuando partes significativas de los URL de peticiones de entrada son idénticos.

No se pueden utilizar los formularios de Configuración y Administración para especificar la colocación en antememoria basada en URL parciales. En su lugar, utilice la directiva SignificantUrlTerminator en el archivo de configuración de proxy para especificar un código de terminación para las peticiones URL. Esta especificación hace que Caching Proxy evalúe sólo los caracteres previos al código de terminación al procesar la petición y determina si el archivo solicitado se ha colocado en antememoria. Cuando se define más de un código de terminador, Caching Proxy compara los URL de entrada con los códigos de terminador en el orden en el que están definidos en el archivo ibmproxy.conf. Consulte “SignificantURLTerminator; especificar un código de terminación para las peticiones URL” en la página 283 para obtener más información.

---

## Directivas relacionadas del archivo de configuración

Para establecer los filtros editando directamente el archivo de configuración de proxy, consulte los apartados de referencia de las siguientes directivas:

- “NoCaching: especificar que no se coloquen en antememoria los archivos con los URL que coinciden con una plantilla” en la página 247
- “CacheOnly: colocar en antememoria sólo los archivos con los URL que coinciden con una plantilla” en la página 199
- “CacheQueries: especificar las respuestas de antememoria a los URL que contienen un signo de interrogación (?)” en la página 200
- “CacheLocalDomain: especificar si se debe colocar en antememoria el dominio local” en la página 196
- “SignificantURLTerminator; especificar un código de terminación para las peticiones URL” en la página 283

Consulte el Capítulo 16, “Visión general de la colocación en antememoria del servidor proxy”, en la página 75 para obtener información sobre los documentos que se pueden colocar en antememoria.



---

## Capítulo 19. Mantenimiento del contenido de la antememoria

Como la colocación en antememoria requiere crear y guardar una copia del archivo servido, es necesario cierto mantenimiento de rutina para que la antememoria funcione correctamente. Debe comprobarse la *antigüedad* de los archivos en antememoria y deben invalidarse cuando ya no son coherentes con los archivos del servidor de origen. Este proceso de caducidad de archivos se explica en “Caducidad de los archivos”. Asimismo, los archivos invalidados o no utilizados deben eliminarse de la antememoria para dejar espacio para los nuevos archivos. Este proceso de depuración de la antememoria se describe en “Recogida de basura” en la página 92.

---

### Caducidad de los archivos

El mantenimiento de los objetos en antememoria que son coherentes con el objeto original del servidor de contenido se conoce como mantenimiento de la antigüedad en la antememoria. Para todos los documentos u otros objetos que coloca en antememoria, Caching Proxy calcula una hora en la que caduca el objeto.

Para las páginas HTTP, la cabecera del documento, generada por el servidor de contenido, contiene la información de caducidad.

Como el protocolo FTP no incluye información de caducidad equivalente, Caching Proxy genera su propia cabecera Last-Modified: para los archivos FTP, basándose en la información de directorios FTP para todos los archivos y utiliza esta información para calcular los tiempos de caducidad. Si el servidor proxy no puede obtener la información de directorio para el archivo a partir del servidor FTP, se utiliza el valor por omisión que coincide con el URL de FTP. Asimismo, como no existe un formato de fecha estándar para los servidores FTP, es posible que Caching Proxy no pueda entender la fecha y hora enviadas por algunos servidores FTP. En ese caso, se utiliza el valor de tiempo de caducidad por omisión del servidor proxy. Este procedimiento permite que el proxy gestione la colocación en antememoria de las páginas HTTP y los archivos FTP de una forma parecida.

Un servidor de contenido puede especificar la caducidad de uno de los siguientes modos (en orden de preferencia):

1. El servidor de contenido especifica una cabecera que dice Cache-control: s-maxage= *n*. Esta cabecera indica al proxy que el objeto es nuevo durante *n* segundos después de que se reciba.
2. El servidor de contenido especifica una cabecera que dice Cache-control: max-age= *n*. Esta cabecera indica al proxy que el objeto es nuevo durante *n* segundos después de que se reciba.
3. El servidor de contenido especifica una cabecera indicando: Expires: *n*. Esta cabecera indica al proxy que el objeto es nuevo hasta la hora indicada por *n*.
4. El servidor de contenido indica cuando se ha modificado un documento por última vez mediante una cabecera Last-Modified: *n*. El servidor proxy calcula el periodo de tiempo desde que el documento se ha modificado por última vez, lo multiplica por el factor de última modificación de antememoria establecido en el archivo de configuración de proxy y asume que el documento es válido durante ese periodo de tiempo. Por ejemplo, si el servidor de contenido indica que el documento se ha modificado por última vez hace una semana (siete días) y si el factor de última modificación de antememoria es 0,14, el servidor

proxy asume que el documento es válido sólo durante un día. Consulte “Configuración de la antigüedad de antememoria” en la página 90 para obtener instrucciones sobre cómo establecer el factor de última modificación de antememoria.

5. Si el servidor de contenido no especifica ninguno de los datos indicados previamente, Caching Proxy busca el valor de Caducidad por omisión de antememoria que coincide con el URL actual y lo utiliza para el tiempo de caducidad. Consulte “Configuración de la antigüedad de antememoria” en la página 90 para obtener instrucciones sobre cómo establecer los valores de Caducidad por omisión de antememoria.

Después de calcular el tiempo de caducidad como se acaba de describir, Caching Proxy comprueba si existe un valor de Espera mínima que se aplica a este URL. Si existe este valor y el periodo que especifica es mayor que el tiempo de caducidad calculado, el tiempo especificado por el valor de Espera mínima se utiliza como tiempo de caducidad del objeto. Esto es cierto incluso si Caching Proxy calcula un tiempo de caducidad de 0 minutos para un documento. Por lo tanto, para evitar servir contenido que no es actual, tenga cuidado con la utilización del valor de Espera mínima. (Para establecer el valor de Espera mínima, utilice la directiva `CacheMinHold` o el valor **Configuración de antememoria → Valores de caducidad de antememoria: Caducidad del URL**. Consulte “Configuración de la antigüedad de antememoria” en la página 90 para obtener información adicional.

El valor de tiempo de caducidad final se contrasta con el tiempo especificado en el valor Margen de tiempo. Si el tiempo de caducidad es mayor que el valor Margen de tiempo, el documento se coloca en antememoria; de lo contrario no se añade a la antememoria. Para establecer el valor de Margen de tiempo, utilice la directiva `CacheTimeMargin` o consulte las instrucciones en “Configuración de la antigüedad de antememoria” en la página 90.

Si se encuentra el documento en la antememoria pero ha caducado, Caching Proxy emite una petición especial conocida como *if-modified-since* al servidor de contenido. Esta petición provoca que el servidor de contenido envíe el documento sólo si se ha modificado desde que el proxy lo recibió por última vez. Si el documento no se ha modificado, el servidor de contenido envía un mensaje que lo indica y no vuelve a enviar la página. En ese caso, el proxy sirve el documento en antememoria. Para los archivos FTP, el servidor proxy simula este proceso *if-modified-since*. Si se determina que el archivo no se ha modificado en el servidor FTP, éste sirve el archivo desde la antememoria. De lo contrario, obtiene la versión más reciente del servidor FTP.

## Información adicional sobre la antigüedad en la antememoria

- Casi todos los documentos Web estáticos, en lugar de los documentos generados dinámicamente, incluyen la cabecera `Last-Modified`. Este es el modo más habitual en que los proxies calculan los periodos de caducidad de los documentos y el primer método que Caching Proxy intenta con los archivos FTP. Si este método no se realiza satisfactoriamente, el proxy hace referencia a los valores de Caducidad por omisión.
- Apenas ningún documento utiliza `Cache-control: s-maxage`, `Cache-control: max-age` o `Expires` header.
- Las páginas generadas dinámicamente, que no se pueden colocar en antememoria con frecuencia, pueden incluir una cabecera mostrando `Expires: 0` o `Cache-control: no-cache`, que significa que el documento caduca inmediatamente. Para obtener información sobre la colocación en antememoria de los archivos generados dinámicamente de servidores IBM WebSphere

Application Server, consulte el Capítulo 22, “Colocación en antememoria de contenidos generados dinámicamente”, en la página 105.

- Tenga especial cuidado al establecer el valor de Caducidad por omisión en cualquier valor que no sea 0 minutos para los URL que utilicen la sintaxis HTTP:. Numerosas páginas generadas dinámicamente no incluyen ninguna de las cabeceras de caducidad y por lo tanto están sujetas al valor de Caducidad por omisión. El establecimiento de Caducidad por omisión en un valor superior a 0 minutos permite que el proxy coloque en antememoria esos objetos, aunque esto puede indicar que los usuarios obtienen contenido desfasado o resultados inesperados de los programas CGI o servlets.
- En las siguientes circunstancias, el servidor proxy vuelve a validar los documentos con el servidor para todas las peticiones, independientemente de si han caducado los documentos en antememoria:
  - El documento incluye una de las siguientes cabeceras:
    - Cache-control: s-maxage
    - Cache-control: must-revalidate
    - Cache-control: proxy-revalidate
  - El documento requiere las credenciales de usuario pero permite que el servidor lo coloque en antememoria.
  - El documento contiene una cabecera Cache-Control: no-cache pero se coloca en antememoria de todas formas (debido a una colocación en antememoria agresiva).

## Acerca de las fechas en FTP

Sólo se aplica a configuraciones de proxy de reenvío.

Como el protocolo FTP no define las fechas y horas de forma tan estricta como lo hace el protocolo HTTP, existen varios factores que pueden provocar que la cabecera Last-Modified generada por el proxy para los archivos sea ligeramente distinta de la fecha de archivo real. Estos factores son los siguientes:

- A diferencia del protocolo HTTP, el protocolo FTP no especifica que las fechas devueltas deben estar en la Hora Media de Greenwich (GMT). Es probable que la fecha devuelta por el servidor FTP esté en la hora local del servidor FTP. Como el proxy no tiene forma de determinar en qué huso horario se está ejecutando el servidor FTP, interpreta la hora en su propio huso horario. Una excepción a este hecho lo constituye el servidor FTP de Windows, que devuelve las fechas en GMT. Si el proxy detecta que el servidor FTP se está ejecutando en los sistemas Windows, asume que la fecha del directorio está en GMT.
- Algunos servidores FTP especifican la fecha de la información de directorio devuelta en el formato de *Mes Día Año* sólo y no incluye la información de horas y minutos reales de la fecha especificada. Si el servidor FTP no devuelve la información de hora y minutos del archivo, el proxy asume que el archivo se modificó por última vez en la hora y minutos más recientes posibles de la fecha devuelta por el servidor FTP. Por ejemplo, si el servidor FTP devuelve la información de directorio de un directorio indicando que el archivo se ha modificado por última vez el 13 de octubre de 1998 pero no incluye información sobre las horas y minutos, el proxy asume que el archivo se ha modificado a las 11:59:59 de la noche, el 13 de octubre de 1998. A continuación, si el servidor FTP no es un servidor FTP de Windows, el proxy convierte esta fecha de su propio huso horario local a la GMT correspondiente.

Cuando un archivo FTP caduca en la antememoria, el proxy simula el proceso de revalidación if-modified-since de HTTP para el archivo FTP. Lleva a cabo esta

acción volviendo a emitir el mandato FTP LIST para el archivo solicitado, analizando la fecha de archivo de la respuesta devuelta por el servidor FTP y comparando esta fecha con la fecha que el servidor proxy ha generado para la cabecera Last-Modified cuando el archivo se ha recuperado inicialmente. Si la fecha de archivo no se ha modificado, el servidor proxy marca el archivo FTP en antememoria como revalidado, establece una nueva fecha de caducidad del archivo y sirve el archivo de la antememoria en lugar de recuperarlo del servidor FTP de nuevo. Si las dos fechas de archivo no coinciden, el proxy recupera el archivo del servidor FTP de nuevo y coloca la nueva copia con la nueva fecha de archivo.

No siempre es posible obtener la información de directorio del archivo a partir del servidor FTP. Si el proxy no puede determinar la fecha de archivo del archivo FTP, no genera una cabecera Last-Modified del archivo. En su lugar, utiliza el valor especificado para la directiva CacheDefaultExpiry que coincide con el URL para determinar el periodo de tiempo que se debe mantener en archivo en la antememoria. Cuando este periodo de tiempo caduca, el proxy siempre recupera el archivo del servidor FTP de nuevo. Si archivos FTP específicos de la antememoria parecen utilizar la directiva CacheDefaultExpiry con mucha frecuencia y se recuperan con asiduidad (generando un alto volumen de tráfico de red), es recomendable especificar un valor CacheDefaultExpiry más granular para esos archivos específicos. Con esta acción, se consigue mantenerlos en la antememoria durante un periodo de tiempo más largo.

Para especificar los valores de caducidad de la antememoria de los formularios de Configuración y Administración, utilice el formulario **Configuración de antememoria** → **Valores de caducidad de antememoria** → **Límite de tiempo para archivos de antememoria**. Para obtener más detalles sobre cómo establecer las fechas de caducidad del archivo en antememoria, consulte “Caducidad de los archivos” en la página 87.

## Configuración de la antigüedad de antememoria

Para especificar los tiempos de caducidad de los archivos en antememoria, seleccione **Configuración de antememoria** → **Valores de caducidad de antememoria** en los formularios de Configuración y Administración. Los siguientes formularios son de gran utilidad.

### Caducidad basada en URL

Utilice este formulario para establecer el periodo mínimo de tiempo que los archivos se mantienen en antememoria, basándose en sus URL. Puede especificar diferentes comportamientos de colocación en antememoria para las distintas plantillas de petición URL.

Para establecer la caducidad de archivos basada en URL editando el archivo de configuración de proxy, consulte los apartados de referencia del Apéndice B, “Directivas del archivo de configuración”, en la página 177 para obtener información sobre las siguientes directivas:

- “CacheMinHold: especificar el periodo de tiempo que están disponibles los archivos” en la página 198

### Valores de caducidad por omisión

Utilice el formulario **Valores de caducidad de antememoria** para especificar los valores de caducidad por omisión de los archivos usados y sin usar. Puede establecer valores distintos para los archivos HTTP, FTP y Gopher y también para los archivos usados y no usados.

Este formulario contiene opciones adicionales de caducidad de archivos:

- **Habilite la comprobación de caducidad de archivos en antememoria.** Este recuadro de selección se selecciona por omisión. Generalmente, es deseable seleccionar esta opción de modo que el servidor no envíe contenido que no es actual.
- **Inhabilite la recuperación de los archivos de los servidores remotos.** Seleccione esta opción si no desea que el servidor recupere los archivos de los servidores remotos.
- **No coloque en antememoria archivos que caducarán dentro.** Para evitar la colocación en antememoria de los archivos que caducan en breve, especifique el periodo de tiempo con esta opción. Por omisión, los archivos que caducan al cabo de 10 minutos no se colocan en antememoria.

Para establecer los valores de caducidad por omisión editando el archivo de configuración de proxy, consulte las páginas de referencia de las siguientes directivas:

- “CacheDefaultExpiry: especificar el tiempo de caducidad por omisión de los archivos” en la página 193
- “CacheExpiryCheck: especificar si el servidor devuelve los archivos caducados” en la página 194
- “CacheTimeMargin: especificar la duración mínima para colocar en antememoria un archivo” en la página 201
- “CacheUnused: especificar el periodo de tiempo que se deben mantener los archivos en antememoria no utilizados” en la página 201
- “CacheNoConnect: especificar la modalidad de antememoria autónoma” en la página 199

## Valores de Factor de última configuración

Utilice el formulario **Factor de última modificación** para establecer el valor que el proxy utiliza para calcular una fecha de caducidad de los archivos en antememoria sin fecha de caducidad en las cabeceras. Puede establecer diferentes valores para los archivos que coincidan con distintas plantillas de petición. La primera plantilla que coincida se utiliza para calcular la fecha de caducidad.

Para establecer el factor de última modificación editando directamente el archivo de configuración de proxy, consulte “CacheLastModifiedFactor: especificar el valor para determinar las fechas de caducidad” en la página 195.

## Límite de tiempo en antememoria

Utilice el formulario de configuración **Límite de tiempo para archivos de antememoria** para establecer el tiempo máximo que un archivo puede permanecer en la antememoria. Los límites de tiempo se establecen basándose en las plantillas de petición, y se puede especificar que las plantillas se descarten o se vuelvan a validar cuando caduque el límite de tiempo. Estos valores pueden utilizarse para mantener los archivos cuyas fechas de caducidad no son válidas o los archivos con tiempos de caducidad muy largos.

Para establecer el límite máximo de tiempo de caducidad de los archivos en antememoria editando el archivo de configuración de proxy, consulte las siguientes directivas:

- “CacheMaxExpiry: especificar la duración máxima de los archivos en antememoria” en la página 197
- “CacheClean: especificar el periodo de tiempo que se deben mantener los archivos en antememoria” en la página 193

---

## Recogida de basura

Como parte del esfuerzo para mantener en antememoria los URL populares y minimizar el uso de los recursos del sistema, Caching Proxy realiza el proceso de limpieza conocido como *recogida de basura*, mediante el cual se eliminan los archivos antiguos o usados de la antememoria para dejar espacio para los archivos más recientes.

El proceso de recogida de basura examina los archivos del directorio de antememoria e intenta eliminar los archivos caducados para reducir el tamaño de la antememoria y dejar espacio para los archivos nuevos. La recogida de basura se realiza automáticamente, pero algunos valores pueden configurarse para adaptar el proceso a sus necesidades.

### Configuración de la recogida de basura

Para configurar la recogida de basura, seleccione **Configuración de antememoria** -> **Valores de recogida de basura** en los formularios de Configuración y Administración. Utilice este formulario para establecer la *marca alta* y la *marca baja*, que determinan cuándo se inicia y se detiene la recogida de basura. Cuando la cantidad de espacio utilizado en la antememoria alcanza o excede el porcentaje establecido para la marca alta, se inicia la recogida de basura. La recogida de basura continúa hasta que el porcentaje de espacio utilizado en la antememoria es igual al valor establecido para la marca baja o menor que él.

Puede escoger entre dos algoritmos de recogida de basura. El algoritmo **responsetime** optimiza el tiempo necesario para responder a los usuarios mediante la eliminación preferencial de los archivos de gran tamaño de la antememoria. El algoritmo **bandwidth** optimiza el uso de la banda ancha de red mediante la eliminación preferencial de archivos de menor tamaño de la antememoria. Escoja uno de los dos o utilice una combinación de los dos.

Para configurar la recogida de basura editando el archivo de configuración de proxy, consulte los apartados de referencia de las siguientes directivas:

- “Gc: especificar la recogida de basura” en la página 224
- “GcHighWater: especificar cuándo empieza la recogida de basura” en la página 224
- “GcLowWater: especificar cuándo termina la recogida de basura” en la página 224
- “CacheAlgorithm: especificar el algoritmo de antememoria” en la página 192



---

## Capítulo 20. Configuración del agente de carga para la renovación y precarga automática

La mayoría de los servidores proxy de antememoria colocan en antememoria un archivo únicamente después de que lo solicite un usuario. Caching Proxy tiene un agente que proporciona la precarga automática de antememoria. Puede especificar que el agente de antememoria recupere automáticamente los URL especificados, los URL más populares o ambos y los coloca en la antememoria antes de que se soliciten.

En algunos casos, es necesario establecer el nombre de sistema principal del servidor proxy e identificar anotaciones cronológicas de acceso de antememoria antes de cargar previamente la antememoria. Para configurar el agente de antememoria, seleccione **Configuración de antememoria** en los formularios de Configuración y Administración y utilice los formularios **Precarga de antememoria** y **Renovación de antememoria**. Tenga en cuenta que los archivos que representan los resultados de las consultas, es decir, los archivos cuyos URL incluyen el signo de interrogación (?) se colocan en antememoria sólo si la colocación en antememoria está habilitada.

La renovación y precarga automática proporciona las siguientes ventajas:

- La colocación en antememoria se aplica a los URL específicos antes de que un usuario solicite las páginas.
- La antememoria se llena antes de que se servidor esté ocupado con la actividad de usuario.
- Los archivos actuales se proporcionan a los usuarios con mayor rapidez desde la antememoria que si se buscan en la primera petición.

Las desventajas son las siguientes:

- El servidor proxy está ocupado colocando en antememoria las páginas incluso durante las horas de baja actividad del usuario.
- Debe ejercer algún tipo de control sobre lo que se carga automáticamente. La carga de archivos enlazados procedentes de las páginas de alto nivel como, por ejemplo los índices Web y los sitios de búsqueda, pueden generar peticiones para un gran número de páginas.

Para obtener una eficacia óptima, establezca el agente de antememoria para que se ejecute cuando la actividad del servidor sea baja y antes de que el servidor esté ocupado con las peticiones de cliente. A continuación, los archivos están listos en la antememoria para proporcionar un servicio rápido la primera vez que un usuario los solicita. Por omisión, el agente de antememoria se inicia cada noche a las 3 de la mañana hora local.

### Consideraciones especiales de las configuraciones de proxy de retorno:

Por razones de seguridad, cuando utilice una configuración de proxy de retorno, la regla Proxy http:\* debe estar inhabilitada por omisión. (Es decir, esta regla aparece como comentario en el archivo ibmproxy.conf.) Sin embargo, si la regla está inhabilitada, se impide que el agente de antememoria envíe peticiones satisfactoriamente y renueve el contenido de antememoria de Caching Proxy. Un error "403 Prohibido por norma" en los resultados de anotaciones cronológicas de error y no se completará la renovación de antememoria.

Para evitar este problema, utilice `cacheAgentService`, que es un servicio interno proporcionado por Caching Proxy. Para habilitar el servicio, ponga la siguiente directiva `Service` antes de cualquier otra regla de correlación en el archivo `ibmproxy.conf`:

```
Service    /any-valid-string*  INTERNAL:cacheAgentService
```

La variable `any-valid-string` es cualquier serie que sea válida y no esté en conflicto con otras reglas de correlación en el archivo `ibmproxy.conf`.

Tanto Caching Proxy como el agente de antememoria analizan el URI basado en esta directiva de servicio. En vez de enviar el URI directamente a Caching Proxy, el programa de utilidad de agente de antememoria añade el URI como prefijo con el patrón `/any-valid-string` en la directiva `Service`.

Por ejemplo, el agente de antememoria transforma el siguiente URI:

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

en

```
/any-valid-string/http://www.ibm.com/
```

El agente de antememoria envía el URI con el prefijo a Caching Proxy. Cuando Caching Proxy recibe la petición, elimina el prefijo `/any-valid-string/`. Si el URI restante es una unidad totalmente calificada, Caching Proxy sirve la petición directamente sin correlacionar el URI con otras reglas.

Además, el agente de antememoria puede enviar un URI relativo a Caching Proxy. Por ejemplo, si añade `LoadURL /abc/` utilizando la directiva `Service` referenciada previamente en el archivo `ibmproxy.conf`, el agente de antememoria lo transforma en `/any-valid-string/abc/` y lo envía a Caching Proxy. Caching Proxy recibe el URL, elimina el prefijo, correlaciona `/abc/` con otras reglas de correlación y maneja la petición si hay una coincidencia.

Para obtener información sobre la directiva `Service`, consulte “Service: personalizar el paso de servicio” en la página 282.

---

## Establecimiento del nombre de sistema principal del servidor

En las plataformas Linux y UNIX, especifique el nombre de sistema principal del servidor proxy cuya antememoria se está precargando y renovando. En las plataformas Windows, especifique el nombre de sistema principal sólo si el servidor proxy que se está renovando no está en la máquina local. Tenga en cuenta que no es posible renovar la antememoria de un servidor remoto basándose en los archivos a los que se ha accedido con mayor frecuencia, ya que el agente de antememoria local no tiene acceso a las anotaciones cronológicas de acceso de antememoria de un servidor remoto.

Para establecer el nombre de sistema principal del servidor proxy, seleccione **Configuración de antememoria → Renovación de antememoria: Identificar servidor de destino de antememoria** en los formularios de Configuración y Administración.



---

## Precarga de la antememoria con archivos específicos

Para precargar la antememoria con el contenido almacenado en los URL específicos, utilice **Configuración de antememoria** → **Precarga de antememoria** en los formularios de Configuración y Administración. En este formulario, puede especificar los URL para el agente de antememoria que se desea cargar. El proxy recupera esas páginas cuando el agente de antememoria se inicia, independientemente de si se encontraban en la antememoria previamente. Estos URL se especifican en el archivo de configuración de proxy mediante la directiva LoadURL. Este formulario también puede utilizarse para definir los URL cuyo contenido nunca se coloca en antememoria. El acceso a las anotaciones cronológicas de acceso de antememoria no es necesario para este tipo de precarga en antememoria.

Utilice el formulario **Precarga de antememoria** para configurar las siguientes opciones:

- **Renovar la antememoria diariamente:** compruebe este recuadro si desea que el agente de antememoria renueve la antememoria todas las noches. Si no desea iniciar el agente de antememoria, asegúrese de que este recuadro no esté seleccionado.
- **Tiempo de renovación de la antememoria:** si desea que el agente de antememoria se ejecute a una hora distinta de las 3:00 de la mañana hora local, especifique cuándo desea que se inicie.
- **Contenido de antememoria:** en el campo **URL o dirección IP**, especifique los URL que se desea cargar. Para evitar que los URL se precarguen, especifique los URL y pulse **Ignorar** en el recuadro **Estado de la antememoria**.

---

## Precarga de la antememoria con archivos frecuentemente en antememoria

Para precargar automáticamente las páginas a las que se accede frecuentemente, utilice el formulario **Configuración de antememoria** → **Renovación de antememoria**. Esta función requiere anotaciones cronológicas de acceso a antememoria para el servidor proxy. La ubicación y el nombre de las anotaciones cronológicas pueden modificarse; para obtener información consulte la Parte 6, “Supervisión de Caching Proxy”, en la página 149. Los URL más solicitados se determinan automáticamente desde las anotaciones cronológicas de acceso de antememoria. El administrador también puede especificar el número de páginas más solicitadas que se van a precargar en la antememoria. Este número se especifica en el archivo de configuración de proxy mediante la directiva LoadTopCached.

Utilice el formulario **Renovación de antememoria** para configurar las siguientes opciones:

- **Renovar la antememoria diariamente:** compruebe este recuadro si desea que el agente de antememoria renueve la antememoria todas las noches. Si no desea iniciar el agente de antememoria, asegúrese de que este recuadro no esté seleccionado.
- **Tiempo de renovación de la antememoria:** si desea que el agente de antememoria se ejecute a una hora distinta de las 3:00 de la mañana, especifique la hora y minutos cuando desea que se inicie.

- **Identificar servidor de destino de antememoria:** utilice esta opción si desea renovar un servidor distinto de la máquina local. Tenga en cuenta que no puede renovar un servidor remoto basándose en la frecuencia de acceso a archivos específicos.
- **Colocar en antememoria los URL más populares:** especifique el número de los URL que se desean colocar en antememoria procedentes de las anotaciones cronológicas de acceso de antememoria de la noche anterior.
- **Cargar páginas enlazadas:** utilice este valor para configurar la profundización (consulte el apartado siguiente para obtener información detallada sobre la profundización). Establezca el número de niveles que se desea profundizar, y si se deben profundizar en todas las páginas ( **always**), ninguna página (**never**), sólo las páginas especificadas por el administrador (**admin**) o únicamente las páginas más visitadas (**topn**). Asimismo especifique si desea profundizar entre sistemas principales, crear un retraso entre las peticiones y colocar en antememoria las imágenes en línea.
- **Número de hebras:** establece el número máximo de hebras que se van a utilizar para la renovación de la antememoria.
- **Longitud máxima de cola de trabajo** establece la cola máxima que pueden solicitar los URL.
- **Máximo de URL de petición:** establece el número máximo de páginas que se van a cargar. Este número se comprueba antes de que empiece la recuperación de páginas de profundización.
- **Tiempo máximo:** establece el tiempo máximo para que se ejecute el agente de antememoria. Si esta hora se establece en 0 horas 0 minutos, el agente de antememoria se ejecuta hasta el final.

---

## Profundización

La *profundización* es una parte opcional de la característica de renovación de antememoria automática. La mayoría de las páginas Web tienen enlaces con otras páginas con información relacionada, y los usuarios a menudo siguen la ruta que enlaza una página una página con otra y un sitio con otro. La profundización es un modo de colocar en antememoria estas rutas de información lógica. En la profundización, el agente de antememoria sigue un nivel especificado de enlaces (HTML) de hipertexto en las páginas que está cargando y además coloca en antememoria todas esas páginas enlazadas. Las páginas enlazadas pueden residir en el mismo sistema principal como la página de origen o en otros sistemas principales. Se muestra una ilustración en la Figura 1 en la página 97.

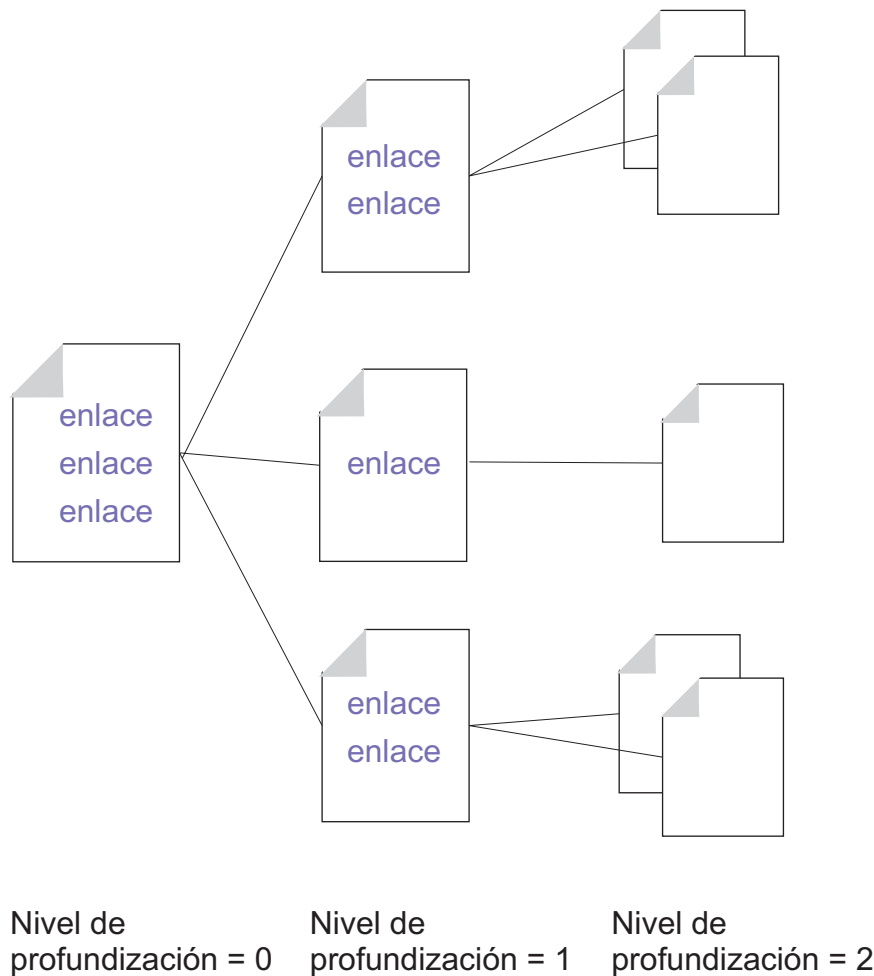


Figura 1. Profundización

Para controlar el proceso de profundización, el administrador especifica al agente de antememoria el número máximo de los URL que puede cargar (el valor por omisión es 2000), el periodo máximo de tiempo que puede ejecutarse (el valor por omisión es de dos horas) y un número máximo de hebras que puede utilizar (el valor por omisión es cuatro). El administrador también puede configurar controles adicionales. Por omisión, la profundización se habilita para dos niveles de la jerarquía y no es posible entre sistemas principales. Adicionalmente, se inserta un retraso entre las peticiones. Para modificar estos valores, consulte “Directivas relacionadas del archivo de configuración de proxy” en la página 98.

El agente de antememoria carga y, a continuación, refresca la antememoria en el siguiente orden:

1. Carga las páginas específicas que ha especificado el administrador.
2. Carga las páginas más conocidas (a las que se accede frecuentemente) a partir de las anotaciones cronológicas de acceso de antememoria.
3. Si el número máximo de páginas no se alcanza en este punto, las páginas adicionales se cargan mediante la profundización.

Tenga en cuenta que el agente de antememoria no comprueba si el número máximo de páginas se ha alcanzado hasta que empieza la profundización entre enlaces. Si el valor del número máximo de páginas (llamado MaxURLs en el archivo de configuración de proxy) es menor que el número de páginas recuperadas en los pasos 1 y 2, no se recupera ninguna página enlazada.

Los siguientes ejemplos muestran cómo el agente de antememoria maneja las prioridades de renovación de antememoria y la profundización, relativas al número máximo de URL que se han especificado (asuma que se ha configurado la profundización para todos estos ejemplos).

valores del archivo de configuración	Resultado
LoadURL http://www.getthis.com/main.html LoadURL http://www.getmetoo.com/welcome.htm LoadTopCached 30 MaxURLs 50	Si las anotaciones cronológicas de acceso de antememoria tienen más de 30 URL únicos, el agente de antememoria recupera main.html, welcome.htm y los 30 primeros URL solicitados basándose en las anotaciones cronológicas de acceso de antememoria. Como no ha alcanzado el valor MaxURLs, recupera y carga hasta 18 URL enlazados de páginas colocadas en antememoria.
LoadURL http://www.joesmith.edu/favorites.html LoadURL http://www.janesmith.edu/dislikes.html LoadTopCached 30 MaxURLs 25	Si las anotaciones cronológicas de acceso de antememoria tienen más de 30 URL únicos, el agente de antememoria recupera favorites.html, dislikes.html y los 30 primeros URL solicitados de las anotaciones cronológicas de acceso de antememoria. No se recupera ningún otro archivo ya que se ha excedido el valor de MaxURLs.
LoadURL http://www.hello.com/hi.htm LoadURL http://www.ballyhoo.com/index.html LoadTopCached 20 MaxURLs 25	Si las anotaciones cronológicas de acceso de antememoria tienen más de 20 URL únicos, el agente de antememoria recupera hi.htm, index.html, los 20 primeros URL solicitados de las anotaciones cronológicas de acceso de antememoria y hasta 3 URL enlazados de las páginas anteriores. No se recupera ningún otro archivo ya que se alcanzado el valor de MaxURLs.

## Directivas relacionadas del archivo de configuración de proxy

El agente de antememoria también puede configurarse editando directamente las directivas del archivo de configuración de proxy. Para obtener información sobre las directivas del archivo de configuración de proxy relacionadas con el agente de antememoria, consulte las siguientes páginas de referencia que aparecen en el Apéndice B, "Directivas del archivo de configuración", en la página 177:

- "AutoCacheRefresh: especificar si se desea utilizar la renovación de antememoria" en la página 190
- "CacheAccessLog: especificar la vía de acceso de los archivos de anotaciones cronológicas de acceso a la antememoria" en la página 191
- "CacheRefreshTime: especificar cuándo se desea iniciar el agente de antememoria" en la página 201

- “DelayPeriod: especificar si debe haber una pausa entre peticiones” en la página 209
- “DelveAcrossHosts: especificar la colocación en antememoria entre dominios” en la página 209
- “DelveDepth: especificar hasta dónde se deben seguir los enlaces durante la colocación en antememoria” en la página 209
- “DelveInto: especificar si el agente de antememoria debe seguir los enlaces” en la página 210
- “IgnoreURL: especificar los URL que no se van a renovar” en la página 229
- “LoadInlineImages: controlar la renovación de imágenes anidadas” en la página 236
- “LoadTopCached: especificar el número de páginas más solicitadas que se van a renovar” en la página 236
- “LoadURL: especificar los URL que se van a renovar” en la página 236
- “MaxUrls: especificar el número máximo de los URL que se van a renovar” en la página 245

---

## Inicio del agente de antememoria manualmente

Si se habilita la renovación de antememoria automática, el agente de antememoria ejecuta automáticamente una operación de renovación a la hora especificada. No obstante, también puede ejecutar el agente de antememoria desde una línea de mandatos cuando lo desee.

El archivo ejecutable es el siguiente:

- En las plataformas Linux y UNIX: `usr/sbin/cacheagt`
- En las plataformas Windows: `server_root\bin\cacheagt.exe`

Donde *server\_root* es la unidad y el directorio donde se ha instalado Caching Proxy (por ejemplo, `C:\Archivos de programa\IBM\edge\cp`).

En las plataformas Linux y UNIX, puede ejecutar automáticamente el agente de antememoria en varios momentos distintos mediante el daemon **cron**. Los trabajos controlados por **cron** se especifican añadiendo una línea al archivo `crontab` del sistema. Una entrada de ejemplo del archivo de mandatos en Linux y UNIX es:

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

Este ejemplo de mandato inicia el agente de antememoria cada día a las 4:45 de la tarde, hora local. Puede utilizar varias entradas para ejecutar el agente de antememoria más de una vez, si así lo desea. Para obtener más información, consulte la documentación del sistema operativo sobre el daemon **cron**.

Al utilizar un daemon **cron** para ejecutar el agente de antememoria, no olvide desactivar la opción de renovación automática, ya sea utilizando la configuración **Configuración de antememoria** → **Renovación de antememoria** o editando el archivo de configuración de proxy. De lo contrario, el agente de antememoria se ejecuta más de una vez al día.



---

## Capítulo 21. Utilización de una antememoria compartida

Es común que un punto de presencia en la Web tenga más tráfico que lo que puede manejar un único servidor. Una solución consiste simplemente en añadir más servidores. No obstante, cuando se utilizan varios servidores proxy de colocación en antememoria, el contenido de una antememoria con frecuencia se solapa con el contenido de las demás antememorias. Además de la innecesaria redundancia en el almacenamiento, el ahorro máximo de banda ancha no se logra ya que un archivo en antememoria vuelve a buscarse en el servidor de origen cuando una petición solicitándolo llega a un servidor proxy que no tiene ese archivo en su propia antememoria. Aunque la colocación duplicada en antememoria puede minimizarse mediante una cadena jerárquica de servidores proxy, este escenario no evita generar tráfico adicional a través de un determinado servidor a la vez que cada enlace adicional de la cadena añade latencia.

El compartimiento de antememoria soluciona estos problemas permitiendo que todas las antememorias compartan su contenido con las demás antememorias. El ahorro de banda ancha se produce debido a los siguientes hechos:

- Los objetos no se buscan varias veces.
- La mayor antememoria lógica combinada genera una mayor Proporción de coincidencias.

Se proporcionan dos métodos para utilizar varias antememorias como si fuesen una antememoria lógica:

- El Acceso a antememoria remota (RCA) es una característica de Caching Proxy, que define una matriz de antememorias de miembro. Un archivo se almacena en una de estas antememorias basadas en la lógica interna.
- Se proporciona un plug-in de Caching Proxy para permitir que el servidor proxy utilice el Protocolo de antememoria de Internet (ICP). Puede utilizar el plug-in ICP en lugar de RCA si desea compartir los datos entre máquinas de Caching Proxy y antememorias que no sean de Caching Proxy.

RCA y ICP pueden utilizarse juntos.

---

### Acceso a antememoria remota

Al planificar RCA, considere las siguientes recomendaciones:

- Los servidor proxy que participan deben estar cerca el uno del otro y estar conectados con enlaces de banda ancha alta (por ejemplo, FDDI, SP2 bus).
- La participación en la matriz RCA debe ser a largo plazo de modo que la configuración sea lo más estable posible.
- Los servidores proxy deben tener posibilidades similares, por ejemplo, CPU, tamaño de memoria y tamaño de antememoria.
- Los cortes de suministro no deben ser frecuentes.
- Es necesario que haya menos de 100 miembros en cualquier matriz.
- Todos los miembros de la matriz debe utilizar la misma versión del software de Caching Proxy.

**Nota:** Si los proxies de la matriz RCA utilizan distintos sistemas operativos Linux (por ejemplo, SUSE y Red Hat), asegúrese de que el usuario "nobody" tenga el mismo UID en todos sus iguales. Compruebe las

entradas del archivo de grupo y de contraseña del directorio /etc/ de todos los sistemas y asigne el mismo UID a "nobody."

El acceso a antememoria remota no es adecuado si se viola alguna de estas condiciones o si distintas organizaciones gestionan distintos servidores que sean miembros de la matriz.

## Configuración del acceso a antememoria remota

Para configurar el acceso a antememoria remota, seleccione **Configuración de antememoria** -> **Acceso a antememoria remota** en los formularios de Configuración y Administración. Los campos de este formularios definen una matriz determinada que comparte una antememoria lógica. Especifique la información necesaria para todos los miembros de la matriz.

Para configurar el acceso a antememoria remota editando el archivo de configuración de proxy, consulte los apartados de referencia del Apéndice B, "Directivas del archivo de configuración", en la página 177 para obtener información sobre las siguientes directivas:

- "ArrayName: nombrar la matriz de antememoria remota" en la página 189
- "Member: especificar un miembro de una matriz" en la página 245

---

## Configuración del plug-in de Protocolo de antememoria de Internet

El plug-in de Protocolo de antememoria de Internet permite que Caching Proxy consulte las antememorias compatibles con ICP que buscan páginas HTML y otros recursos que puedan colocarse en antememoria. Cuando el servidor proxy recibe una petición HTTP, busca su propia antememoria para el recurso. Si no se encuentra el recurso en la antememoria local y el plug-in ICP está habilitado, el servidor proxy encapsula la petición URL en un paquete de consulta ICP y, a continuación, envía este paquete a todas las antememorias de igual de ICP identificadas. Si una antememoria de igual responde que tiene el recurso, el servidor proxy recupera el recurso de esa antememoria de igual. Si dos o más iguales responden afirmativamente, se procesa la primera respuesta. Si ningún igual responde con coincidencias, el servidor original continúa procesando la petición en función de su flujo de trabajo. Por ejemplo, el servidor proxy puede invocar otro plug-in, continuar con la rutina de Acceso a antememoria remota, si RCA está habilitada, o recuperar el recurso solicitado.

## Configuración del plug-in ICP

El plug-in ICP se activa y se configura editando el archivo de configuración de proxy `ibmproxy.conf`. Una directiva `ServerInit`, una directiva `PreExit` o ambas deben añadirse al apartado de directivas de la API del archivo de configuración para utilizar el plug-in ICP. Qué directivas se utilicen depende del rol que Caching Proxy tenga en el sistema ICP:

- Para que Caching Proxy funcione como un servidor ICP, utilice la directiva `ServerInit` para llamar al módulo `icpServer`.
- Para que Caching Proxy funcione como un cliente ICP, utilice la directiva `PreExit` para llamar al módulo `icpClient`.
- Para que Caching Proxy funcione como cliente ICP y como servidor ICP, utilice ambas directivas.
- Utilice las directivas `icpAddress`, `icpMaxThreads`, `icpPeer`, `icpPort`, y `icpTimeout` para configurar los valores que utiliza el plug-in.



Para crear estas directivas, edite el archivo `ibmproxy.conf` manualmente o, si el servidor proxy ya está en ejecución, conéctese al formulario de Configuración y Administración **Configuración de servidor Server -> Proceso de peticiones -> Petición de proceso de API**.

Tenga en cuenta que las directivas de prototipo (en forma de comentarios) se han añadido al apartado API del archivo `ibmproxy.conf`. Estas directivas API aparecen en un orden determinado. Al añadir las directivas API para habilitar nuevas características y módulos de plug-in, ordene las directivas como se muestran en la parte de prototipo del archivo de configuración. Alternativamente, elimine los comentarios de las directivas API y edítelas, si es necesario, para incluir el soporte de todas las funciones o plug-ins deseados.

Las directivas `ServerInit` y `PreExit` tienen dos argumentos: (1) la vía de acceso plenamente cualificada de la biblioteca compartida y (2) la llamada de función. Estos argumentos se delimitan por dos puntos (:). El primer argumento es específico del sistema y depende de dónde están instalados los componentes de plug-in. El segundo argumento se codifica en la biblioteca compartida y debe escribirse exactamente como se muestra.

Todas las directivas deben aparecer en una única línea en el archivo de configuración de proxy.

```
ServerInit vía_acceso_biblioteca_compartida:icpServer
```

Ejemplo de Linux y UNIX:

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

Ejemplo de Windows:

```
ServerInit C:\Archivos de programa\IBM\edge\cp\Bin\plugins\icp\icpplugin.dll:  
icpServer
```

```
PreExit vía_acceso_biblioteca_compartida:icpClient
```

Ejemplo de Linux y UNIX:

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

Ejemplo de Windows:

```
PreExit C:\Archivos de programa\IBM\edge\cp\Bin\plugins\icp\icpplugin.dll:icpClient
```

Para configurar los valores del plug-in, añada o modifique las directivas ICP\* que se facilitan en el archivo de configuración de proxy. Para obtener información adicional, consulte las descripciones de las directivas siguientes.

- “ICP\_Address: especificar la dirección IP para las consultas ICP” en la página 227
- “ICP\_MaxThreads: especificar el número de hebras para las consultas ICP” en la página 227
- “Occupier: especificar un miembro de un clúster ICP” en la página 228
- “ICP\_Port: especificar el número de puerto para las consultas ICP” en la página 228
- “ICP\_Timeout: especificar el tiempo de espera máximo para las consultas ICP” en la página 228
- “PreExit: personalizar el paso de PreExit” en la página 258
- “ServerInit: personalizar el paso de inicialización de servidor” en la página 281



---

## Capítulo 22. Colocación en antememoria de contenidos generados dinámicamente

Sólo se aplica a configuraciones de proxy de retorno.

La función de colocación en antememoria dinámica permite que Caching Proxy se coloque en antememoria el contenido generado dinámicamente en forma de respuestas de JavaServer Pages (JSP) y servlets generados IBM WebSphere Application Server. Se utiliza un módulo del adaptador de Caching Proxy en el servidor de aplicaciones para modificar las respuestas de modo que se puedan colocar en antememoria en el servidor proxy además de en la antememoria dinámica del servidor de aplicaciones. Con esta característica, el contenido generado dinámicamente puede colocarse en antememoria en los límites de la red de modo que el sistema principal que aloja contenidos quede exento de realizar peticiones repetidas al servidor de aplicaciones cuando más de un cliente solicite el mismo contenido.

**Nota:** La característica de colocación en antememoria dinámica no permite que el servidor proxy coloque en antememoria los resultados de las consultas URL. Para colocar en antememoria los resultados de la consulta, configure los filtros de colocación en antememoria, que se describen en el Capítulo 18, “Control de los elementos colocados en antememoria”, en la página 83 y en la documentación de referencia de las directivas en “CacheQueries: especificar las respuestas de antememoria a los URL que contienen un signo de interrogación (?)” en la página 200. Los resultados de la consulta de los servidores de origen que no son IBM WebSphere Application Servers pueden colocarse en antememoria.

En ocasiones es necesario habilitar la colocación en antememoria de consultas para que funcione la característica de colocación en antememoria dinámica, por ejemplo, si los servlets utilizan los URL en forma de consulta. El servidor proxy considera cualquier URL que contenga un signo de interrogación (?) como una consulta.

La colocación en antememoria del contenido generado dinámicamente ofrece las siguientes ventajas:

- Reduce la carga en los sistemas principales que alojan contenidos.
- Reduce la carga en los servidores de aplicaciones.
- Acelera el envío de recursos solicitados a los usuarios finales.
- Reduce el uso de ancho de banda entre los servidores.
- Mejora la escalabilidad de los sitios Web que crean o sirven el contenido generado dinámicamente.

El servidor de aplicaciones sólo exporta páginas públicas compuestas completamente para la antememoria de proxy. El proxy no coloca en antememoria las páginas privadas. Por ejemplo, una página generada dinámicamente desde un sitio público que facilita el pronóstico del tiempo actual puede exportarse mediante IBM WebSphere Application Server y colocarse en antememoria mediante Caching Proxy. No obstante, una página generada dinámicamente que enumera el contenido del carro de la compra de un usuario no puede colocarse en antememoria mediante el servidor proxy. Asimismo, para colocar en antememoria

una página generada dinámicamente, todos los subcomponentes de esa página también deben poder colocarse en antememoria.

Los archivos dinámicos en antememoria no caducan del mismo modo que lo hacen los archivos normales; pueden invalidarse mediante el servidor que los ha generado.

Las entradas de la antememoria dinámica se invalidan en las siguientes circunstancias:

- El recolector de basura de la antememoria dinámica elimina una entrada debido a la congestión de la antememoria.
- El tiempo de espera establecido en la entrada de servlet (servletcache.xml) o en la directiva ExternalCacheManager del proxy caduca.
- Un aplicación o un agente externos invocan a las API de antememoria dinámica para invalidar las entradas de antememoria.

La invalidación de las entradas de antememoria dinámica se realiza mediante la generación de un mensaje de invalidación para la instancia específica del plug-in de colocación en antememoria dinámica de Caching Proxy. Caching Proxy recibe los mensajes de invalidación como apéndices del localizador de recursos /WES\_External\_Adapter. A continuación, Caching Proxy borra las entradas no válidas de la antememoria.

La colocación en antememoria dinámica requiere los siguientes pasos de configuración.

- Configuración de IBM WebSphere Application Server:
  - Configure todos los servidores de aplicaciones para realizar la colocación en antememoria dinámica local.
  - Configure todos los servidores de aplicaciones para utilizar el adaptador de antememoria externa.
  - Especifique qué antememorias externas pueden utilizarse para cada archivo de servlet y JSP que puede colocarse en antememoria.
- Configuración de Caching Proxy:
  - Habilita Caching Proxy para utilizar el plug-in de colocación en antememoria dinámica.
  - Especifique los recursos a partir de los cuales se colocará en antememoria el contenido dinámico.

---

## Configuración de IBM WebSphere Application Server para la antememoria de proxy

### Configuración de la colocación en antememoria dinámica en los servidores de aplicaciones

Siga las instrucciones de la documentación de IBM WebSphere Application Server para configurar el servidor de aplicaciones a fin de que utilice la antememoria dinámica local (también denominada la antememoria de fragmentos dinámica). La antememoria de fragmentos dinámica interacciona con la antememoria externa de Application Server Caching Proxy.

## Configuración del adaptador del servidor de aplicaciones

IBM WebSphere Application Server se comunica con Caching Proxy utilizando un módulo de software denominado adaptador de antememoria externa, que se instala con Application Server.

**Nota:** Consulte el sitio Web de soporte de IBM WebSphere Application Server para obtener una nota técnica sobre la configuración de la colocación en antememoria dinámica.

---

## Configuración de Caching Proxy para la colocación en antememoria dinámica

Para habilitar el servidor proxy para que coloque en antememoria el contenido generado dinámicamente (resultados de servlets y JSP), debe realizar dos cambios en el archivo de configuración de proxy `ibmproxy.conf`. El primer cambio habilita el módulo de plug-in de colocación en antememoria dinámica mientras que el segundo lo configura para que reconozca los orígenes del contenido dinámico que se puede colocar en antememoria.

### Establecimiento de la directiva Service para habilitar el plug-in de colocación en antememoria dinámica

Se utiliza una directiva API para el paso Service con el fin de habilitar el plug-in de colocación en antememoria dinámica. Para crear esta directiva, edite el archivo `ibmproxy.conf` manualmente o, si el servidor proxy ya está en ejecución, utilice los formularios de Configuración y Administración para seleccionar **Configuración de servidor** → **Proceso de peticiones** → **Petición de proceso de API**. El contenido de la directiva se muestra en ejemplo que aparecen posteriormente en este apartado.

Existe una directiva Service prototipo para habilitar la colocación en antememoria dinámica como un comentario en el apartado API del archivo `ibmproxy.conf`. Tiene la cabecera JSP Plug-in. Tenga en cuenta que las directivas API prototipo aparecen en un orden determinado. Al añadir las directivas API para habilitar nuevas características y módulos de plug-in, ordene las directivas como se muestran en la parte de prototipo del archivo de configuración. Opcionalmente, puede eliminar los caracteres de comentario de las directivas API prototipo y editarlas si es necesario para incluir soporte para todas las funciones o plug-ins deseados.

Establezca la directiva Service como se muestra en los siguientes ejemplos. Tenga en cuenta que todas las directivas deben aparecer en una única línea en el archivo de configuración de proxy; estos ejemplos en ocasiones contienen divisiones de línea para que sean legibles.

- Para AIX:

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

- Para Solaris:

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

- Para Linux:

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

- Para Windows:

```
Service /WES_External_Adapter C:\Archivos de programa\IBM\edge\cp\bin\plugins\  
dynacache\dyna_plugin.dll:exec_dynacmd
```

Si el software de Caching Proxy se instala en un directorio que no sea el directorio por omisión, sustituya la vía de acceso por la vía de acceso de estos ejemplos.

## **Establecimiento de la directiva ExternalCacheManager para especificar los orígenes de archivo**

Todos los Caching Proxy también deben configurarse para que reconozcan el origen de los archivos generados dinámicamente. Añada una directiva ExternalCacheManager al archivo ibmproxy.conf para todos los servidores de aplicaciones que colocan en antememoria el contenido generado dinámicamente en este servidor proxy. Esta directiva especifica un servidor de WebSphere Application Server que coloca en antememoria los resultados del proxy y establece un tiempo de caducidad máximo para el contenido de ese servidor. Encontrará más información detallada en “ExternalCacheManager: configurar Caching Proxy para la colocación en antememoria dinámica desde IBM WebSphere Application Server” en la página 220.

El ID de servidor utilizado en la directiva ExternalCacheManager debe coincidir con el ID de grupo del apartado de grupo de antememoria externa del archivo dynacache.xml del servidor de aplicaciones.

Para el ejemplo anterior, añada la siguiente entrada a todos los archivos ibmproxy.conf de proxy.

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

Caching Proxy coloca en antememoria sólo el contenido de un servidor de IBM WebSphere Application Server cuyo ID de grupo coincida con una entrada ExternalCacheManager del archivo ibmproxy.conf.

---

## Capítulo 23. Ajuste de la antememoria del servidor proxy

Cuando se habilita la colocación en antememoria, la velocidad de los dispositivos de almacenamiento de antememoria es crítica para el rendimiento de Caching Proxy. Este apartado proporciona sugerencias sobre cómo elegir un tipo de almacenamiento de antememoria y configurar los dispositivos de almacenamiento de antememoria para un mejor rendimiento.

---

### Elección del soporte de almacenamiento de antememoria

Caching Proxy puede utilizar dos tipos distintos de soporte de almacenamiento de antememoria:

- Memoria
- Particiones de disco sin procesar

Una antememoria de memoria proporciona la recuperación de archivos más rápida, aunque el tamaño de una antememoria de memoria está limitada por la cantidad de memoria disponible en la máquina del servidor proxy. Una antememoria de disco, compuesta de una o más particiones de disco sin procesar, es más lenta que una antememoria de memoria pero permite tamaños de antememoria mayores en la mayoría de los casos.

---

### Optimización del rendimiento de antememoria de disco

Es necesario que las particiones de dispositivo utilizadas para la colocación en antememoria de discos estén dedicadas a la antememoria; es decir, no utilice estos discos físicos para contener ningún otro sistema de archivos y no los utilice tampoco para ningún otro propósito que no sea el de almacenar la antememoria de proxy. Adicionalmente, no utilice la compresión de datos en ningún disco utilizado para la antememoria de proxy porque reduce el rendimiento.

Todos los dispositivos de almacenamiento de antememoria, ya sea un disco ya un archivo, incurren en una actividad adicional de la memoria del servidor proxy. En general, la utilización de un disco físico entero como un único dispositivo de antememoria proporciona el mejor rendimiento. La utilización de RAID u otros mecanismos para combinar varios discos físicos en un único disco lógico puede ser contraproducente. Si desea utilizar varios discos, especifíquelos como varios dispositivos de antememoria mediante el formularios de configuración **Valores de antememoria** o mediante la edición de la directiva CacheDev del archivo de configuración de proxy. Este método permite que el servidor proxy controle el paralelismo de escritura y lectura en varios discos y no confía en el rendimiento del sistema operativo o un subsistema de disco.

---

### Recogida de basura de antememoria

La recogida de basura de antememoria del servidor proxy elimina los archivos caducados de la antememoria, liberando espacio para la colocación en antememoria de archivos para peticiones nuevas. La recogida de basura se desencadena automáticamente cuando la cantidad de espacio usado en la antememoria alcanza un límite especificado por el administrador que se denomina *marca alta* y continúa hasta que la cantidad de espacio utilizado alcanza una *marca baja*.

Como la rutina de recogida de basura utiliza unos recursos de CPU mínimos y no afecta a la disponibilidad de material en antememoria caducado, no es necesaria la configuración de la recogida de basura para que se ejecute en momentos específicos.

Para mejorar el rendimiento de la recogida de basura, puede establecer la marca alta y la marca baja. Puede configurar el tipo de algoritmo utilizado para la recogida de basura. Consulte “Recogida de basura” en la página 92 para obtener más información sobre cómo modificar la recogida de basura.

---

## Optimizaciones específicas de la plataforma

A continuación aparecen una serie de sugerencias adicionales para optimizar el rendimiento de antememoria en todas las plataformas.

### AIX

Cree un único volumen lógico de disco, preferiblemente utilizando todas las particiones físicas (PP) disponibles. Por ejemplo, dado un disco de 9 GB, cree un volumen lógico de 9 GB denominado cpcache1. Formatéelo y especifíquelo como un dispositivo de antememoria de proxy utilizando el volumen lógico sin procesar, /dev/rcpcache1.

### HP-UX y Solaris

En el dispositivo de antememoria, cree una única partición (o porción) que utilice todo el tamaño del disco. Por ejemplo, en un disco de 9 GB, cree una partición de 9 GB denominada c1t3d0s0. Formatéela y especifíquela como un dispositivo de antememoria de proxy utilizando el dispositivo sin procesar, /dev/rdisk/c1t3d0s0.

### Windows

Cree una única partición utilizando todo el tamaño del disco. Por ejemplo, en un disco de 9 GB, cree una partición de 9 GB denominada i:. Formatéela y especifíquela como un dispositivo de antememoria de proxy utilizando el dispositivo sin procesar, \\.\i:.

Encontrará información sobre cómo configurar la antememoria del servidor proxy en la Parte 4, “Configuración de la antememoria y el servidor proxy”, en la página 73.



---

## Parte 5. Configuración de la seguridad de Caching Proxy

En esta parte se proporciona información sobre la seguridad básica, cómo utilizar SSL con Caching Proxy, cómo habilitar el hardware criptográfico y cómo utilizar el plug-in de IBM Tivoli Access Manager (anteriormente Tivoli Policy Director) y el módulo de autorización PAC-LDAP.

Esta parte contiene los siguientes capítulos:

Capítulo 24, “Acerca de la seguridad del servidor proxy”, en la página 113

Capítulo 25, “Configuraciones de protección del servidor”, en la página 115

Capítulo 26, “SSL (Secure Sockets Layer)”, en la página 119

Capítulo 27, “Habilitación del soporte de hardware criptográfico”, en la página 135

Capítulo 28, “Utilización del plug-in de Tivoli Access Manager”, en la página 137

Capítulo 29, “Utilización del módulo de autorización PAC-LDAP”, en la página 139



---

## Capítulo 24. Acerca de la seguridad del servidor proxy

Cualquier servidor accesible desde Internet corre el riesgo de atraer la atención de modo indeseado sobre el sistema en el se ejecuta. Es posible que las personas no autorizadas intenten averiguar las contraseñas, los archivos de actualización y los archivos o leer los datos confidenciales. Parte de la atracción de Internet es su accesibilidad. No obstante, la Web está abierta tanto a una utilización positiva como al abuso.

Los siguientes apartados describen cómo controlar quién tiene acceso a los archivos de su servidor de Caching Proxy.

Caching Proxy da soporte a las conexiones SSL (Secure Sockets Layer), en las que las transmisiones seguras que impliquen el cifrado y descifrado se establecen entre el navegador de cliente y el servidor de destino (bien un servidor de contenido, bien un servidor sustituto).

Cuando Caching Proxy se configura como sustituto, puede establecer conexiones seguras con los clientes, con los servidores de contenido o ambos. Para habilitar las conexiones SSL, en los formularios de Configuración y Administración, seleccione **Configuración de proxy -> Valores SSL**. En este formulario, seleccione el recuadro de selección **Habilitar SSL** y especifique una base de datos de conjunto de claves y un archivo de contraseñas de la base de datos de conjunto de claves.

Cuando Caching Proxy se configura como un servidor proxy de reenvío, sigue un protocolo de paso a través denominado *Túneles SSL* para pasar peticiones cifradas entre el cliente y el servidor de contenido. La información cifrada no se coloca en antememoria porque el servidor proxy no descifra las peticiones de túnel. En una instalación de proxy de reenvío, se habilitan los túneles SSL. Para inhabilitarlos, en los formularios de Configuración y Administración, seleccione **Configuración de proxy -> Valores de proxy** y deseccione el cuadro de selección **Túneles SSL** de este formulario.

Puede tomar varias precauciones básicas para proteger el sistema.

- Coloque un servidor diseñado para el acceso público en una red independiente de la red local o interna.
- Inhabilite los programas de utilidad que permitan a los usuarios remotos acceder a los procesos internos del servidor. En concreto, se recomienda inhabilitar los clientes **telnet**, **TN3270**, **rlogin** y **finger** del sistema donde se está ejecutando el servidor.
- Utilice los cortafuegos y los filtros de paquetes.

Los filtros de paquetes le permiten definir desde donde pueden venir los datos y a dónde pueden ir. Puede configurar el sistema para rechazar ciertas combinaciones de origen y destino.

Un cortafuegos separa una red interna de una red accesible públicamente como, por ejemplo, Internet. El cortafuegos puede ser un grupo de sistemas o un único sistema que actúe como una pasarela en ambas direcciones, regulando y haciendo un seguimiento del tráfico que pase por él. IBM Firewall es un ejemplo de software de cortafuegos.

- Controle los scripts CGI. La utilización de scripts CGI en un servidor Web puede poner en riesgo la seguridad ya que es posible que estos scripts muestren varias

variables de entorno que incluyan datos confidenciales como, por ejemplo, los ID de usuario y contraseñas. Asegúrese de que sabe exactamente lo que puede hacer un programa CGI antes de ejecutarlo en el servidor y controle quién tiene acceso a los scripts CGI del servidor.

**Nota:** Si el Asistente de configuración se utiliza para configurar el servidor proxy, debe crearse una norma de correlación en las peticiones de proxy recibidas mediante el puerto 443 para habilitar SSL. Para obtener más información, consulte “Definición de normas de correlación” en la página 44.

Ejemplos:

```
Proxy /* http://content server :443
```

o

```
Proxy /* https://content server :443
```

---

## Capítulo 25. Configuraciones de protección del servidor

En este capítulo se describe cómo proteger los datos y archivos del servidor mediante las configuraciones de protección. Las configuraciones de protección se desencadenan basándose en la petición que recibe el servidor, específicamente en el directorio, archivo o tipo de archivo específicos a los que se dirige la petición. En una configuración de protección, las subdirectivas controlan cómo se otorga o deniega el acceso basándose en las características de los directorios o archivos que se van a proteger.

---

### Utilización de los formularios de Configuración y Administración para establecer la protección

Para definir una configuración de protección y cómo se aplica seleccione **Configuración de servidor** → **Protección de documentos** en los formularios de Configuración y Administración. Utilice este formulario para los pasos siguientes:

1. Establezca el orden de esta norma de protección.

Las normas de protección se aplican en el orden en el que se enumeran en la tabla del formulario de configuración. En general, las normas se enumeran de lo específico a lo genérico.

Utilice el menú desplegable y los botones para especificar la colocación de una norma de protección.

2. Defina una plantilla de petición.

La protección se activa basándose en las plantillas de petición, que se comparan con el contenido de las peticiones que los clientes envían al servidor proxy.

Una *petición* es la parte de un URL completo que sigue al nombre del sistema principal del servidor. Por ejemplo, si su servidor se denomina `fine.feathers.com` y un navegador especifica el URL `http://fine.feathers.com/waterfowl/schedule.html`, el servidor recibe la petición `/waterfowl/schedule.html`. Las plantillas de petición especifican los nombres de archivo o de directorio, o ambos, que están sujetos a la protección. Por ejemplo, algunas peticiones que activan la protección basándose en la plantilla de petición recién descrita (`/waterfowl/schedule.html`) incluyen `/waterfowl/*` y `/*schedule.html`.

Escriba la plantilla de petición en el campo **Plantilla de petición de URL**.

3. Defina una configuración de protección.

Una configuración de protección indica a Caching Proxy qué hacer con una petición que coincida con una plantilla de petición. Puede utilizar una configuración de protección con nombre o definir una nueva configuración en el formulario **Protección de documentos**.

Para utilizar una configuración determinada, pulse el botón de selección **Protección con nombre** y escriba el nombre en el campo facilitado. Para definir una nueva configuración, pulse el botón de selección **En línea** y siga la instrucciones que se facilitan (consulte el paso 6).

4. Elija una dirección del solicitante (opcional).

Se pueden aplicar distintas normas a las peticiones de diferentes direcciones de servidor. Por ejemplo, es posible que desee aplicar una configuración de protección distinta a las peticiones de archivos de anotaciones cronológicas cuando estas peticiones se reciben desde direcciones IP asignadas a su empresa.

**Nota:** Para que las direcciones del solicitante se filtren, debe habilitarse la búsqueda DNS. Consulte “DNS-Lookup: especificar si el servidor debe buscar los nombres de nombre de sistema principal de cliente” en la página 214.

Si desea incluir la dirección del solicitante en la norma, escríbala en el campo **Dirección IP de servidor o nombre de sistema principal**.

5. Pulse **Someter**.

Si ha utilizado una configuración de protección con nombre, no es necesaria más entrada. Si ha seleccionado una configuración de protección en línea o especificado una configuración determinada que no exista, el sistema abre formularios adicionales.

6. Establezca los detalles de protección.

Si no ha especificado una configuración de protección con nombre existente, se abre un formulario adicional, en el que puede especificar qué usuarios pueden acceder a los documentos o directorios que coincidan con la plantilla de petición y qué acciones se les permiten a esos usuarios.

- **Valores de autenticación de contraseña:** especifica el archivo de contraseñas, el archivo de grupo, o ambos, que se va a utilizar para la autenticación de usuario. Asimismo, especifica el nombre que se utiliza para identificar el servidor cuando solicita el nombre y contraseña de un solicitante.

**Nota:** Algunos navegadores colocan en antememoria los ID de usuario y contraseñas y los asocian con un ID de servidor. Es posible que los usuarios consideren más cómodo que siempre utilice el mismo ID de servidor con el mismo archivo de contraseñas.

- **Permisos:** especifique qué usuarios o grupos están autorizados a leer, escribir o eliminar los archivos protegidos.

7. Pulse **Someter**.

8. Reinicie el servidor.

---

## Utilización de las directivas del archivo de configuración para establecer la protección

Para establecer la protección mediante la edición directa del archivo de configuración de Caching Proxy, primero debe estar familiarizado con los siguientes temas:

- Las diferencias entre las directivas Protect, defProt y Protection
    - La directiva Protect establece la protección mediante el enlace entre una plantilla de petición y una configuración de protección. Consulte “Protect: activar una configuración de protección de las peticiones que coinciden con una plantilla” en la página 258 para obtener más información.
    - La directiva defProt establece una configuración de protección por omisión para una determinada plantilla de petición. Consulte “DefProt: especificar la configuración de protección por omisión de las peticiones que coinciden con una plantilla” en la página 206 para obtener más información.
    - La directiva Protection se utiliza para definir una configuración de protección con nombre. Consulte “Protection: definir una configuración de protección con nombre dentro del archivo de configuración” en la página 263 para obtener más información.
  - Cómo la protección interactúa con el direccionamiento de peticiones
- Las directivas de direccionamiento de peticiones como Map, Exec, Pass y Proxy se utilizan para controlar qué peticiones acepta el servidor y cómo redirecciona

las peticiones a ubicaciones de archivo reales, El direccionamiento de peticiones utiliza el mismo tipo de plantillas de petición que las directivas de protección. Dado que se ejecutan las indicaciones asociadas con la primera plantilla coincidente de cada petición, deben enumerarse las directivas de protección antes que las directivas de direccionamiento en el archivo de configuración para que la protección se realice correctamente. Para obtener más información, consulte “Protect: activar una configuración de protección de las peticiones que coinciden con una plantilla” en la página 258.

- La diferencia entre las configuraciones de protección en línea y con nombre  
La directiva Protect puede utilizarse para especificar una configuración de protección en línea o puede hacer referencia a una configuración con nombre existente. La sintaxis de los dos tipos de sentencias es ligeramente distinta. Para obtener información, consulte “Protect: activar una configuración de protección de las peticiones que coinciden con una plantilla” en la página 258.
- Cómo escribir una configuración de protección  
Una configuración de protección es una serie de sentencias que utilizan las subdirectivas de protección. Encontrará la sintaxis y la información de referencia sobre cómo escribir las configuraciones de protección en el Apéndice B, “Directivas del archivo de configuración”, en la página 177; consulte los siguientes apartados de referencia:
  - “Protect: activar una configuración de protección de las peticiones que coinciden con una plantilla” en la página 258
  - “Protection: definir una configuración de protección con nombre dentro del archivo de configuración” en la página 263
  - “Subdirectivas de protección: especificar cómo proteger un conjunto de recursos” en la página 264

---

## Valores de protección por omisión

El archivo de configuración de proxy por omisión incluye una configuración de protección que requiere un ID y una contraseña de administrador para acceder a los archivos del directorio /admin-bin/. Este valor limita el acceso a los formularios de Configuración y Administración.





---

## Capítulo 26. SSL (Secure Sockets Layer)

SSL (Secure Sockets Layer) es un sistema que cifra automáticamente la información antes de enviarla a través de Internet y la descifra en el otro extremo antes de utilizarla. Con estas operaciones se protege la información confidencial como, por ejemplo, los dígitos de las tarjetas de crédito, mientras se transmite a través de Internet.

Caching Proxy utiliza SSL para proteger los servidores sustitutos y proporcionar una administración remota segura como se describe en los apartados siguientes. SSL también puede utilizarse para proteger las conexiones con los servidores de programa de fondo (por ejemplo, los servidores de contenido y de aplicaciones) además de las comunicaciones entre el servidor proxy y sus clientes.

Para el proxy de reenvío, Caching Proxy da soporte a los túneles SSL, que ignora SSL y reenvía los datos ya cifrados sin modificarlos.

---

### Protocolo de enlace SSL

La protección se inicia cuando se envía una petición de conexión segura desde una máquina a otra, por ejemplo, cuando un navegador envía una petición a un servidor proxy sustituto. La sintaxis de petición `https://` en lugar de `http://` indica al navegador que envíe la petición al puerto 443, que es donde el servidor escucha las peticiones de conexiones seguras, y no al puerto 80 para las peticiones rutinarias. Para establecer una sesión segura entre el navegador y el servidor, las dos máquinas realizan un intercambio denominado *protocolo de enlace SSL* para acordar una especificación de cifrado y seleccionar una clave que se utilice para cifrar y descifrar la información. Las claves se generan automáticamente y caducan cuando lo hace la sesión. Un escenario típico para SSL Versión 3 es el que se describe a continuación:

1. Saludo del cliente

El cliente inicia una sesión SSL con Caching Proxy mediante el envío de un mensaje de saludo del cliente que describe las posibilidades de cifrado del cliente.

2. Saludo del servidor

El servidor envía su certificado al cliente y elige el conjunto de cifrado que se va a utilizar para el cifrado de datos.

3. Finalización del cliente

El cliente envía la información de claves de cifrado que se utilizan para crear las claves de cifrado simétricas de los datos cifrados. Este material de claves se conoce como *secreto premaestro* y se cifra con la clave pública del servidor, que se obtiene del certificado del servidor; consulte “Gestión de claves y certificados” en la página 123. Tanto el servidor como el cliente pueden derivar las claves de cifrado simétricas de lectura y escritura a partir del secreto premaestro.

4. Finalización del servidor

El servidor envía una confirmación final y un código de autenticación de mensajes (MAC) para todo el protocolo de establecimiento de comunicación).

5. Validación del cliente

El cliente envía un mensaje para validar el mensaje de finalización del servidor.

## 6. Flujo de datos seguros

Si el cliente valida el mensaje de finalización del servidor, comienza el flujo de datos cifrado.

La utilización de Caching Proxy como punto final para las conexiones seguras puede reducir la carga de los servidores de contenido o de aplicación. Cuando Caching Proxy mantiene una conexión segura, realiza el cifrado, el descifrado y la creación de claves, que son todas operaciones de uso intensivo de la CPU. Asimismo, Caching Proxy le permite configurar los tiempos de espera de sesiones SSL para maximizar la utilización de todas las claves.

### Limitaciones de SSL

Las siguientes limitaciones se aplican a SSL en Caching Proxy de WebSphere Application Server:

- Caching Proxy no puede utilizarse como una autoridad certificadora (consultar “Gestión de claves y certificados” en la página 123).
- Es posible que algunos navegadores no den soporte a toda la tecnología de cifrado utilizada en Caching Proxy.

## Ajuste de rendimiento de SSL

Durante volúmenes de tráfico altos de HTTPS, el servidor Caching Proxy puede causar un uso elevado de la CPU. Cambios en el ajuste de una variable de entorno (GSK\_V3\_SIDCACHE\_SIZE) y de una directiva de proxy (SSLV3Timeout) pueden ayudar al servidor proxy a gestionar la carga y reducir el uso de CPU.

El ID de sesión de SSL identifica las sesiones SSL reutilizables, incluidas las claves de cifrado o descifrado utilizadas por ambos navegadores y servidores, y se utiliza para evitar protocolos de enlace SSL innecesarios en las conexiones nuevas, que consumen buena parte del tiempo de CPU del servidor. La biblioteca de GSKit para el servidor Caching Proxy da soporte al ID de sesión SSL e incluye una antememoria de ID de sesión SSL. Por omisión, la antememoria del ID de sesión SSL contiene 512 entradas. Cuando se alcanza el límite de la entrada, la entrada de sesión más antigua se eliminará y la nueva entrada se añadirá a la antememoria.

Utilice la variable de entorno GSK\_V3\_SIDCACHE\_SIZE para cambiar el tamaño por omisión de la antememoria de ID de sesión SSL. Un valor válido de la variable está entre 1 y 4096. Si aumenta el tamaño, aumentará el tiempo de búsqueda necesario para localizar una sesión SSL en antememoria. No obstante, el aumento del tiempo de búsqueda es insignificante comparado con la actividad general que es necesaria para establecer una conexión SSL. Si aumenta el tamaño de la antememoria, ayudará al servidor proxy a gestionar más sesiones SSL simultáneas y reducir el uso de la CPU cuando el servidor proxy esté por debajo de cargas elevadas de HTTPS.

Caching Proxy también tiene una directiva ajustable, SSLV3Timeout. (Consulte el “SSLV3Timeout: especificar el tiempo de espera antes de que caduque una versión de SSLV3” en la página 288.) El valor por omisión de la directiva es de 1000 segundos. Esta directiva define la duración de una sesión SSL en la antememoria de sesión. Si ninguna conexión SSL entrante utiliza una sesión SSL existente y la duración de la sesión sobrepasa este valor, la sesión será eliminada de la antememoria de sesión. Es recomendable que ajuste el valor de SSLV3Timeout a la duración típica de una sesión segura de cliente. Si el tiempo de espera es demasiado corto, puede reducir el rendimiento del proxy porque se necesitan

varias sesiones de protocolo de enlace SSL para completar una sola sesión segura. Sin embargo, si el valor es demasiado grande, también puede perjudicar la seguridad de una sesión segura.

## Túneles SSL

Sólo se aplica a configuraciones de proxy de reenvío.

Cuando Caching Proxy se configura como un proxy de reenvío, utiliza los túneles SSL para dar soporte a las conexiones seguras entre los clientes y los servidores de contenido. En los túneles SSL, los datos cifrados se pasan a través del servidor proxy sin experimentar modificaciones. Como el servidor proxy no descifra los datos, no se da soporte en los túneles SSL a las funciones que requieren que el servidor proxy lea las peticiones o las cabeceras de documento. Asimismo, las peticiones de túnel no se colocan en antememoria.

Figura 2 muestra cómo una conexión se establece mediante los túneles SSL.

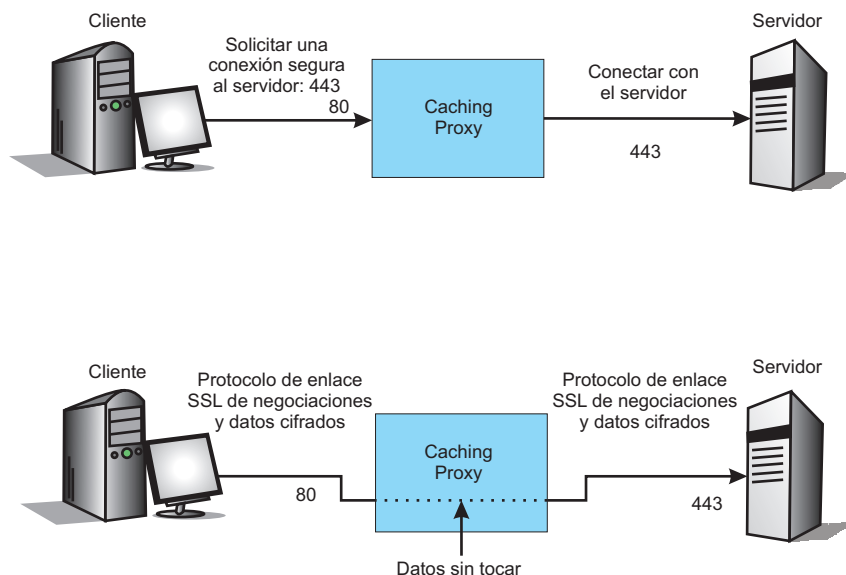


Figura 2. Túneles SSL

El proceso de túneles SSL es el siguiente:

1. El cliente realiza una petición de túnel: `CONNECT nombre_sistppal-servidor:puerto HTTP/1.1` (o `HTTP/1.0`). El número de puerto es opcional y es 443 generalmente. El navegador del cliente enviará automáticamente la petición `CONNECT` primero al servidor proxy para cada petición HTTPS si el proxy de reenvío se ha configurado en el navegador.
2. El proxy acepta la conexión en su puerto 80, recibe la petición y se conecta al servidor de destino en el puerto solicitado por el cliente.
3. El proxy responde al cliente que se ha establecido una conexión.
4. El proxy difunde mensajes de protocolo de enlace en ambas direcciones: desde el cliente al servidor de destino y desde éste al cliente.
5. Después de que se haya completado el protocolo de enlace seguro, el proxy envía y recibe datos cifrados para que se descifren en el cliente o en el servidor de destino.

6. Si el cliente o el servidor de destino solicita el cierre de cualquiera de los puertos, el servidor proxy cierra ambas conexiones (los puertos 443 y 80) y continúa con su actividad normal.

## Configuración de túneles SSL

En un valor de proxy de reenvío, únicamente están disponibles los túneles SSL. Para habilitar los túneles SSL, seleccione **Configuración de Proxy -> Valores de proxy** en los formularios de Configuración y Administración.. Seleccione el recuadro de selección **Túneles SSL**.

El método CONNECT (que se habilita por omisión) también debe habilitarse para las conexiones de túneles SSL. Para habilitarlo en los formularios de configuración, seleccione **Configuración de servidor -> Proceso de peticiones** y utilice el formulario **Métodos HTTP**.

Se proporcionan tres opciones (OutgoingPorts, OutgoingIPs, IncomingIPs) para la directiva Enable CONNECT para la seguridad ampliada de túneles SSL. Es necesario que especifique un valor para OutgoingPorts como mínimo; en caso contrario, el método CONNECT no se habilitará.

- OutgoingPorts (para limitar el acceso para túneles SSL según los puertos del servidor remoto). El formato es,

```
Enable CONNECT OutgoingPorts [all | [port1|port1-port2|port1-*],...]
```

Para permitir que los clientes se conecten sólo al puerto 443 de los servidores remotos para túneles SSL, establezca las directivas siguientes. (Normalmente, el puerto 443 es para peticiones HTTPS en el servidor remoto.)

```
Enable CONNECT OutgoingPorts 443
SSLTunneling on
```

Para permitir que los clientes se conecten a cualquier puerto de los servidores remotos para túneles SSL, establezca las directivas siguientes:

```
Enable CONNECT OutgoingPorts all
SSLTunneling on
```

Para permitir que los clientes se conecten a los puertos 80, 8080-8088 y 9000 y superiores de los servidores remotos para túneles SSL, establezca las directivas siguientes:

```
Enable CONNECT OutgoingPorts 80,8080-8088,9000-*
SSLTunneling on
```

Los puertos y los rangos de puertos se separan con una coma sin dejar ningún espacio en la lista.

IMPORTANTE: para las configuraciones de proxy de reenvío, especifique como mínimo 443 o all con la opción OutgoingPorts para habilitar los túneles SSL normales.

- OutgoingIPs (para limitar el acceso para túneles SSL según la dirección IP del servidor remoto). El formato es,

```
Enable CONNECT OutgoingIPs [(!)IP_pattern,...]
```

Por ejemplo, para permitir que los clientes se conecten a cualquier puerto de los servidores remotos que coincida con la dirección IP/nombre de sistema principal \*.ibm.com y que no coincida con 192.168.\*.\* , establezca las directivas siguientes:

```
Enable CONNECT OutgoingPorts all OutgoingIPs *.ibm.com,!192.168.*.*
SSLTunneling on
```

**Nota:** Los valores IP\_patterns se separan con una coma sin dejar ningún espacio en la lista.

- IncomingIPs (para limitar el acceso para túneles SSL según la dirección IP del cliente). El formato es,

Enable CONNECT IncomingIPs [[!]IP\_Pattern,...]

Por ejemplo, para permitir que los clientes procedentes de la dirección IP 192.168.\*.\* establezcan una conexión con cualquier puerto de los servidores remotos para túneles SSL, establezca las directivas siguientes:

Enable CONNECT OutgoingPorts all IncomingIPs 192.168.\*.\*  
SSLTunneling on

**Notas:**

1. Suponiendo que 192.168.\*.\* sea la máscara IP de LAN interna, la opción antedicha sólo permite que los usuarios internos utilicen el método de conexión y la función de túneles SSL.
2. Los valores IP\_patterns se separan con una coma sin dejar ningún espacio en la lista.

Para obtener más información para habilitar los túneles SSL y las directivas CONNECT editando el archivo de configuración de proxy, consulte los apartados de referencia del Apéndice B, “Directivas del archivo de configuración”, en la página 177 correspondientes a las siguientes directivas:

- “Enable: habilitar los métodos HTTP” en la página 214
- “SSLTunneling: habilitar los túneles SSL” en la página 287

---

## Configuración de la administración remota segura

La administración remota de Caching Proxy puede llevarse a cabo mediante las características de seguridad proporcionadas por SSL (Secure Sockets Layer) y la autenticación de contraseña. Con ello, se reduce significativamente la probabilidad de acceso al servidor proxy por las personas no autorizadas.

Para aplicar SSL durante la administración remota del servidor, utilice una petición `https://` en lugar de una petición `http://` para abrir los formularios de Configuración y Administración. Por ejemplo:

`https://su.nombre.servidor/suPáginaPresentación.html`

---

## Gestión de claves y certificados

Como se ha indicado anteriormente, antes de configurar SSL, debe configurar una base de datos de claves y obtener o crear un certificado. Los certificados se utilizan para autenticar las identidades de servidor. Utilice el programa de utilidad IBM Key Management, en ocasiones denominado iKeyman, para configurar los archivos de certificación. Este programa de utilidad forma parte del software GSKit, que se incluye con Application Server. GSKit además incluye una interfaz gráfica basada en Java para abrir los archivos de certificados.

A continuación aparecen los pasos básicos para configurar los certificados y las claves SSL.

1. Asegúrese de que se ha instalado GSKit. En la mayoría de plataformas, se instala automáticamente con el componente Caching Proxy. El nombre del paquete es `gsk7ikm` (`gsk7ikm_gcc295` en los sistemas Linux para i386). GSKit se

instala generalmente en el directorio `ibm/gsk7/` (`ibm/gskit/` en los sistemas AIX). En las plataformas Windows, también se puede acceder a él desde el menú **Inicio**.

**Nota:** En Windows, si GSKit no se instala al utilizar InstallShield, asegúrese de que la vía de acceso al directorio de instalación de soportes no contiene ningún espacio en blanco.

2. Utilice el gestor de claves para crear una clave para las comunicaciones de red seguras y recibir un certificado de una autoridad certificadora. Es posible que decida crear un certificado autofirmado mientras espera recibir el certificado de la autoridad certificadora.
3. Cree una base de datos de claves y especifique una contraseña de base de datos de claves.

**Nota:** Los archivos de claves y keystore se desinstalan siempre que se desinstale Caching Proxy. Para evitar tener que solicitar un nuevo certificado a la autoridad certificadora, guarde copias de seguridad de estos dos archivos en otro directorio antes de desinstalar el software de proxy.

En todos los sistemas operativos excepto en Linux, si el certificado ha caducado, Caching Proxy no se iniciará de forma adecuada y aparecerá un mensaje de error indicando que la base de datos de claves ha caducado. En Linux, el proxy parece iniciarse, pero el proceso desaparece rápidamente y no se genera ningún mensaje de error.

Para prevenir este problema en los sistemas Red Hat Enterprise Linux 3.0, asegúrese de que los paquetes GCC estén en los niveles siguientes o superiores:

- `libstdc++-3.2.3-52`
- `libgcc-3.2.3-52`

---

## Autoridades certificadoras

La clave pública debe asociarse con un certificado firmado digitalmente procedente de una autoridad certificadora (CA) designada como CA raíz de confianza del servidor. Puede comprar un certificado firmado sometiendo una petición de certificado a un proveedor de autoridades certificadoras (CA). Caching Proxy da soporte a las siguientes CA externas:

- VeriSign
- Thawte

Por omisión, se designan como CA de confianza a las siguientes CA:

- 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 (de VeriSign)

- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA

---

## Utilización del programa de utilidad IBM Key Manager

Este apartado proporciona una referencia rápida para utilizar el programa de utilidad IBM Key Manager (iKeyman). Utilice el gestor de claves para crear el archivo de base de datos de claves SSL, el par de claves pública y privada y la petición de certificado. Después de recibir el certificado firmado por la CA, utilice el gestor de claves para colocar el certificado en la base de datos de claves donde ha creado la petición de certificado original.

Con el software GSKit se incluye más documentación detallada sobre IBM Key Manager y GSKit.

### Configure el sistema para que ejecute el gestor de claves

Antes de iniciar la GUI de IKeyman, realice las acciones siguientes:

1. Instale Java 2 Technology, versión 1.4.2, de 32 bits, de IBM o equivalente
2. Establezca JAVA\_HOME en la ubicación del directorio Java. Por ejemplo:
  - Windows: set JAVA\_HOME=C:\Archivos de programa\IBM\Java142
  - Linux y UNIX: export JAVA\_HOME=/usr/opt/IBMJava2-142
3. Elimine los archivos ibmjsse.jar, gskikm.jar (si está presente) y ibmjcaprovider.jar del directorio JAVA\_HOME/jre/lib/ext.

#### Notas:

- a. Para Solaris, sustituya el directorio JAVA\_HOME/lib/ext/ por el directorio JAVA\_HOME/jre/lib/ext.
  - b. No mueva ni suprima archivos jar en un JDK del que dependa otro producto (por ejemplo, WebSphere Application Server). Si lo hace, puede interrumpir o impedir el funcionamiento correcto del producto dependiente. Si no está seguro si el JDK está utilizándose, instale un JDK independiente para el programa de utilidad IBM Key Management.
4. Todos los archivos JAR siguientes están actualmente en *vía\_acceso\_instalación\_GSKit/classes/jre/lib/ext/*.
    - Copie los archivos JAR especificados en JAVA\_HOME/jre/lib/
      - ibmjcefw.jar
      - ibmpkcs11.jar
    - Copie los archivos JAR especificados en JAVA\_HOME/jre/lib/ext/
      - ibmjceprovider.jar
      - ibmpkcs.jar
    - Copie los archivos JAR especificados en JAVA\_HOME/jre/lib/security/
      - local\_policy.jar
      - US\_export\_policy.jar
  5. Registre los proveedores de servicios IBM JCE, IBM CMS y/o IBMJCEFIPS:
 

Actualice el archivo JAVA\_HOME/jre/lib/security/java.security para añadir los proveedores IBM CMS y IBM JCE después del proveedor Sun. Por ejemplo:



```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.spi.IBMCMSProvider
security.provider.3=com.ibm.crypto.provider.IBMJCE
```

Encontrará un ejemplo de archivo `java.security` en `vía_acceso_instalación_GSKit/classes/gsk_java.security`.

- Para habilitar la operación FIPS, actualice el archivo `JAVA_HOME/jre/lib/security/java.security` para que también añada `IBMJCEFIPS` después del proveedor `Sun`. Asegúrese de que el proveedor `IBMJCEFIPS` se ha registrado con una prioridad mayor que `IBMJCE`. Por ejemplo:

```
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. (Opcional) Si es un usuario JSSE y utiliza JSSE para acceder al hardware criptográfico, instale `ibmpkcs11.jar` en el directorio `JAVA_HOME/jre/lib` y siga las instrucciones que aparecen en `vía_acceso_instalación_GSKit/classes/native/native-support.zip` para configurar las bibliotecas compartidas de hardware criptográfico.

**Nota:** Asimismo, puede encontrar `ibmpkcs11.jar` en el paquete JSSE salió al mercado publicado el 5 de agosto de 2002. Para registrar un proveedor de servicios `IBMPKCS11`, se ofrece a continuación un ejemplo que actualiza el archivo `JAVA_HOME/jre/lib/security/java.security`:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.crypto.pkcs11.provider.IBMPKCS11
```

## Inicio del gestor de claves

Inicie la interfaz gráfica de usuario del gestor de claves del siguiente modo:

- En las plataformas Linux y UNIX, especifique `gsk7ikm` en un indicador de mandatos.
- En las plataformas Windows, pulse **Inicio → Programas → IBM WebSphere → Edge Components → Caching Proxy → Iniciar el Programa de utilidad de gestión de claves**

Tenga en cuenta que si crea un nuevo archivo de base de datos de claves durante esta sesión, éste se almacena en el directorio a partir del cual se inició el gestor de claves.

## Creación de una nueva base de datos de claves, una contraseña y un archivo stash

Una base de datos de claves es un archivo que el servidor utiliza para almacenar un o más pares de claves y certificados. Se puede utilizar una base de datos de claves para todos los pares de claves y certificados o crear varias bases de datos. El programa de utilidad de gestión de claves se utiliza para crear nuevas bases de datos de claves y especificar sus contraseñas y archivos stash.

Para crear una base de datos de claves y un archivo stash:

1. Inicie el programa de utilidad de gestión de claves.
2. En el menú principal, seleccione **Key Database File → New** (Archivo de base de datos de claves > Nuevo).



3. En el nuevo **New** (Nuevo), asegúrese de que está seleccionado el tipo de archivo **CMS Key Database** (Base de datos de claves CMS). Escriba el nombre de base de datos de claves y la ubicación del archivo o acepte el valor por omisión **key.kdb**. Pulse **OK** (Aceptar).
4. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba y confirme la contraseña de esta base de datos. Pulse **OK** (Aceptar).
5. Seleccione el recuadro de selección para ocultar el archivo de contraseñas. Cuando se le solicite, escriba y confirme una contraseña para su verificación. Aparecerá el siguiente mensaje: DB-Type: CMS key database file  
*nombre\_basedatos\_archivo\_claves*

**Nota:** Si no oculta el archivo de contraseñas, se inicia el servidor pero no escucha en el puerto 443.

La contraseña que especifique cuando cree una base de datos de claves nueva protege la clave privada. La clave privada es la única clave que puede firmar documentos o descifrar mensajes cifrados con la clase pública.

Utilice las siguientes directrices al especificar la contraseña:

- La contraseña debe estar formada por el juego de caracteres de inglés americano.
- La contraseña debe tener seis caracteres como mínimo y contener al menos dos números no consecutivos. Asegúrese de que la contraseña no contenga información personal que se pueda obtener públicamente como, por ejemplo, su nombre, iniciales o fecha de nacimiento o los de sus familiares mas cercanos.
- Oculte la contraseña.

Es aconsejable modificar la contraseña de base de datos de claves con frecuencia. No obstante, si especifica una fecha de caducidad para la contraseña, registre cuándo debe modificarse. Si la contraseña caduca antes de modificarla, se escribe un mensaje en las anotaciones cronológicas de error y se inicia el servidor, pero no puede realizar conexiones de red seguras.

Siga estos pasos para modificar la contraseña de base de datos de claves:

1. En el menú principal, pulse **Key Database File -> Open** (Archivo de base de datos de claves > Abrir).
2. En el recuadro de diálogo **Open** (Abrir), escriba el nombre de la base de datos de claves o acepte el valor por omisión, **key.kdb**. Pulse **OK** (Aceptar).
3. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba la contraseña establecida y pulse **OK** (Aceptar).
4. En el menú principal, pulse **Key Database File -> Change Password** (Archivo de base de datos de claves > Modificar contraseña).
5. En el recuadro de diálogo **Change Password** (Modificar contraseña), escriba y confirme una contraseña nueva. Pulse **OK** (Aceptar).

Para realizar una conexión SSL entre un proxy y un servidor LDAP, introduzca la contraseña de base de datos de claves en el archivo **pac\_keyring.pwd**. Tenga en cuenta que el archivo **pac\_keyring.pwd** no es el archivo **stash** generado por IKeyMan.

### Creación de un nuevo par de claves y una petición de certificados

La base de datos de claves almacena pares de claves y peticiones de certificado. Para crear un par de claves pública y privada y una petición de certificado, siga los pasos siguientes:

1. Si no ha creado la base de datos de claves, siga las instrucciones que aparecen en “Creación de una nueva base de datos de claves, una contraseña y un archivo stash” en la página 126.
2. En el programa de utilidad de gestión de claves, pulse **Key Database → File → Open** (Base de datos de claves > Archivo > Abrir) en el menú principal.
3. En el recuadro de diálogo **Abrir** (Abrir), escriba el nombre de la base de datos de claves o pulse **key.kdb** si está utilizando el valor por omisión. Pulse **OK** (Aceptar).
4. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba la contraseña y pulse **OK** (Aceptar).
5. En el menú principal, pulse **Create → New Certificate Request** (Crear > Nueva petición de certificado).
6. En el recuadro de diálogo **New Key and Certificate Request** (Nueva clave y petición de certificado), especifique la siguiente información:
  - **Key Label (Etiqueta de clave):** escriba un nombre (etiqueta) que se utilice para identificar la clave y el certificado de la base de datos, por ejemplo, *my self-signed certificate* o *www.companyA.com*.
  - **Keysize (Tamaño de clave):** tamaño de la clave, por ejemplo, 1024. Para beneficiarse de un cifrado de 128 bits, se recomienda un tamaño de 1024.
  - **Organization Name (Nombre de la organización):** nombre de la organización que se va a asociar con la clave, por ejemplo, *Company A*.
  - **Organization Unit (Unidad organizativa)** (opcional)
  - **Locality (Localidad)** (opcional)
  - **State/Province (Estado/Provincia)** (opcional)
  - **Zipcode (Código postal)** (opcional)
  - **Country (País):** código del país. Debe especificar dos caracteres como mínimo, por ejemplo, *US*.
  - **Certificate request file name (Nombre de archivo de petición de certificado):** nombre del archivo de petición. Opcionalmente, se puede utilizar un nombre por omisión.
7. Pulse **OK** (Aceptar). Se visualizará un mensaje de confirmación:  
Se ha creado una nueva petición de certificado satisfactoriamente en el archivo *nombre\_basedatos\_archivo\_claves*.
8. Pulse **OK** (Aceptar). Se visualizará el nombre de etiqueta que ha especificado bajo la cabecera **Personal Certificate Requests** (Peticiones de certificados personales).
9. En el recuadro de diálogo **Information** (Información), pulse **OK** (Aceptar). Se le recuerda que envíe el archivo a una autoridad certificadora.
10. A menos que haya creado un certificado autofirmado (consulte el apartado siguiente, “Creación de un certificado autofirmado”, para obtener detalles), envíe la petición de certificado a una CA:
  - Deje el gestor de despliegue en ejecución.
  - Inicie un navegador Web y especifique el URL de la CA de la que desea obtener el certificado.
  - Siga las instrucciones facilitadas por la CA para enviar la petición de certificado.

Las peticiones de certificado pueden tardar de dos a tres semanas en satisfacerse. Mientras que espera que la CA procese la petición de certificado, puede actuar como su propia CA y utilizar iKeyman para crear un certificado de servidor autofirmado para habilitar las sesiones SSL entre los clientes y el servidor de Caching Proxy.

### Creación de un certificado autofirmado

Utilice el programa de utilidad de gestión de claves para crear un certificado de servidor autofirmado para habilitar las sesiones SSL entre los clientes y el servidor proxy mientras se espera que se envíe un certificado. Asimismo, puede utilizar certificados autofirmados sólo para pruebas.

Siga este procedimiento para crear un certificado autofirmado:

1. Si no ha creado la base de datos de claves, siga las instrucciones que aparecen en “Creación de una nueva base de datos de claves, una contraseña y un archivo stash” en la página 126.
2. En el programa de utilidad de gestión de claves, pulse **Key Database -> File -> Open** (Base de datos de claves > Archivo > Abrir) en el menú principal.
3. En el recuadro de diálogo **Open** (Abrir), escriba el nombre de la base de datos de claves o acepte el valor por omisión, **key.kdb**. Pulse **OK** (Aceptar).
4. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba la contraseña y pulse **OK** (Aceptar).
5. En el marco de contenido **Key Database** (Base de datos de claves), seleccione **Personal Certificates** (Certificados personales) y pulse **Create New Self-Signed Certificate** (Crear certificado autofirmado nuevo).
6. En la ventana **Create New Self-Signed Certificate** (Crear certificado autofirmado nuevo), especifique la siguiente información:
  - **Key Label (Etiqueta de clave):** nombre (etiqueta) que se utilice para identificar la clave y el certificado de la base de datos, por ejemplo, *my self-signed certificate*.
  - **Key Size (Tamaño de clave):** tamaño de la clave, por ejemplo, 512.
  - **Common Name (Nombre común):** nombre completo del sistema principal de servidor, por ejemplo, *www.myserver.com*
  - **Organization Name (Nombre de la organización):** nombre de la organización que se va a asociar con la clave, por ejemplo, *Company A*
  - **Organization Unit (Unidad organizativa)** (opcional)
  - **Locality (Localidad)** (opcional)
  - **State/Province (Estado/Provincia)** (opcional)
  - **Zipcode (Código postal)** (opcional)
  - **Country (País):** código del país. Debe especificar dos caracteres como mínimo, por ejemplo, *US*.
  - **Período de validez:** período de tiempo que el certificado es válido.
7. Pulse **OK** (Aceptar).
8. Registre la base de datos de claves con el servidor añadiendo el archivo de claves y el archivo a los valores de configuración (consulte “Creación de una nueva base de datos de claves, una contraseña y un archivo stash” en la página 126).

### Claves de exportación

Utilice este procedimiento para exportar claves a otra base de datos de claves:

1. Inicie el programa de utilidad de gestión de claves.
2. En el menú principal, pulse **Key Database File -> Open** (Archivo de base de datos de claves > Abrir).
3. En el recuadro de diálogo **Open** (Abrir), escriba el nombre de la base de datos de claves o acepte el valor por omisión, **key.kdb**. Pulse **OK** (Aceptar).
4. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba la contraseña y pulse **OK** (Aceptar).
5. En el marco de contenido **Key Database** (Base de datos de claves), seleccione **Personal Certificates** (Certificados personales) y, a continuación, pulse el botón **Export/Import** (Exportar/Importar) en la etiqueta.
6. En la ventana **Export/Import Key** (Exportar/Importar clave):
  - Seleccione **Export Key** (Exportar clave).
  - Seleccione el tipo de base de datos de destino (por ejemplo, **PKCS12** ).
  - Escriba el nombre de archivo o pulse **Browse** (Explorar) para seleccionarlo.
  - Escriba la ubicación correcta.
7. Pulse **OK** (Aceptar).
8. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba la contraseña correcta, escriba la contraseña de nuevo para confirmarla y, a continuación, pulse **OK** (Aceptar) para exportar la clave seleccionada a otra base de datos de claves.

#### Importing keys (Claves de importación)

Para importar claves de otra base de datos de claves:

1. Inicie el programa de utilidad de gestión de claves.
2. En el menú principal, seleccione **Key Database File -> Open** (Archivo de base de datos de claves > Abrir).
3. En el recuadro de diálogo **Open** (Abrir), escriba el nombre de la base de datos de claves o acepte el valor por omisión, **key.kdb**. Pulse **OK** (Aceptar).
4. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba la contraseña correcta y pulse **OK** (Aceptar).
5. En el marco de contenido **Key Database** (Base de datos de claves), seleccione **Personal Certificates** (Certificados personales) y, a continuación, pulse el botón **Export/Import** (Exportar/Importar) en la etiqueta.
6. En la ventana **Export/Import Key** (Exportar/Importar clave):
  - Seleccione **Import Key** (Importar clave).
  - Seleccione el tipo de archivo de base de datos de claves (por ejemplo, **PKCS12**).
  - Escriba el nombre de archivo o pulse **Browse** (Explorar) para seleccionarlo.
  - Seleccione la ubicación correcta.
7. Pulse **OK** (Aceptar).
8. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba la contraseña correcta y pulse **OK** (Aceptar).
9. En la lista **Select from Key Label** (Seleccionar de etiqueta de clave), seleccione el nombre de etiqueta correcto y pulse **OK** (Aceptar).

#### Listado de autoridades certificadoras

Para visualizar una lista de las autoridades certificadoras (CA) de confianza en la base de datos de claves:

1. Inicie el programa de utilidad de gestión de claves.
2. En el menú principal, pulse **Key Database File** → **Open** (Archivo de base de datos de claves > Abrir).
3. En el recuadro de diálogo **Open** (Abrir), escriba el nombre de la base de datos de claves o acepte el valor por omisión, **key.kdb**. Pulse **OK** (Aceptar).
4. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba la contraseña correcta y pulse **OK** (Aceptar).
5. En el marco de contenido **Key Database** (Base de datos de claves), seleccione **Signer Certificates** (Certificados de firmante).
6. Pulse **Signer Certificates** (Certificados de firmante), **Personal Certificates** (Certificados personales) o **Certificate Requests** (Peticiones de certificados) para ver la lista de las CA en la ventana **Key Information** (Información de claves).

## Recepción de un certificado de CA

Utilice este procedimiento para recibir un certificado que se le envíe electrónicamente desde una autoridad certificadora (CA) que esté designada como una CA de confianza por omisión (consulte la lista en “Autoridades certificadoras” en la página 124). Si la CA que emite el certificado firmado por CA o no es una CA de confianza en la base de datos de claves, primero debe almacenar el certificado de la CA y designar la CA como una CA de confianza. Seguidamente ya puede recibir el certificado firmado por CA en la base de datos. No puede recibir un certificado firmado por CA de una CA que no sea de confianza (consulte “Almacenamiento de un certificado de CA”).

Para recibir un certificado firmado por CA en una base de datos de claves:

1. Inicie el programa de utilidad de gestión de claves.
2. En el menú principal, seleccione **Key Database File** → **Open** (Archivo de base de datos de claves > Abrir).
3. En el recuadro de diálogo **Open** (Abrir), escriba el nombre de la base de datos de claves o acepte el valor por omisión, **key.kdb**. Pulse **OK** (Aceptar).
4. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba la contraseña y pulse **OK** (Aceptar).
5. Asegúrese de que el nombre de archivo del listado **DB-Type** (Tipo-BD) es correcto.
6. En la ventana **Key Database** ((Base de datos de claves), seleccione **Personal Certificates** (Certificados personales) y, a continuación, pulse **Receive** (Recibir).
7. En el recuadro de diálogo **Receive Certificate from a File** (Recibir certificado de un archivo), escriba el nombre de un archivo codificado en Base 64 válido en el campo de texto **Certificate filename** (Nombre de archivo de certificados). Pulse **OK** (Aceptar).
8. Para cerrar el programa de utilidad del gestor de claves, pulse **Key Database File** → **Exit** (Archivo de base de datos de claves > Salir) en el menú principal.

## Almacenamiento de un certificado de CA

Sólo los certificados firmados por las CA de confianza se aceptan para establecer conexiones seguras. Para añadir una CA a la lista de autoridades de confianza, debe obtener y almacenar el certificado como de confianza. Siga este procedimiento para almacenar un certificado de una CA nueva, antes de recibirlo en la base de datos:

1. Inicie el programa de utilidad de gestión de claves.
2. En el menú principal, pulse **Key Database File -> Open** (Archivo de base de datos de claves > Abrir).
3. En el recuadro de diálogo **Open** (Abrir), escriba el nombre de la base de datos de claves o acepte el valor por omisión, **key.kdb**. Pulse **OK** (Aceptar).
4. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba la contraseña y pulse **OK** (Aceptar).
5. En el marco de contenido **Key Database** (Key Database), seleccione (Certificados de firmante) y, a continuación, pulse **Add** (Añadir).
6. En el recuadro de diálogo **Add CA's Certificate from a File** (Añadir certificado de CA de un archivo), seleccione el nombre de archivo de certificado de datos codificados en Base 64 o utilice la opción **Examinar** (Examinar). Pulse **OK** (Aceptar).
7. En el recuadro de diálogo **Label** (Etiqueta), escriba el nombre de etiqueta y pulse **OK** (Aceptar).
8. Utilice el recuadro de selección para designar el certificado como de confianza (por omisión).

**Nota:** Visualice el recuadro de selección *después* de crear el certificado mediante el botón "View/Edit" (Ver/Editar). El recuadro de selección aparecerá en el panel pero no se visualizará durante la adición del certificado.

### Visualización de la clave por omisión en una base de datos de claves

Visualice la entrada de clave por omisión del siguiente modo:

1. Inicie el programa de utilidad de gestión de claves.
2. En el menú principal, pulse **Key Database File -> Open** (Archivo de base de datos de claves > Abrir).
3. En el recuadro de diálogo **Open** (Abrir), escriba el nombre de la base de datos de claves o acepte el valor por omisión, **key.kdb**. Pulse **OK** (Aceptar).
4. En el recuadro de diálogo **Password Prompt** (Solicitud de contraseña), escriba la contraseña y pulse **OK** (Aceptar).
5. En el marco de contenido **Key Database** (Base de datos claves), seleccione **Personal Certificates** (Certificados personales) y seleccione el nombre de etiqueta del certificado de CA.
6. En la ventana **Key Information** (Información de claves), pulse **View/Edit** (Ver/Editar) para visualizar la información de claves por omisión del certificado.

## Especificaciones de cifrado soportadas

Los algoritmos de cifrado y hashes utilizados para SSL versiones 2 y 3 aparecen enumerados en las tablas siguientes.

Generación de pares de claves: tamaños de clave pública de RSA 512–1024

### SSL Versión 2

Versión para EE.UU.	Versión para exportar
RC4 US	RC4 Export
RC2 US	RC2 Export



DES 56-bit	<i>no aplicable</i>
Triple DES US	<i>no aplicable</i>
RC4 Export	<i>no aplicable</i>
RC2 Export	<i>no aplicable</i>

### SSL Versión 3

Versión para EE.UU.	Versión para exportar
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>no aplicable</i>
DES CBC SHA	<i>no aplicable</i>
NULL SHA	<i>no aplicable</i>
NULL MD5	<i>no aplicable</i>
NULL NULL	<i>no aplicable</i>

Estas especificaciones SSL también pueden configurarse editando directamente el archivo de configuración de proxy. Para obtener detalles, consulte los apartados de referencia del Apéndice B, “Directivas del archivo de configuración”, en la página 177 para obtener información sobre las siguientes directivas:

- “V2CipherSpecs: enumerar las especificaciones de cifrado soportadas para SSL Versión 2” en la página 293
- “V3CipherSpecs: enumerar las especificaciones de cifrado soportadas para SSL Versión 3” en la página 293
- “FIPSEnable: cifrados aprobados por FIPS (Enable Federal Information Processing Standard) para SSLV3 y TLS” en la página 222

### Cifrado de 128 bits para Caching Proxy

Sólo está disponible una versión de cifrado de 128 bits de Caching Proxy. Ya no se puede acceder a la versión de 56 bits. Si está actualizando una versión anterior, puede instalar Caching Proxy directamente en la versión de 128 o 56 bits instalada actualmente. Si previamente utilizaba un navegador de 56 bits (de exportación), debe actualizarlo a un navegador de 128 bits para aprovechar el cifrado de 128 bits del proxy.

Después de actualizar Caching Proxy de la versión de 56 bits a la versión de 128 bits, si el tamaño de clave utilizado para cifrar los certificados se establece en 1024, no es necesario modificar la configuración. No obstante, si el tamaño de clave se establece en 512, para aprovechar el cifrado de 128 bits del proxy, debe crear nuevos certificados con un tamaño de clave de 1024. Cree claves nuevas mediante el programa de utilidad IBM Key Manager (iKeyman).

1. Inicie el gestor de claves.

- En las plataformas Linux y UNIX, especifique gsk7ikm en un indicador de mandatos.
  - En los sistemas Windows, pulse **Inicio -> Programas -> IBM WebSphere -> Edge Components -> Iniciar el Programa de utilidad de gestión de claves.**
2. En el menú principal, pulse **Key Database File -> Open** (Archivo de base de datos de claves > Abrir).
  3. En el recuadro de diálogo **Open** (Abrir), escriba el nombre de la base de datos de claves o pulse **key.kdb** si está utilizando el valor por omisión, y pulse **OK** (Aceptar).
  4. Si el recuadro de diálogo **Password Prompt** se abre, escriba la contraseña y pulse **OK** (Aceptar).
  5. En el menú principal, pulse **Create -> New Certificate Request** (Crear > Nueva petición de certificado).
  6. En la ventana **New Key and Certificate Request** (Nueva clave y petición de certificado), especifique la siguiente información:
    - **Key Label** (Etiqueta de clave): escriba un nombre que se utilice para identificar la clave y el certificado de la base de datos.
    - **Keysize** (Tamaño de clave): seleccione **1024**.
    - **Organization Name** (Nombre de la organización): escriba el nombre de la organización que se vaya a asociar con la clave.
    - **Country** (País): escriba el código del país. Debe especificar dos caracteres como mínimo, por ejemplo, US.
    - **Certificate request file name** (Nombre de archivo de petición de certificado): escriba un nombre para el archivo de petición, u opcionalmente, utilice un nombre por omisión.
  7. Pulse **OK** (Aceptar).

Consulte “Gestión de claves y certificados” en la página 123 para obtener información detallada del programa de utilidad IBM Key Manager.

Tenga en cuenta que esta versión del producto no da soporte al cifrado en SUSE Linux.



---

## Capítulo 27. Habilitación del soporte de hardware criptográfico

Sólo se aplica a configuraciones de proxy de retorno.

Siga este procedimiento para permitir que la rutina de protocolo de enlace SSL se descargue en una tarjeta de hardware criptográfico:

1. Instale la tarjeta de hardware criptográfico de acuerdo con las instrucciones del fabricante.
2. Habilite SSL para Caching Proxy. Para obtener más información, consulte Capítulo 26, "SSL (Secure Sockets Layer)", en la página 119.
3. Edite manualmente la directiva SSLCryptoCard del archivo de configuración ibmproxy.conf. No aparece ninguna entrada de esta directiva en los formularios de Configuración y Administración. Para obtener más información, consulte la referencia de la directiva SSLCryptoCard, "SSLCryptoCard: especificar la tarjeta criptográfica instalada" en la página 286.

En AIX, para dar soporte a la tarjeta IBM 4960 PCI Cryptographic Accelerator Card, consulte "PKCS11DefaultCert, PKCS11DriverPath, PKCS11TokenPassword — Da soporte a la tarjeta IBM 4960 PCI Cryptographic Accelerator Card (sólo AIX)" en la página 255.



---

## Capítulo 28. Utilización del plug-in de Tivoli Access Manager

Se proporciona un plug-in de Caching Proxy con Tivoli Access Manager (anteriormente Tivoli Policy Director) que permite que Caching Proxy utilice Access Manager para las funciones de autenticación y autorización. Este plug-in permite que una empresa que utilice Access Manager para el control de accesos a Internet con el fin de añadir la tecnología Edge sin tener que duplicar el trabajo mediante el establecimiento de esquemas de autorización separados para el servidor proxy.

Para obtener información adicional sobre Tivoli Access Manager, visualice el sitio Web del producto en <http://www.ibm.com/software/tivoli/products/>. Para obtener información sobre los requisitos de software y hardware y sobre la instalación del plug-in de Access Manager, consulte la documentación facilitada con Tivoli Access Manager.

**Nota:** Es posible que el plug-in de Tivoli Access Manager no reciba soporte en Red Hat Linux. Póngase en contacto con Tivoli para obtener información de soporte actualizada sobre las plataformas Linux.

---

### Configuración

Se facilita un script de configuración para Caching Proxy con el plug-in de Access Manager.

#### Pasos previos a la utilización del script de configuración

Antes de ejecutar el script, realice las siguientes acciones:

- Instale todo el software necesario.
- Asegúrese de que el servidor proxy está establecido para que utilice el puerto 80 (este es el valor por omisión).
- Configure los componentes LDAP y de Access Manager y asegúrese de que están en ejecución mientras configura el plug-in de Access Manager.
- Asegúrese de que puede acceder al ID de administrador de Access Manager y al nombre de administrador LDAP. Estos valores son necesarios para establecer el servidor proxy.

#### Utilización del script de configuración

El script de configuración se denomina **wslconfig.sh** y se facilita en el directorio `/opt/pdweb-lite/bin/`. Especifique el ID de administrador de Access Manager y el nombre de administrador LDAP cuando se le soliciten.

El script de configuración automáticamente realiza los pasos siguientes:

- Establece el ID de usuario de Caching Proxy en `root` y el ID de grupo en `other`
- Establece la directiva `noLog` en `*`, que provoca que ningún elemento se escriba en las anotaciones cronológicas de Caching Proxy
- Crea una directiva `ServerInit` con la siguiente información:  

```
ServerInit /opt/pdweb-lite/lib/wesauth.so:WTESeal_Init  
/opt/pdweb-lite/etc/ibmwesas.conf
```
- Crea una directiva `PreExit` con la siguiente información:  

```
PreExit /opt/pdweb-lite/lib/wesauth.so:WTESeal_PreExit
```

- Crea una directiva Authorization con la siguiente información:  
Authorization \* /opt/pdweb-lite/lib/wesauth.so:WTESeal\_Authorize
  - Crea una directiva ServerTerm con la siguiente información:  
ServerTerm /opt/pdweb-lite/lib/wesauth.so:WTESeal\_Term
- Crea una sentencia Protect y una configuración de protección que reenvía todas las peticiones al proceso de autenticación de Access Manager del siguiente modo:
- ```
Protection PROXY-PROT {  
    ServerId WebSEAL-Lite  
    Mask All@(*)  
    AuthType Basic  
}  
Protect * PROXY-PROT
```

---

## Inicio de Caching Proxy y del plug-in de Access Manager

Después de configurar el servidor proxy y el plug-in de Access Manager, utilice el mandato **wsstartwte** en lugar de **ibmproxy start** para iniciar el servidor proxy. El mandato **wsstartwte** carga automáticamente las variables de entorno que el plug-in de Access Manager necesita para inicializarse. Si no utiliza **wsstartwte** al iniciar el servidor proxy, aparecerán mensajes de error sobre el plug-in de Access Manager. El mandato stop correspondiente, **ibmproxy stop**, aún es válido cuando se utiliza el plug-in.

---

## Capítulo 29. Utilización del módulo de autorización PAC-LDAP

---

### Visión general

El módulo de autorización PAC-LDAP permite que Caching Proxy acceda al servidor LDAP (Lightweight Directory Access Protocol) al realizar rutinas de autorización o autenticación. El módulo consta de dos conjuntos de componentes: un par de bibliotecas compartidas que añaden las funciones LDAP a la API de Caching Proxy y un daemon PAC (Policy Authentication Control). Una directiva `ServerInit` del archivo `ibmproxy.conf` indica a la biblioteca compartida que inicialice uno o más daemons PAC cuando se inicie Caching Proxy. Las bibliotecas compartidas leen un archivo `paccp.conf` para determinar el número y características de los daemons PAC. Durante la inicialización, el daemon lee el archivo `pac.conf` para las directivas de configuración y el archivo `pacpolicy.conf` para la información de políticas. A continuación, una directiva `Authentication` del archivo `ibmproxy.conf` indica al servidor proxy que llame a la biblioteca compartida siempre que la autenticación sea necesaria, o bien una directiva `Authorization` usurpa el flujo de trabajo de Caching Proxy durante el proceso de peticiones HTTP.

### Autenticación

El proceso de autenticación determina si un conjunto proporcionado de credenciales – nombre de usuario y contraseña – es válido. Este proceso incluye la verificación de que un usuario esté en el registro y que la contraseña facilitada coincida con la contraseña almacenada en ese registro. A continuación, se indican las acciones realizadas mediante el módulo PAC-LDAP durante el paso de autenticación.

Cuando se habilita el módulo de autorización PAC-LDAP para las funciones de autenticación, se convierte en el depósito por omisión del que se obtienen los ID de usuario, las contraseñas y los grupos. Cuando una petición HTTP pasa a través del flujo de trabajo de Caching Proxy, todas las directivas `Protect` comparan el URL solicitado con la correspondiente plantilla de petición. Si se produce una coincidencia, la directiva `Protect` invoca un esquema de protección, que incluye el ID de servidor, el tipo de autenticación que se va a utilizar, las normas de enmascaramiento que se deben aplicar al cliente solicitante y las ubicación de los archivos de grupos y contraseñas. Si no se define el archivo de contraseñas, el ID de usuario y contraseña se recuperan a través del módulo de autorización PAC-LDAP. Las políticas del tipo 0, 1, 2 y 3 definen los esquemas de autenticación. Si se pasa la autenticación, se sirve la autenticación; de lo contrario, Caching Proxy devuelve un error 401 al cliente.

### Autorización

El proceso de autorización determina si un usuario tiene el permiso necesario para acceder al recurso protegido. Cuando se utiliza el módulo PAC-LDAP, es necesaria la aplicación de las normas de autorización que residan en el archivo `pacpolicy.conf` para la petición HTTP.

Cuando se habilita el módulo de autorización PAC-LDAP para las funciones de autorización, las normas de autorización del archivo `pacpolicy.conf` se aplican a la petición HTTP. Cuando una petición HTTP pasa a través del flujo de trabajo de Caching Proxy, todas las directivas `Protect` comparan el URL solicitado con la

correspondiente plantilla de petición. Si se produce una coincidencia, la directiva Protect invoca un esquema de protección. En este caso, el esquema de protección es la rutina de autorización tomada por el módulo de autorización PAC-LDAP. La directiva Authorization compara el URL solicitado con la correspondiente plantilla de petición y, si se produce una coincidencia, se invoca al módulo de autorización PAC-LDAP. Las políticas de tipo 4 definidas en el archivo pacpolicy.conf que ajustan de forma adicional la autenticación necesaria para varias peticiones URL.

## Lightweight Directory Access Protocol (LDAP)

LDAP proporciona acceso interactivo a los directorios X.500 con un consumo mínimo de los recursos del sistema. IANA ha asignado el puerto TCP 389 y el puerto UDP 389 a LDAP. Para obtener más información, consulte RFC 1777, que define LDAP.

Son ejemplos de clientes LDAP soportados: el cliente LDAP de IBM Tivoli y el cliente LDAP de IBM SecureWay.

---

## Instalación

Todos los componentes del módulo de autorización PAC-LDAP se instalan automáticamente cuando se instala el sistema Caching Proxy de WebSphere Application Server, Versión 6.1. En los sistemas Linux y UNIX, se crean en el directorio /opt/ibm/edge/cp/ un directorio de biblioteca de Caching Proxy (./lib/), un directorio de biblioteca del módulo de autorización PAC-LDAP (./lib/plugins/pac/), un directorio de binarios (./bin/) y un directorio de configuración (./etc/). A continuación, se crean enlaces simbólicos desde los directorios /usr/lib/, /usr/sbin/ y /etc con estos directorios específicos de productos.

Estructura de directorio

| Directorio Linux y UNIX           | Directorio Windows                                 | Contenido                                                                       |
|-----------------------------------|----------------------------------------------------|---------------------------------------------------------------------------------|
| /opt/ibm/edge/cp/                 | \Archivos de programa\IBM\edge\cp\                 | Directorio base de Caching Proxy ( <i>raíz_cp</i> )                             |
| <i>raíz_cp</i> /sbin/             | \Archivos de programa\IBM\edge\cp\Bin\             | Binarios y scripts de Caching Proxy                                             |
| /usr/sbin/                        |                                                    | Enlaces simbólicos con <i>raíz_cp</i> /sbin/                                    |
| <i>raíz_cp</i> /etc/              | \Archivos de programa\IBM\edge\cp\etc\             | Archivo de configuración de Caching Proxy                                       |
| /etc/                             |                                                    | Enlaces simbólicos con <i>raíz_cp</i> /etc/                                     |
| <i>raíz_cp</i> /lib/              | \Archivos de programa\IBM\edge\cp\lib\ plugins\    | Bibliotecas de Caching Proxy                                                    |
| <i>raíz_cp</i> /lib/ plugins/pac/ | \Archivos de programa\IBM\edge\cp\lib\plugins\pac\ | Bibliotecas de módulo de autorización PAC-LDAP                                  |
| /usr/lib/                         |                                                    | Enlaces simbólicos con <i>raíz_cp</i> /lib/ y <i>raíz_cp</i> /lib/ plugins/pac/ |

| Directorio Linux y UNIX                | Directorio Windows                                       | Contenido                                                  |
|----------------------------------------|----------------------------------------------------------|------------------------------------------------------------|
| <i>raíz_cp</i> /server_root/pac/data/  | \Archivos de programa\IBM\edge\cp\server_root\pac\data\  | Almacenamiento de datos de módulo de autorización PAC-LDAP |
| <i>raíz_cp</i> /server_root/pac/creds/ | \Archivos de programa\IBM\edge\cp\server_root\pac\creds\ | Credenciales del módulo de autorización PAC-LDAP           |

#### Archivos del plug-in LDAP

| Nombre de archivo Linux y UNIX       | Nombre de archivo Windows            | Descripción                              |
|--------------------------------------|--------------------------------------|------------------------------------------|
| libpacwte.so                         | pacwte.dll                           | Biblioteca compartida                    |
| libpacman.so                         | pacman.dll                           | Biblioteca compartida                    |
| pacd_restart.sh                      | pacd_restart.bat                     | Script de reinicio de daemons PAC        |
| paccp.conf, pac.conf, pacpolicy.conf | paccp.conf, pac.conf, pacpolicy.conf | archivos de configuración y de políticas |

## Requisitos y restricciones adicionales para las conexiones seguras del servidor PACD-LDAP

### GSKit es necesario para el paquete de cliente LDAP

Para habilitar las conexiones SSL (Secure Sockets Layer) entre el daemon PACD y el servidor LDAP, debe instalar el paquete GSKit que el paquete de cliente LDAP necesita. GSKit 7 es necesario en la máquina de Caching Proxy, donde se facilita por omisión, pero es posible que no sea la versión que requiere el cliente LDAP en la máquina. Se pueden utilizar versiones distintas de GSKit en la misma máquina para procesos distintos.

Coloque el archivo de claves de GSKit en `$pacd_creds_dir/pac_keyring.kdb` y la contraseña en `$pacd_creds_dir/pac_keyring.pwd`.

**Nota:** Para obtener información sobre los requisitos de GSKit en el servidor LDAP, consulte la documentación de IBM Tivoli Directory Server (ITDS) en el sitio Web siguiente: <http://www.ibm.com/software/tivoli/products/directory-server/>

### La variable de entorno LD\_PRELOAD debe establecerse para los sistemas Linux

En los sistemas Linux, la variable de entorno LD\_PRELOAD debe configurarse del siguiente modo para habilitar las conexiones SSL entre el PACD y el servidor LDAP. Establezca la variable en el siguiente valor:

```
LD_PRELOAD=/usr/lib/libstdc++-libc6.1-1.so.2
```

El requisito de GSKit al que se hace referencia anteriormente también se aplica a los sistemas Linux.

## En los sistemas Linux, el proceso PACD no se inicia al utilizar el cliente LDAP de IBM Tivoli Directory Server (ITDS)

En los sistemas Red Hat Enterprise Linux 4.0, el proceso PACD no se inicia cuando se configura Caching Proxy para utilizar el plug-in LDAP de ITDS 6.0 para realizar la autenticación. Se produce el siguiente mensaje de error:

```
"error while loading shared libraries:
/usr/lib/libldapiconv.so: R_PPC_REL24 relocation at 0x0fb58ad0
for symbol 'strpbrk' out of range"
```

Existe actualmente la restricción de que ITDS 6.0 no da soporte a los sistemas RHEL 4.0.

## En sistemas AIX, el módulo PAC-LDAP no se puede cargar al utilizar el cliente LDAP de IBM Tivoli Directory Server (ITDS)

El proceso PACD no se inicia en los sistemas AIX debido a unos enlaces no resueltos al utilizar el cliente LDAP de ITDS. Cuando se inicia el proceso PACD, podría producirse el siguiente error:

```
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.
```

Para eludir este problema para ITDS versión 5 del cliente LDAP, cree el símbolo siguiente:

```
ln -s /usr/lib/libibmldap.a /usr/lib/libldap.a
```

Para eludir este problema para ITDS versión 6 del cliente LDAP, cree el símbolo siguiente:

```
ln -s /opt/IBM/ldap/V6.0/lib/libibmldap.a /usr/lib/libldap.a
```

---

## Edición del archivo `ibmproxy.conf` para habilitar el módulo de autorización PAC-LDAP

Las tres directivas `ServerInit`, `Authorization` o `Authentication`, y `ServerTerm` deben añadirse al apartado de directivas API del archivo `ibmproxy.conf` para inicializar el módulo de autorización PAC-LDAP. Para crear estas directivas, edite el archivo `ibmproxy.conf` manualmente o, si el servidor proxy ya está en ejecución, conéctese a los formularios de Configuración y Administración con un navegador de Internet y abra el formulario Petición de proceso de API (Pulse **Servidor de configuración** → **Proceso de peticiones** → **Petición de proceso de API**). Todas las directivas deben aparecer en una única línea en el archivo de configuración de proxy, independientemente de si los ejemplos proporcionados en este apartado contienen divisiones de línea para que sean legibles.

Tenga en cuenta que las directivas de prototipo (en forma de comentarios) se facilitan en el apartado API del archivo `ibmproxy.conf`. Estas directivas API aparecen en un orden determinado. Al añadir las directivas API para habilitar nuevas características y módulos de plug-in, ordene las directivas como se muestran en la parte de prototipo del archivo de configuración. Alternativamente, elimine los comentarios de las directivas API y édítelas, si es necesario, para incluir el soporte de todas las funciones o plug-ins deseados.

La directiva `ServerInit` tiene tres argumentos: (1) la vía de acceso plenamente cualificada de la biblioteca compartida, (2) la llamada de función y (3) la vía de



acceso plenamente cualificado del archivo `paccp.conf`. El primer y segundo argumentos se delimitan por dos puntos (:). El segundo y tercer argumentos se delimitan por un espacio. El primer y tercer argumentos son específicos del sistema y dependen de dónde se han instalado los componentes de plug-in. El segundo argumento se codifica en la biblioteca compartida y debe escribirse exactamente como se muestra. Al crear una directiva `ServerInit` mediante el formulario Petición de proceso de API, tanto el segundo como el tercer argumento deben especificarse en el campo **Nombre de función**. El tercer argumento se muestra en la columna **Plantilla de IP**.

La directiva `Authorization` tiene tres argumentos: (1) una plantilla de petición, (2) la vía de acceso plenamente cualificada de la biblioteca compartida y (3) el nombre de función. Las peticiones HTTP se comparan con la plantilla de petición para determinar si se llama a la función de aplicación. La plantilla de petición puede incluir un protocolo, un dominio y un sistema principal; puede estar precedida por una barra inclinada (/), y puede utilizar un asterisco (\*) como carácter comodín. Por ejemplo, las posibilidades `/front_page.html`, `http://www.ics.raleigh.ibm.com/pub*`, `/*` y `*` son todas válidas. El nombre de función es el nombre asignado a la función de aplicación del programa. Está codificado y debe escribirse exactamente como se muestra. Los primeros dos argumentos se delimitan por un espacio. Los dos últimos argumentos se delimitan mediante dos puntos (:).

La directiva `Authentication` tiene dos argumentos: (1) la vía de acceso plenamente cualificada de la biblioteca compartida y (2) el nombre de función. Estos argumentos se delimitan por dos puntos(:). El primer argumento es específico del sistema y depende de dónde está instalada la biblioteca compartida. La plantilla de URL del primer argumento debe empezar en el directorio raíz de documentos (/) al utilizar `Caching Proxy` como proxy de retorno. El segundo argumento se codifica en la biblioteca compartida y debe escribirse exactamente como se muestra.

La directiva `ServerTerm` tiene dos argumentos: (1) la vía de acceso plenamente cualificada de la biblioteca compartida y (2) el nombre de función. Estos argumentos se delimitan por dos puntos(:). El primer argumento es específico del sistema y depende de dónde está instalada la biblioteca compartida. El segundo argumento se codifica en la biblioteca compartida y debe escribirse exactamente como se muestra. Esta directiva finaliza el daemon PAC cuando se cierra el servidor proxy. Si el propietario del daemon es distinto del propietario del servidor proxy, es posible que el servidor proxy no pueda detener el daemon, en cuyo caso un administrador debe detener manualmente el daemon.

```
ServerInit vía_acceso_biblioteca_compartida
: pacwte_auth_init archivo_políticas_conf_vía_acceso
```

Ejemplo de Linux y UNIX:

```
ServerInit /usr/lib/libpacwte.so: pacwte_auth_init /etc/pac.conf
```

Ejemplo de Windows:

```
ServerInit C:\Progra ~1\IBM\edge\cp\lib\plugins\
pac\pacwte.dll: pacwte_auth_init C:\Progra ~1\IBM\edge\cp
Authorization request-template vía_de_biblioteca_compartida: pacwte_auth_policy
```

Ejemplo de Linux y UNIX:

```
Authorization http://* /usr/lib/libpacwte.so: pacwte_auth_policy
```

Ejemplo de Windows:

```
Authorization http://* C:\Archivos de programa\IBM\edge\cp\lib\plugins\
pac\pacwte.dll: pacwte_auth_policy
```

Authentication BASIC *vía\_acceso\_biblioteca\_compartida*:pacwte\_auth\_policy

Ejemplo de Linux y UNIX:

Authentication BASIC /usr/lib/plugins/pac/libpacwte.so:pacwte\_auth\_policy

Ejemplo de Windows:

Authentication BASIC C:\Archivos de programa\IBM\edge\cp\lib\plugins\  
pac\pacwte.dll:pacwte\_auth\_policy

ServerTerm *vía\_acceso\_biblioteca\_compartida*:pacwte\_shutdown

Ejemplo de Linux y UNIX:

ServerTerm /usr/lib/libpacwte.so:pacwte\_shutdown

Ejemplo de Windows:

ServerTerm BASIC C:\Archivos de programa\IBM\edge\cp\lib\plugins\  
pac\bin\pacwte.dll:pacwte\_shutdown

---

## Edición de los archivos de configuración del módulo de autorización PAC-LDAP

Los archivos de configuración y de políticas del módulo de autorización PAC-LDAP deben editarse manualmente con un editor de texto. Un nombre de directiva se separa del primer argumento mediante dos puntos (:). Si existen varios argumentos se delimitan por comas (,). Los comentarios incluidos los archivos de configuración y de políticas ayudan a editarlos. A continuación se muestran las directivas de políticas más relevantes.

### paccp.conf

Las bibliotecas compartidas leen el archivo paccp.conf durante la inicialización de Caching Proxy y dicho archivo contiene las definiciones (apartado [PAC\_MAN\_SERVER]) de cada uno de los daemons PAC que se iniciarán. Todos los daemons PAC deben tener su propio apartado [PAC\_MAN\_SERVER].

```
[PAC_MAN_SERVER]
hostname:                # name of PAC daemon
port:                    # port pacd is listening on

[PACWTE_PLUGIN]
hostname_check:[true|false] # enables DNS lookup. Must have
                                # DNS lookup turned on for ibmproxy to work.
```

### pac.conf

El archivo pac.conf especifica el servidor LDAP con el que el daemon PAC intenta conectarse.

```
[PAC_MAN_SERVER]
hostname:                # name of PAC daemon
port:                    # port pacd is listening on
conn_type:ssl             # comment out if you do not use SSL
authentication_sequence: [primary|secondary|none]
authorization_sequence:  [primary|secondary|none]

[LDAP_SERVER]
hostname:                # LDAP Server hostname
port:389                  # Port LDAP is listening on
ssl_port:636              # SSL port used by the LDAP server
admin_dn:                 # User with permission to access the LDAP server
                                # specify admin_dn=NULL to enable anonymous binding
search_base:              # Portion of LDAP tree to search for policy info
```

```

search_key:                                # If not required, specify search_base=NULL
   # ID field to search

[CACHE]
cred_cache_enabled [TRUE|FALSE] # turn credentials cache on
cred_cache_min_size:100         # minimum number of credentials to cache in pacd
cred_cache_max_size:64000       # maximum number of credentials to cache in pacd
cred_cache_expiration:86400     # when a credential expires
policy_cache_enabled:[TRUE|FALSE] # turns policy cache on/off
policy_cache_min_size:100       # min. number of policy related items to cache
policy_cache_max_size:64000     # max. number of policy related items to cache
policy_cache_expiration:86400   # when a policy related item expires

```

## pacpolicy.conf

Todas las políticas LDAP utilizan la siguiente plantilla en los archivos de configuración y de políticas. Todas las políticas deben empezar por la palabra clave en mayúscula POLICY entre paréntesis.

```

[POLICY]
default_policy:[grant|deny] # describes the default policy for users
                             # that are not described in the POLICY section
pac_client_hotname:         # the instances of Caching Proxy that are allowed
                             # to use a policy list
id:                          # the id for the LDAP entry or ip/hostname
                             # (wildcard supported, such as *.ibm.com)
grant:[true|false]          # true means to grant access, false means
                             # to deny access
type:[0|1|2|3|4]            # 0 LDAP entry that is a group,
                             # 1 LDAP entry that is not a group,
                             # 2 IP address
                             # 3 hostname
                             # 4 URL
propagate:[true|false]      # true means that the access rights (grant
                             # or deny) will be propagated to all
                             # descendants or members
stop_entry:[entry|NULL]     # Propagation of the access right stops
                             # at this entry. If the id is a group,
                             # stop_entry must be set to NULL.
                             # stop_entry may be applied to an IP
                             # address or hostname. Each stop_entry
                             # must be on its own line
exception_entry:[entry|NULL] # Assignment of the access right skips
                             # these entries, but continues through their
                             # subtrees. This may be a list of entries.
                             # exception_entry may be applied to a group,
                             # IP address, or hostname. Each
                             # exception_entry must be on its own line.

Exception_type:
Exception:

```

Sólo se da soporte al carácter comodín (\*) cuando ocupa la última posición de una dirección IP o la primera posición de un nombre de sistema principal de las directivas id y stop\_entry . Los caracteres comodín no reciben soporte en exception\_entry . Tampoco se da soporte a los caracteres comodín en las entradas LDAP de cualquier campo.

Se da soporte a varias políticas y, si las políticas entran en conflicto, el valor false siempre tiene preferencia. Es decir, se bloquea el acceso sólo con que se produzca una única denegación en cualquier política. El orden en que se enumeran las políticas en los archivos de configuración y de políticas es irrelevante y no establece ninguna prioridad.

Para obtener un conjunto de ejemplos de políticas, consulte el archivo `the_pacpolicy.conf` del directorio de archivos de configuración.

**Nota:** Los grupos anidados no heredan las políticas de los grupos padres. Las únicas políticas que se aplican a un grupo son aquellas para las que el grupo es un miembro explícito.

---

## Creación de `pac_ldap.cred`

Cree un archivo de texto plano denominado `pac_ldap.cred` en `/raíz_cp/server_root/pac/creds`. Este archivo contiene la contraseña correspondiente al nombre de usuario de la directiva `admin_dn`, que se encuentra en el archivo `pac.conf`.

**Nota:** Para habilitar enlaces anónimos, modifique la directiva `admin_dn` de `pac.conf` a `admin_dn:NULL` y añada una serie ficticia en el archivo `pac_ldap.cred`.

El daemon PAC cifra la contraseña la primera vez que lee el archivo.

Para crear el archivo `pac_ldap.cred` en las plataformas Linux y UNIX, emita los siguientes mandatos:

```
cd raíz_cp/server_root/pac/creds
echo "password" > pac_ldap.cred
chown nobody pac_ldap.cred
chgrp nobody pac_ldap.cred
(en SUSE Linux, utilice chgrp nogroup pac_ldap.cred.)
```

Para crear el archivo en una plataforma Windows, escriba la contraseña en un archivo de texto y almacene el archivo en el directorio `server_root\pac\creds\`.

---

## Inicio y detención de `pacd`

El daemon de autorización LDAP se ejecuta como el proceso `pacd`. Puede reiniciar el daemon de autorización LDAP sin interrumpir Caching Proxy mediante la utilización de los scripts que se facilitan. Ejecute el script `pacd` del modo siguiente:

- En las plataformas Linux y UNIX:  
`/usr/sbin/pacd_restart.sh id_usuario_pacd`
- En las plataformas Windows:  
`C:\Archivos de programa\IBM\edge\cp\Bin\pacd_restart.bat raíz_instalación_CP`

**Nota:** Es posible que el proceso `pacd` continúe ejecutándose después de que se cierre el servidor de proxy de colocación en antememoria mediante el mandato **stopsrc -ibmproxy** en los sistemas AIX o el mandato **ibmproxy -stop** en los sistemas HP-UX, Linux y Solaris. El proceso `pacd` se puede cerrar de modo seguro mediante el mandato **kill** tal como se muestra a continuación:

```
kill -15 ID_proceso_pacd
```

**En HP-UX:** es posible que el plug-in PAC-LDAP y `pacd` no carguen todas las bibliotecas compartidas dependientes durante el tiempo de ejecución. Antes de utilizarlos, asegúrese de que las variables de sistema estén establecidas del siguiente modo

```
SHLIB_PATH=/usr/lib:/usr/IBMldap/lib
PATH=/usr/IBMldap/bin:$PATH
PATH=/usr/IBMldap/bin
```

/usr/IBMDap/ es la vía de acceso de instalación por omisión del cliente LDAP en HP-UX. Se recomienda que ajuste PATH y SHLIB\_PATH según corresponda si el cliente LDAP se instala en una ubicación distinta. Sin establecer estas variables, pueden ocurrir los siguientes errores:

- Después de habilitar el plug-in del PAC-LDAP, aparecerá el siguiente mensaje en las anotaciones cronológicas de error  
"Serverinit Error: server did not load functions  
from DLL module /opt/ibm/edge/cp/lib/plugins/pac/libpacwte.sl"
- Al intentar iniciar /usr/sbin/pacd, aparecerá el siguiente error de enlace  
"/usr/lib/dld.sl: Can't find path for shared library: libibmldap.sl  
/usr/lib/dld.sl: No such file or directory  
Abort"

**En Linux:** en SUSE Linux Enterprise Server 9, ldd pacd podría informar que no se encuentra libldap.so. Para evitar este problema, cree el siguiente enlace simbólico:

```
ln -s /usr/lib/libldap.so.19 /usr/lib/libldap.so
```

**En AIX:** al iniciar pacd con IBM Tivoli Directory Server 5.2, es posible que el módulo PAC-LDAP no pueda cargarse y se genere el siguiente error:

```
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.
```

Para evitar este problema, cree el siguiente enlace simbólico:

```
ln -s /usr/lib/libibmldap.a /usr/lib/libldap.a
```

**Nota:** Después de la configuración de Caching Proxy para que utilice la autenticación LDAP, se mostrará el siguiente error:

```
Could not extract a value for: Uid, return code:3
```

Este error se mostrará incluso cuando la autenticación LDAP funcione correctamente y puede hacerse caso omiso de él.



---

## Parte 6. Supervisión de Caching Proxy

Esta parte proporciona las instrucciones para supervisar Caching Proxy utilizando las anotaciones cronológicas y el Supervisor de actividad de servidor

Esta parte contiene los siguientes capítulos:

Capítulo 30, “Configuración de las anotaciones cronológicas”, en la página 151

Capítulo 31, “Utilización del Supervisor de actividad del servidor”, en la página 159





---

## Capítulo 30. Configuración de las anotaciones cronológicas

Para personalizar las anotaciones cronológicas, puede utilizar los formularios de Configuración y Administración o editar las directivas del archivo de configuración de proxy. Puede establecer las siguientes opciones:

- Vías de acceso y nombres de archivo para almacenar los archivos de anotaciones cronológicas
- Filtros para incluir información en los archivos de anotaciones cronológicas de acceso y excluirla
- Opciones de mantenimiento para archivar o eliminar las anotaciones cronológicas

---

### Acerca de las anotaciones cronológicas

Caching Proxy puede crear tres tipos de anotaciones cronológicas de acceso, además de las anotaciones cronológicas de sucesos y las anotaciones cronológicas de error:

- Anotaciones cronológicas de acceso:
  - **Anotaciones cronológicas de acceso:** hacen un seguimiento de las peticiones administrativas a Caching Proxy.
  - **Anotaciones cronológicas de acceso a la antememoria:** hacen un seguimiento de las peticiones de objetos que se encuentran en la antememoria.
  - **Anotaciones cronológicas de acceso al proxy:** hacen un seguimiento de las peticiones que pasan por el proxy procedentes de los servidores de origen.
- **Anotaciones cronológicas de sucesos:** hacen un seguimiento de los mensajes informativos de antememoria.
- **Anotaciones cronológicas de error:** hacen un seguimiento de los mensajes de error relacionados con Caching Proxy.

Caching Proxy crea nuevos archivos de anotaciones cronológicas todos los días a las doce de la noche. Si el proxy no se está ejecutando a esa hora, se crean nuevas anotaciones cronológicas la primera vez que se inicia ese día. Puede especificar el directorio y el prefijo de nombre de archivo de todos los archivos de anotaciones cronológicas. Todos estos archivos creados también contienen un sufijo de fecha con el formato *.Mmmddaaaa* (por ejemplo, *.Apr142000*).

Como las anotaciones cronológicas pueden utilizar una gran cantidad de espacio, se le recomienda que almacene los archivos de anotaciones cronológicas en un dispositivo de almacenamiento que sea independiente del sistema operativo y de la antememoria para prevenir errores. Asimismo, configure las rutinas de mantenimiento como se especifica en “Mantenimiento y archivado de las anotaciones cronológicas” en la página 155.

---

### Nombres de los archivos de anotaciones cronológicas y opciones básicas

Para especificar la configuración básica de las anotaciones cronológicas de servidor proxy, seleccione **Configuración de servidor** -> **Anotación cronológica** -> **Archivos de anotaciones cronológicas** en los formularios de Configuración y Administración. Especifique la vía de acceso y el nombre de archivo de todos los

archivos de anotaciones cronológicas que desee utilizar. El nombre de archivo actual de cada uno de los archivos de anotaciones cronológicas se muestra en el recuadro de texto correspondiente. Si no ha especificado una vía de acceso, se visualiza la vía de acceso por omisión.

La información que se anota cronológicamente en las anotaciones cronológicas del proxy no se escribe automáticamente en las anotaciones cronológicas del sistema, pero puede configurar Caching Proxy para que escriba en las anotaciones cronológicas del sistema además de sus propias anotaciones cronológicas o en lugar de ellas. En el formulario **Archivos de anotaciones cronológicas**, seleccione el recuadro de selección **Registrar información en Syslog**. Tenga en cuenta que las anotaciones cronológicas del sistema deben crearse antes de que se seleccione esta opción.

Para especificar que la información de las anotaciones cronológicas del servidor proxy se escriban únicamente en las anotaciones cronológicas del sistema, debe editar el archivo de configuración de proxy. Consulte el apartado de referencia “LogToSyslog: especificar si se va a enviar la información de acceso a las anotaciones cronológicas del sistema (Linux y UNIX sólo)” en la página 238.

### **Directivas de archivos de configuración relacionadas**

Para configurar las anotaciones cronológicas mediante el archivo de configuración de proxy, consulte los apartados de referencia del Apéndice B, “Directivas del archivo de configuración”, en la página 177 para obtener información sobre las siguientes directivas:

- “AccessLog: nombrar la vía de acceso del archivo de anotaciones cronológicas de acceso” en la página 179
- “CacheAccessLog: especificar la vía de acceso de los archivos de anotaciones cronológicas de acceso a la antememoria” en la página 191
- “ErrorLog: especificar el archivo donde se anotan cronológicamente los errores de servidor” en la página 215
- “EventLog: especificar la vía de acceso del archivo de anotaciones cronológicas de sucesos” en la página 218
- “LogToSyslog: especificar si se va a enviar la información de acceso a las anotaciones cronológicas del sistema (Linux y UNIX sólo)” en la página 238
- “MaxLogFileSize: especificar el tamaño máximo para todos los archivos de anotaciones cronológicas” en la página 242
- “ProxyAccessLog: nombrar la vía de acceso del archivo de anotaciones cronológicas de acceso al proxy” en la página 267

---

## **Filtros de las anotaciones cronológicas de acceso**

Las anotaciones cronológicas registran la actividad de la máquina del sistema principal, el proxy y la antememoria. Para todas las peticiones de acceso que recibe el proxy, existe una entrada de las anotaciones cronológicas adecuadas que incluye la siguiente información:

- Qué se ha solicitado
- Cuándo se ha solicitado
- Quién lo ha solicitado
- Método de la petición
- Tipo de archivo que el servidor ha enviado en respuesta a la petición
- Código de retorno, que indica si la petición se ha realizado correctamente

- Tamaño de los datos enviados

Los errores de acceso se anotan cronológicamente en las anotaciones cronológicas de error del servidor.

## Razones para controlar los elementos que se anotan cronológicamente

Existen varias razones para limitar qué elementos se anotan cronológicamente:

- Para reducir el tamaño de las anotaciones cronológicas

Los archivos de anotaciones cronológicas de un servidor ocupado pueden hacerse lo suficientemente grande para ocupar todo el espacio de disco del servidor. Por omisión, todas las peticiones de acceso se anotan cronológicamente, lo que significa que las entradas de anotaciones cronológicas se realizan no sólo para una página HTML sino también para todas las imágenes que contiene la página. La inclusión sólo de las peticiones de acceso relevantes puede reducir significativamente el número de entradas en las anotaciones cronológicas. Por ejemplo, es posible que desee configurar las anotaciones cronológicas de acceso para que incluyan las entradas de anotaciones cronológicas de las peticiones de acceso a las páginas HTML pero no de las peticiones de imágenes GIF.

- Para recopilar información de destino

Por ejemplo, si está interesado en quién está accediendo al servidor desde fuera de la empresa, puede especificar un filtro que excluya las peticiones de acceso que se originan a partir de las direcciones IP de la empresa. Si está interesado en averiguar el volumen de usuarios que visitan un determinado sitio Web, puede crear anotaciones cronológicas de acceso que sólo muestren las peticiones de acceso a ese URL.

La información que se excluye de las anotaciones cronológicas de acceso no se registra en ningún informe de acceso y no está disponible para su uso futuro. Por lo tanto, si no está seguro de la cantidad de información sobre la que es necesario hacer un seguimiento, aplique los filtros de exclusión con moderación hasta que tenga la suficiente experiencia en la supervisión del servidor.

## Configuración de las anotaciones cronológicas de acceso

Las entradas de anotaciones cronológicas de acceso pueden filtrarse basándose en cualquiera de los atributos siguientes:

- URL (archivos o directorios)
- Dirección IP o nombre de sistema principal
- Agentes de usuario
- Método
- Tipo MIME
- Código de retorno

Para especificar los filtros, seleccione **Configuración de servidor -> Exclusiones de anotaciones cronológicas de acceso** en los formularios de Configuración y Administración. Especifique sólo las exclusiones que desee. No es necesario que utilice todas las categorías.

- En el apartado encabezado por **No registrar las peticiones en los directorios/archivos siguientes del Archivo de anotaciones cronológicas de acceso:**, enumere las vías de acceso de URL para las que desea excluir las entradas de anotaciones cronológicas.

- En el apartado encabezado por **No registrar las peticiones de los usuarios-agentes siguientes**:, enumere los agentes de proxy para los que desea excluir las entradas de anotaciones cronológicas.
- En el apartado encabezado por **No registrar las peticiones de los Nombres de sistema principal o las direcciones IP siguientes**:, enumere los nombres de sistema principal o direcciones IP para los que desea excluir las entradas de anotaciones cronológicas.
- En el apartado encabezado por **No registrar peticiones con los Métodos siguientes**:, seleccione los recuadros de cualquiera de los métodos para los que desea excluir las entradas de anotaciones cronológicas.
- En el apartado encabezado por **No registrar peticiones de archivos de los tipos MIME siguientes**:, seleccione los recuadros de cualquiera de los tipos MIME para los que desea excluir las entradas de anotaciones cronológicas.

**Nota:** Esta directiva sólo afecta a las anotaciones cronológicas de acceso al proxy. No es posible filtrar las anotaciones cronológicas que enumeren estos objetos a partir del tipo MIME. Utilice AccessLogExcludeURL para llevar a cabo esta acción.

- En el apartado encabezado por **No registrar peticiones con los Códigos de retorno siguientes**:, seleccione los recuadros de los códigos de retorno de petición para los que desea excluir las entradas de anotaciones cronológicas.

Pulse **Someter**.

### Directivas de archivos de configuración relacionadas

Para establecer los filtros de anotaciones cronológicas de acceso mediante el archivo de configuración de proxy, consulte los apartados de referencia del Apéndice B, “Directivas del archivo de configuración”, en la página 177 para obtener información sobre las siguientes directivas:

- “AccessLogExcludeMethod: suprimir las entradas de anotaciones cronológicas de los archivos y directorios solicitados por un método específico” en la página 180
- “AccessLogExcludeMimeType: suprimir las entradas de anotaciones cronológicas de acceso al proxy para tipos MIME específicos” en la página 181
- “AccessLogExcludeReturnCode: suprimir las entradas de anotaciones cronológicas de códigos de retorno específicos” en la página 181
- “AccessLogExcludeURL: suprimir las entradas de anotaciones cronológicas de archivos o directorios específicos” en la página 182
- “AccessLogExcludeUserAgent: suprimir las entradas de anotaciones cronológicas de navegadores específicos” en la página 182
- “NoLog: suprimir las entradas de anotaciones cronológicas de los sistemas principales o dominios específicos que coinciden con una plantilla” en la página 248

---

## Valores de anotaciones cronológicas por omisión

- **Vías de acceso por omisión**

Todas las anotaciones cronológicas se habilitan en la configuración por omisión de Caching Proxy. Se almacenan en el subdirectorio logs/ del directorio de instalación. Las vías de acceso por omisión son las siguientes:

- Anotaciones cronológicas de acceso (administrativo) local:
  - Linux y UNIX: /opt/ibm/edge/cp/server\_root/logs/local
  - Windows: *unidad*:\Archivos de programa\IBM\edge\cp\logs\local

- Anotaciones cronológicas de acceso a la antememoria:
  - Linux y UNIX: /opt/ibm/edge/cp/server\_root/logs/cache
  - Windows: *unidad:*\Archivos de programa\IBM\edge\cp\logs\cache
- Anotaciones cronológicas de acceso al proxy:
  - Linux y UNIX: /opt/ibm/edge/cp/server\_root/logs/proxy
  - Windows: *unidad:*\Archivos de programa\IBM\edge\cp\logs\proxy
- Anotaciones cronológicas de error:
  - Linux y UNIX: /opt/ibm/edge/cp/server\_root/logs/error
  - Windows: *unidad:*\Archivos de programa\IBM\edge\cp\logs\error
- Anotaciones cronológicas de sucesos:
  - Linux y UNIX: /opt/ibm/edge/cp/server\_root/logs/event
  - Windows: *unidad:*\Archivos de programa\IBM\edge\cp\logs\event

Todos los nombres de archivo de anotaciones cronológicas son una combinación del nombre base y un sufijo de fecha con el formato *.Mmmddaaaa*, por ejemplo, *proxy.Feb292000*.

- **Formatos por omisión**

Las anotaciones cronológicas se almacenan en el formato de archivo común por omisión. También está disponible un formato de anotaciones cronológicas combinado, que puede establecerse añadiendo la siguiente línea al archivo de configuración de proxy (*ibmproxy.conf*).

```
LogFileFormat combined
```

El formato de anotaciones cronológicas combinado es parecido al formato común pero tiene campos añadidos que muestran al referente, el agente de usuario y la información de cookie. El formato de tiempo local es el formato de tiempo por omisión.

- **Contenido por omisión**

Por omisión, todas las peticiones de acceso se registran en las anotaciones cronológicas de acceso adecuadas y no se registra ninguna información de acceso en las anotaciones cronológicas del sistema. La información de anotaciones cronológicas de error sólo se escribe en las anotaciones cronológicas de error y la información de anotaciones cronológicas de sucesos sólo en las anotaciones cronológicas de sucesos.

- **Mantenimiento por omisión**

En la configuración por omisión, las anotaciones cronológicas no se archivan ni se suprimen.

---

## Mantenimiento y archivado de las anotaciones cronológicas

Caching Proxy utiliza un plug-in para gestionar las anotaciones cronológicas. Para obtener más información, consulte la página de referencia en el Apéndice B, "Directivas del archivo de configuración", en la página 177 para obtener información sobre la directiva del archivo de configuración "Midnight: especificar el plug-in de API utilizado para archivar las anotaciones cronológicas" en la página 246.

Ahora puede especificar cómo archivar y eliminar las anotaciones cronológicas diariamente. Las opciones básicas son:

- Comprimir y eliminar las anotaciones cronológicas que sean anteriores a una antigüedad especificada.

- Eliminar las anotaciones cronológicas después de que alcancen una antigüedad especificada o después de que la categoría de anotaciones cronológicas alcance un tamaño colectivo especificado.
- Ejecutar su propio programa a las doce de la noche todas las noches para mantener y archivar las anotaciones cronológicas.

Por omisión, las anotaciones cronológicas del día actual y de los días anteriores no se suprimen nunca mediante un agente de mantenimiento. Todas las anotaciones cronológicas del día actual y las anotaciones cronológicas de acceso a la antememoria de los días anteriores nunca se comprimen mediante el agente de mantenimiento.

Para configurar el mantenimiento de las anotaciones cronológicas, seleccione **Configuración de servidor -> Anotación cronológica -> Archivado de anotaciones cronológicas** en los formularios de Configuración y Administración. En este formulario, utilice el recuadro desplegable para especificar el método de mantenimiento.

- Si ha optado por **Purge**, establezca la antigüedad, el tamaño de archivo o ambos para utilizarlos con el fin de determinar qué anotaciones cronológicas se desea suprimir. Cuando los archivos se depuran en función de la antigüedad y el tamaño, los archivos anteriores a la antigüedad máxima se depuran antes que los archivos mayores que el tamaño máximo. Cuando los archivos se depuran según el tamaño, las anotaciones cronológicas más antiguas se suprimen primero.
- Si opta por **Compress**, establezca la antigüedad de las anotaciones cronológicas que se vayan a comprimir y el mandato que se vaya a utilizar para comprimir los archivos de anotaciones cronológicas (incluidos todos los parámetros). Asimismo, establezca la antigüedad máxima de las anotaciones cronológicas. Después de comprimir las anotaciones cronológicas, el agente de mantenimiento suprime las anotaciones cronológicas comprimidas anteriores a la antigüedad máxima.

### Directivas relacionadas del archivo de configuración

Para configurar el archivado de anotaciones cronológicas mediante el archivo de configuración de proxy, consulte las páginas de referencia del Apéndice B, “Directivas del archivo de configuración”, en la página 177 para obtener información sobre las siguientes directivas:

- “CompressAge: especificar cuándo comprimir las anotaciones cronológicas” en la página 202
- “CompressDeleteAge: especificar cuándo suprimir las anotaciones cronológicas” en la página 204
- “CompressCommand: especificar el mandato y los parámetros de compresión” en la página 203
- “LogArchive: especificar el comportamiento del archivado de las anotaciones cronológicas” en la página 237
- “Midnight: especificar el plug-in de API utilizado para archivar las anotaciones cronológicas” en la página 246
- “PurgeAge: especificar el límite de antigüedad para las anotaciones cronológicas” en la página 271
- “PurgeSize: especificar el límite del tamaño del archivador de anotaciones cronológicas” en la página 272.



---

## Escenario de archivo de anotaciones cronológicas

El siguiente ejemplo muestra cómo puede personalizar el registro cronológico para satisfacer sus necesidades. Suponga que acaba de adquirir e instalar Caching Proxy. Y desea configurar el servidor para anotar cronológicamente la información de error y acceso con los siguientes requisitos:

- Las anotaciones cronológicas deben incluir una indicación de hora local y deben aparecer en un formato de archivo de anotaciones cronológicas común.
- Las anotaciones cronológicas de acceso deben depurarse cuando tengan una antigüedad superior a 30 días o cuando las anotaciones cronológicas alcancen un tamaño colectivo de 25 MB.
- Los siguientes tipos de peticiones no deben anotarse cronológicamente en las anotaciones cronológicas de acceso:
  - Peticiones de imágenes GIF
  - Peticiones procedentes de sistemas principales con direcciones IP que coinciden con el patrón 130.128.\*.\*
  - Peticiones de redirección (estas peticiones emiten un código de retorno entre 300 y 399)

Para configurar Caching Proxy de modo que mantenga las anotaciones cronológicas de acuerdo con estos criterios, en los formularios de Configuración y Administración, seleccione **Configuración de servidor** → **Anotación cronológica**.

1. Opcionalmente, seleccione el **formulario Archivos de anotaciones cronológicas** para especificar las vías de acceso de los archivos de anotaciones cronológicas de acceso. Se facilitan vías de acceso por omisión.
2. Utilice el formulario **Archivado de anotaciones cronológicas** para especificar cómo archivar los archivos:
  - Especifique **Depurar** como método de archivado.
  - Bajo **Al utilizar Depurar**, rellene los campos como se indica a continuación:
    - **Suprimir anotaciones cronológicas con más de 30 días**
    - **Suprimir anotaciones cronológicas mayores de 25 MB**
3. Utilice el formulario **Exclusiones de anotaciones cronológicas** para filtrar las entradas de anotaciones cronológicas como se indica a continuación:
  - En la lista **No registrar las peticiones de los Nombres de sistema principal o las direcciones IP siguientes**:, añada 130.128.\*.\* en el campo **Sistema principal excluido**.
  - Bajo **No registrar peticiones de archivos de los tipos MIME siguientes**:, seleccione el recuadro de selección **image/gif**.
  - Bajo **No registrar peticiones con los Códigos de retorno siguientes**:, seleccione el recuadro de selección (3xx) **Redirección**.

Si se siguen estas instrucciones, se generan las siguientes líneas en el archivo de configuración de proxy:

```
LogArchive purge
PurgeAge 30
PurgeSize 25
AccessLogExcludeURL *.gif
NoLog 130.128.*.*
AccessLogExcludeReturnCode 300
```





---

## Capítulo 31. Utilización del Supervisor de actividad del servidor

El Supervisor de actividad de servidor de Caching Proxy muestra las estadísticas del rendimiento de red y de servidor, el estado de la red y el servidor, y las entradas de anotaciones cronológicas de acceso. El supervisor puede utilizarse de forma remota y no es necesario que esté en la misma máquina en la que se está ejecutando el servidor proxy. El Supervisor de actividad del servidor se habilita por omisión y no requiere ninguna configuración.

Existen dos formas de abrir el Supervisor de actividad del servidor:

- En cualquier navegador Web conectado, especifique el siguiente URL utilizando donde se indica el nombre completo del servidor.  
`http://su.nombre.servidor/Usage/Initial`
- En los formularios de Configuración y Administración, seleccione **Supervisor de actividad de servidor**.

A diferencia de otros formularios del cliente de configuración, los formularios de esta categoría no establecen las configuraciones del servidor, pero visualizan los datos sobre el uso del servidor. Estos formularios proporcionan mucha más información de la que puede visualizarse en una única ventana de la consola.

Los apartados siguientes muestran el tipo de información que proporciona **Supervisor de actividad de servidor** y sugieren cómo utilizar la información para ajustar el rendimiento.

Existen varias páginas de **Supervisor de actividad de servidor** a las que se puede acceder:

- **Estadísticas de actividad**
- **Estadísticas de red**
- **Estadísticas de acceso**
- **Estadísticas de acceso a proxy**
- **Estadísticas de antememoria**
- **Resumen de renovación de la antememoria**

Todas las páginas tienen un botón **Renovar**, que se pueden utilizar para actualizar la información.

### Estadísticas de actividad

La Tabla 4 muestra un ejemplo de la página de **Estadísticas de actividad**.

*Tabla 4. Estadísticas de actividad*

| Estadísticas de actividad      |                           |
|--------------------------------|---------------------------|
| Conexiones                     | 1 Activa, 431 como máximo |
| Tiempo de respuesta            | No está disponible        |
| Productividad                  | 0 conexiones/segundo      |
| Peticiones procesadas hoy      | 0                         |
| Total de peticiones procesadas | 114                       |

Tabla 4. Estadísticas de actividad (continuación)

| Estadísticas de actividad |   |
|---------------------------|---|
| Errores de petición       | 3 |

Estas estadísticas de actividad del servidor pueden utilizarse para supervisar el tráfico del servidor en términos del número de peticiones de acceso, tiempo de respuesta, productividad, peticiones procesadas hoy, total de peticiones procesadas y errores. Los siguientes cambios de configuración tienen un efecto sobre las estadísticas de la página **Actividad**.

- **Número de hebras activas:** esta opción especifica cuántas hebras se desea utilizar para las peticiones de servidor. Puede aumentar o disminuir el número de hebras disponibles, dependiendo de la memoria de la que disponga. Para modificar el número de hebras activas en los formularios de Configuración y Administración, seleccione **Configuración de servidor → Gestión del servidor → Rendimiento** o bien edite la directiva MaxActiveThreads del archivo de configuración. (Consulte “MaxActiveThreads: especificar el número máximo de hebras activas” en la página 242.)
- **Conexiones persistentes:** el hecho de que el proxy permita conexiones persistentes con un cliente puede afectar al rendimiento de red. Para modificar este valor en los formularios de Configuración y Administración, seleccione **Configuración de proxy → Rendimiento del proxy** para habilitar o inhabilitar las conexiones persistentes y, a continuación, seleccione **Configuración de servidor → Gestión del servidor** para definir cómo mantener las conexiones. Para modificar estos valores utilizando el archivo de configuración, consulte los apartados de referencia de las siguientes directivas:
  - “MaxPersistRequest: especificar el número máximo de peticiones que se van a recibir en una conexión persistente” en la página 243
  - “PersistTimeout: especificar el tiempo de espera para que el cliente envíe otra petición” en la página 254
  - “ProxyPersistence: permitir las conexiones persistentes” en la página 269

## Estadísticas de red

Tabla 5 muestra un ejemplo de la página de **Estadísticas de red**.

Tabla 5. Estadísticas de red

| Estadísticas de red          |                               |
|------------------------------|-------------------------------|
| Datos de salida:             | 1K bytes/segundo              |
| Datos de entrada:            | 1K bytes/segundo              |
| Ancho de banda guardado:     | 3 K bytes (0 K bytes/segundo) |
| Ancho de banda guardado hoy: | 0 K bytes (0 bytes/segundo)   |

El formulario **Estadísticas de red** proporciona información sobre la red en la que se está ejecutando el proxy, incluidas las velocidades de los datos enviados y recibidos.

## Estadísticas de acceso

La página **Estadísticas de acceso** muestra las 20 entradas más recientes de las anotaciones cronológicas de acceso. Esta página muestra las entradas más recientes de las anotaciones cronológicas de acceso al proxy (en caracteres negros) y de las

anotaciones cronológicas de acceso a la antememoria (en caracteres azules). Puede personalizar los datos que se muestran personalizando los datos que se anotan cronológicamente. Para obtener más información sobre las estadísticas de las anotaciones cronológicas de acceso, consulte “Filtros de las anotaciones cronológicas de acceso” en la página 152.

### **Estadísticas de acceso a proxy**

El formulario **Estadísticas de acceso a proxy** proporciona información sobre la actividad del proxy como, por ejemplo, cuáles son los URL que se han solicitado y si se han servido desde la antememoria. Después de los URL aparecen los códigos de retorno proporcionados a los clientes y el tamaño de archivo en bytes. Los siguientes valores pueden mejorar las estadísticas de acceso a proxy:

- Utilice la renovación de antememoria automática para aumentar la probabilidad de que un documento solicitado se encuentre en la antememoria. Consulte el Capítulo 20, “Configuración del agente de carga para la renovación y precarga automática”, en la página 93 para obtener detalles.
- Aumente el tiempo mínimo de retención de los archivos en antememoria. Consulte “Configuración de la antigüedad de antememoria” en la página 90 para obtener información detallada.
- No coloque en antememoria los archivos servidos desde el dominio local. Aunque este valor tiende a disminuir el número de peticiones servidas desde la antememoria, no se produce una reducción del rendimiento si los archivos se sirven desde la intranet local tan pronto como lo hacen desde la antememoria (en algunos casos, es más rápido). Consulte el Capítulo 18, “Control de los elementos colocados en antememoria”, en la página 83 para obtener información detallada.

### **Estadísticas de antememoria**

Si se habilita la colocación en antememoria, la página **Estadísticas de antememoria** muestra la información reciente de acceso a la antememoria. Proporciona información sobre la antememoria y el índice, incluidos los siguientes aspectos:

- Si la antememoria funciona actualmente o si se está reindexando a partir de un inicio de servidor
- Si la recogida de basura está en ejecución
- Las proporciones de coincidencias de antememoria

Muchas de las opciones de configuración de la antememoria modifican los resultados de las estadísticas de antememoria (consulte la Parte 4, “Configuración de la antememoria y el servidor proxy”, en la página 73).

### **Resumen de renovación de la antememoria**

Si el agente de antememoria se configura para cargar previamente los archivos en la antememoria, la página **Resumen de renovación de la antememoria** muestra la información sobre la ejecución mas reciente del agente de antememoria. El agente de antememoria debe haberse ejecutado como mínimo una vez para mostrar cualquier información. Para modificar el modo en que funciona el agente de renovación de antememoria, tenga en cuenta los siguientes puntos:

- Si la mayoría del tráfico de su intranet no es a sitios Web locales, es recomendable que inhabilite la colocación en antememoria del dominio local. Consulte el Capítulo 18, “Control de los elementos colocados en antememoria”, en la página 83 para obtener información detallada.

- Si un gran número de los clientes solicitan una página que no aparece en las anotaciones cronológicas de acceso a la antememoria, puede configurar manualmente el URL que se desea cargar. Consulte “Directivas relacionadas del archivo de configuración de proxy” en la página 98 para obtener las instrucciones.
- Ajuste el número de los URL más visitados que se van a cargar previamente. Consulte “Directivas relacionadas del archivo de configuración de proxy” en la página 98 para obtener las instrucciones.
- Especifica el periodo máximo de tiempo que el agente de antememoria puede ejecutarse. Consulte “Directivas relacionadas del archivo de configuración de proxy” en la página 98 para obtener las instrucciones.

---

## **Apéndice A. Utilización de los mandatos de Caching Proxy**

Este apéndice proporciona una referencia de los mandatos del servidor proxy.

---

## Mandato **cgiparse**

### Propósito

Utilice el mandato **cgiparse** para analizar la variable de entorno `QUERY_STRING` para los scripts CGI. Si no se establece la variable de entorno `QUERY_STRING`, el mandato lee los caracteres de `CONTENT_LENGTH` de la entrada estándar. Toda la salida devuelta se escribe en la salida estándar.

### Formato

`cgiparse -Distintivo [Modificador]`

### Parámetros

Los distintivos, junto con sus equivalentes de un único carácter (-k -f -v -r -i -s -p -c -q -P) y funciones, son:

**-keywords | -k**

Analiza `QUERY_STRING` en busca de palabras clave. Las palabras clave se decodifican y se escriben en la salida estándar, una por línea.

**-form | -f**

Analiza `QUERY_STRING` como una petición de formulario. Devuelve una serie que, cuando la evalúa el shell, establece las variables shell con el prefijo `FORM_` seguido de un nombre de campo. Los valores de campo se corresponden con el contenido de las variables.

**-value nombre-campo | -v nombre-campo**

Analiza `QUERY_STRING` como una petición de formulario. Devuelve el valor de *nombre-campo*.

**-read | -r**

Lee los caracteres de `CONTENT_LENGTH` de la entrada estándar y los escribe en la salida estándar.

**-init | -i**

Si no se establece `QUERY_STRING`, lee el valor de la entrada estándar y devuelve una sentencia SET que establece `QUERY_STRING` en este valor. Se puede utilizar con los métodos GET y POST. Un uso típico es:

```
eval 'cgiparse -init'
```

Con ello se establece la variable de entorno `QUERY_STRING`, independientemente de si se ha utilizado el método GET o POST.

Cuando se utiliza el método GET, **cgiparse** puede llamarse en el mismo script varias veces, pero, si se utiliza el método POST, sólo debe llamarse una vez. Con el método POST, después de la lectura de la entrada estándar, el siguiente mandato **cgiparse** encuentra vacía la entrada estándar y espera indefinidamente.

**-sep separador | -s separador**

Especifica la serie utilizada para separar varios valores. Si está utilizando el distintivo **-value**, el separador por omisión es newline. Si está utilizando el distintivo **-form**, el separador por omisión es una coma (,).

**-prefix prefijo | -p prefijo**

Si se utiliza con **-POST** y **-form**, especifica el prefijo que se debe utilizar al crear los nombres de las variables de entorno. El valor por omisión es `"FORM_"`.

**-count | -c**

Si se utiliza con **-keywords**, **-form** y **-value**, devuelve un recuento de los elementos relacionados con estos distintivos.

**-keywords | -k**

Devuelve el número de palabras clave.

**-form | -f**

Devuelve el número de campos exclusivos (varios valores se cuentan como uno).

**-value nombre-campo | -v nombre-campo**

Devuelve el número de valores de *nombre-campo* (si no existe un campo denominado *nombre-campo*, la salida es 0).

**-número**

Si se utiliza con **-keywords**, **-form** y **-value**, devuelve la aparición especificada relacionada con estos distintivos.

**-keywords**

Devuelve la palabra clave número *n*. Por ejemplo, **-2 -keywords** da salida a la segunda palabra clave.

**-form**

Devuelve todos los valores del campo número *n*. Por ejemplo **-2 -form** da salida a todos los valores del segundo campo.

**-value nombre-campo**

Devuelve el número *n* de los distintos valores del campo *nombre-campo*. Por ejemplo **-2 -value -whatsit** da salida al segundo valor del campo **whatsit**.

**-quiet | -q**

Suprime todos los mensajes de error. (Un estado de salida distinto de cero sigue indicando error.)

**-POST | -P**

La información de la entrada estándar (o en el caso de un nombre de archivo, el archivo stdin) se decodifica y analiza en variables shell directamente; no se utiliza QUERY\_STRING. **-POST** es equivalente al uso de las opciones **-init** y **-form**.

## Ejemplos

Los siguientes ejemplos ignoran el hecho de que, en realidad, el servidor ya ha establecido QUERY\_STRING. En los siguientes ejemplos, \$ es el indicador del shell Bourne.

- Búsqueda de palabras clave

```
$ QUERY_STRING="is+2%2B2+really+four%3F"
$ export QUERY_STRING
$ cgifparse -keywords
is
2+2
really
four?
$
```

- Examen de todos los campos de formulario

```
$ 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!"
$
```

- Extracción de un sólo valor de campo

```
$ QUERY_STRING="name1=value1&name2=Second+value%3F+That'\`s%27s"
$ cgiparse -value name1
value1
$ cgiparse -value name2
Second value? That's right!
$
```

## Resultados

- |   |                                                                                                                                                                                                       |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0 | Éxito                                                                                                                                                                                                 |
| 1 | Línea de mandatos no válida                                                                                                                                                                           |
| 2 | Las variables de entorno no se han establecido correctamente                                                                                                                                          |
| 3 | Se ha producido un error al obtener la información solicitada (por ejemplo, no existe ese campo o bien QUERY_STRING contiene palabras clave cuando se solicitan los valores de campos de formulario). |

**Nota:** Al recibir uno de estos códigos de error, es posible que también reciba mensajes de información adicional. El mensaje varía en función del mandato emitido.



---

## Mandato cgiutils

### Propósito

Utilice el mandato **cgiutils** en programas de cabecera que no sean resultado de análisis para producir una respuesta HTTP 1.0 completa.

**Nota:** Si desea proporcionar sus propios programas de cabecera que no sean resultado de análisis (nph) para devolver específicamente sus propios valores de retorno, el nombre del programa debe empezar por **nph-**. Con ello se evita que la cabecera del servidor sobrescriba su propio valor de retorno por el valor de retorno estándar del servidor.

### Formato

`cgiutils -Distintivo [Modificador]`

Si *Modificador* contiene espacios en blanco, inclúyalo entre comillas ("").

### Parámetros

**-version**

Devuelve la información de versión.

**-nodate**

No devuelve la cabecera **Date:**.

**-noel**

No devuelve una línea en blanco después de las cabeceras. Esto es útil si desea otras cabeceras MIME después de las líneas de cabecera iniciales.

**-status nnn**

Devuelve respuestas HTTP completas con el código de estado *nnn*, en lugar de un sólo conjunto de cabeceras HTTP. No utilice este distintivo si sólo desea la cabecera **Expires:**.

**-reason explicación**

Especifica la línea razón para la respuesta HTTP. Sólo puede utilizar este distintivo con el distintivo **-status nnn**.

**-ct [tipo/subtipo]**

Especifica la cabecera MIME Content-Type. Este ejemplo especifica un tipo de contenido MIME de text/html:

```
cgiutils -ct text/html
```

Si omite *tipo/subtipo*, el tipo de contenido MIME se establece en el valor por omisión text/plain. Este ejemplo establece el tipo de contenido MIME en text/plain.

```
cgiutils -ct
```

**-ce codificación**

Especifica la cabecera MIME Content-Encoding. Por ejemplo:

```
cgiutils -ce x-compress
```

**-cl código-idioma**

Especifica la cabecera MIME Content-Language. Por ejemplo:

```
cgiutils -cl en_UK
```

**-length nnn**

Especifica la cabecera MIME Content-Length.

**-expires** *Espec-Tiempo*

Especifica la cabecera MIME **Expires:**. Este distintivo especifica el tiempo de vida (fecha de caducidad de un documento) mediante cualquier combinación de días, horas, minutos y segundos. Se corresponde con el intervalo de tiempo durante el cual un documento se considera válido. Por ejemplo:

```
cgiutils -expires 2 days 12 hours
```

El mandato **cgiutils** añade el tiempo que especifique a la Hora Media de Greenwich actual para determinar la fecha de caducidad. La fecha de caducidad se incluye en la cabecera **Expires:** en el formato HTTP.

**-expires now**

Produce una cabecera **Expires:** que coincide con la cabecera **Date:**.

**-uri** *URI*

Especifica el URI (Universal Resource Identifier) del documento devuelto. El URI puede considerarse idéntico al URL.

**-extra xxx: yyy**

Especifica una cabecera adicional que no se puede especificar de otro modo para el mandato **cgiutils**.

## Ejemplos

- En este ejemplo se calcula la fecha de caducidad de la cabecera **Expires:**.  

```
cgiutils -expires "1 year 3 months 2 weeks 4 days 12 hours 30 mins"
```
- El siguiente ejemplo especifica un código de estado y una razón y establece la cabecera **Expires:** igual a la cabecera **Date:**.

```
cgiutils -status 200 -reason  
"Aparece un doc virtual" -expires now
```

Es posible que se generen cabeceras parecidas a éstas:

```
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
```

El mandato **cgiutils** produce automáticamente la cabecera **Server:**, ya que está disponible en el entorno CGI. El campo **Date:** también se genera automáticamente a menos que se especifique el distintivo **-nodate**.

Este ejemplo incluye una línea después de la salida para marcar el final del apartado de la cabecera MIME. Si desea continuar este ejemplo con más cabeceras, utilice el distintivo **-noel** archivo-configuración(NO-Empty-Line) tal como se muestra en el siguiente ejemplo.

- Si no desea que aparezca la línea en blanco después de la línea de cabecera, utilice el distintivo **-noel**:

```
cgiutils -noel -expires "2 days" -nodate  
HTTP/1.0 200 Virtual doc follows  
MIME-Version: 1.0  
Server: IBM-ICS  
Expires: Tue, 07 Jan 1996 03:43:46 GMT
```

---

## Mandato **htadm**

### Propósito

Utilice el mandato **htadm** para controlar los archivos de contraseñas del servidor. El servidor utiliza archivos de contraseñas para controlar el acceso a los archivos. Puede añadir un nombre de usuario al archivo de contraseñas, suprimir un usuario de un archivo de contraseñas, verificar una contraseña de usuario y crear un archivo de contraseñas vacío. Asimismo, puede modificar la contraseña de un usuario, suprimiendo primero la contraseña del usuario y creando, a continuación, una nueva.

**Nota:** Cuando utilice el mandato **htadm** para añadir un usuario, cambiar una contraseña o comprobar una contraseña, debe especificar la contraseña en la línea de mandatos. Como el mandato destruye la contraseña de la línea de mandatos tan pronto como es posible, es muy poco probable que pueda ver una contraseña del usuario examinando el listado de procesos de la máquina (con el mandato **ps**, por ejemplo).

### Formato

`htadm -Distintivo [Modificador]`

### Parámetros

**-adduser** *archivo-contraseñas* *nombre-usuario* [*contraseña* [*real-name*]]

Añade un usuario y una contraseña al archivo de contraseñas. Si especifica el mandato sólo con *archivo-contraseñas*, se le solicitarán los demás parámetros.

*archivo-contraseñas*

Vía de acceso y nombre del archivo de contraseñas al que desea añadir el usuario.

*nombre-usuario*

Nombre del usuario que desea añadir.

Utilice únicamente caracteres alfanuméricos para el nombre de usuario; no utilice caracteres especiales.

El mandato no se ejecuta correctamente si ya existe un usuario con el mismo nombre en el archivo de contraseñas.

*contraseña*

Contraseña que desea definir para el nombre de usuario.

Las contraseñas pueden tener una longitud de hasta 32 caracteres. Utilice únicamente caracteres alfanuméricos para la contraseña; no utilice caracteres especiales.

#### Notas:

1. Algunos navegadores no pueden leer y enviar contraseñas con una longitud superior a ocho caracteres. Debido a esta limitación, si define una contraseña superior a ocho caracteres, el servidor reconoce la contraseña completa o sólo los ocho primeros caracteres de la contraseña como válidos.
2. El nombre de usuario y la contraseña del administrador son sensibles a las mayúsculas y minúsculas incluso si el sistema operativo no lo es.

Asegúrese de entrar exactamente el nombre de usuario y la contraseña especificados mediante el mandato `htadm` al acceder a los formularios de Configuración y Administración.

*nombre-real*

Comentario o nombre que desea utilizar para identificar el nombre de usuario que está añadiendo. Todo lo que especifique se escribirá en el archivo de contraseñas.

**-deluser** *archivo-contraseñas* [*nombre-usuario*]

Suprime un usuario del archivo de contraseñas. Si especifica el mandato sólo con *archivo-contraseñas*, se le solicitará el parámetro *nombre-usuario*.

*archivo-contraseñas*

Vía de acceso y nombre del archivo de contraseñas del que desea eliminar un usuario.

*nombre-usuario*

Nombre del usuario que desea suprimir. El mandato no se ejecuta correctamente si el usuario que especifica no existe en el archivo de contraseñas.

**-passwd** *archivo-contraseñas* [*nombre-usuario* [*contraseña*]]

Modifica la contraseña de un nombre de usuario ya definido en el archivo de contraseñas. Si especifica el mandato sólo con *archivo-contraseñas*, se le solicitarán los demás parámetros.

*archivo-contraseñas*

Vía de acceso y nombre del archivo de contraseñas que contiene el nombre de usuario cuya contraseña desea modificar.

*nombre-usuario*

Nombre de usuario cuya contraseña desea modificar. El mandato no se ejecuta correctamente si el usuario que especifica no existe en el archivo de contraseñas.

*contraseña*

Nueva contraseña que desea definir para el nombre de usuario.

Las contraseñas pueden tener una longitud de hasta 32 caracteres. Utilice únicamente caracteres alfanuméricos para la contraseña; no utilice caracteres especiales.

**Notas:**

1. Algunos navegadores no pueden leer y enviar contraseñas con una longitud superior a ocho caracteres. Debido a esta limitación, si define una contraseña superior a ocho caracteres, el servidor reconoce la contraseña completa o sólo los ocho primeros caracteres de la contraseña como válidos.
2. El nombre de usuario y contraseña de administrador son sensibles a las mayúsculas y minúsculas incluso si el sistema operativo no lo es. Asegúrese de entrar el nombre de usuario y contraseña exactos especificados mediante el mandato `htadm` al acceder a los formularios de Configuración y Administración.

**-check** *archivo-contraseñas* [*nombre-usuario* [*contraseña*]]

Verifica la contraseña de un nombre de usuario ya definido en el archivo de contraseñas y permite averiguar si es correcta o no. Si especifica el mandato sólo con *archivo-contraseñas*, se le solicitarán los demás parámetros.

*archivo-contraseñas*

Vía de acceso y nombre del archivo de contraseñas que contiene el nombre de usuario cuya contraseña desea verificar.

*nombre-usuario*

Nombre de usuario cuya contraseña desea verificar. El mandato no se ejecuta correctamente si el usuario que especifica no existe en el archivo de contraseñas.

*contraseña*

Contraseña que desea verificar. Si la contraseña que especifica es la contraseña definida para el nombre de usuario, el mandato escribe Correct en la salida estándar y se completa con un código de retorno de 0. Si la contraseña que especifica no es la contraseña definida para el nombre de usuario, el mandato escribe Incorrect en la salida estándar.

**-create** *archivo-contraseñas*

Crea un archivo de contraseñas vacío.

*archivo-contraseñas*

Vía de acceso y nombre del archivo de contraseñas que desea crear.

## Ejemplos

- Para añadir un usuario a un archivo de contraseñas:
  - Sistemas Linux y UNIX:

```
htadm -adduser /opt/ibm/edge/cp/server_root/protect/heroes.pwd  
clark superman "Clark Kent"
```
  - Sistemas Windows:

```
htadm -adduser "C:\Archivos de programa\IBM\edge\cp\server_root\protect\  
heroes.pwd" clark superman "Clark Kent"
```

**Nota:** El mandato **htadm** debe aparecer en una línea. Aquí se muestra en más una línea por razones de claridad. Especifique el mandato real en una línea con un espacio entre clark y superman como mínimo.

- Para eliminar un usuario de un archivo de contraseñas:
  - Sistemas Linux y UNIX:

```
htadm -deluser /opt/ibm/edge/cp/server_root/protect/  
heroes.pwd clark superman "Clark Kent"
```
  - Sistemas Windows:

```
htadm -deluser "C:\Archivos de programa\IBM\edge\cp\server_root\protect\  
heroes.pwd" clark superman "Clark Kent"
```

---

## Mandato **htcformat**

### Propósito

Utilice el mandato **htcformat** para preparar un dispositivo o archivo sin procesar para albergar la antememoria de proxy. Este mandato de formato debe utilizarse antes de que se especifique el dispositivo para utilizarlo con la antememoria de proxy.

La vía de acceso del dispositivo debe especificar el dispositivo original. Consulte la documentación del sistema de archivos para obtener información detallada sobre cómo acceder a los dispositivos originales. Podrá acceder a los ejemplos en la Parte 4, “Configuración de la antememoria y el servidor proxy”, en la página 73.

**Nota:** Los kernels Linux 2.2 no dan soporte a la colocación en antememoria de los dispositivos originales. En las plataformas Linux, sólo pueden utilizarse los archivos y la memoria para el almacenamiento de antememoria.

El tamaño mínimo de una antememoria de Caching Proxy es de 16392 KB, que equivale a 2049 bloques.

### Formato

```
htcformat dispositivo [-blocksize <tamaño de bloque>] [-blocks número de bloques]  
htcformat -file vía_acceso_archivo [-blocksize tamaño de bloque] -blocks número de bloques
```

### Parámetros

#### **-blocksize**

Este parámetro establece el tamaño de bloques en el soporte de almacenamiento del dispositivo de antememoria. El tamaño de bloque es en bytes. El valor por omisión es 8192 y debe utilizarse en todas las situaciones.

#### **-blocks**

Número de bloques que se van a crear en el dispositivo o el archivo. Al formatear un archivo, es necesario este argumento para especificar el tamaño de archivo. Este argumento también puede utilizarse para limitar la cantidad de un determinado dispositivo o partición que se va a utilizar para el almacenamiento de antememoria. Si no se especifica ningún argumento blocks, se crearán tantos bloques como quepan en la partición.

#### **-file**

Se formatea un archivo en lugar de un dispositivo de almacenamiento.

### Utilización

Adicionalmente, el sistema de colocación en antememoria divide los archivos y dispositivos de antememoria en contenedores para la indexación y la recogida de basura. El tamaño de los contenedores se establece en un determinado número de bloques y no se puede configurar. Para que la recogida de basura se ejecute, son necesarios dos contenedores como mínimo, siendo el tamaño mínimo de antememoria de 16392 KB.

El mandato **htcformat** rechaza una petición de formulario que genere un dispositivo de antememoria con menos de dos contenedores.

## Ejemplos

El ejemplo siguiente formatea una partición de disco llamada c0t0d0s0 en Solaris.

```
htcformat /dev/rdisk/c0t0d0s0
```

El ejemplo siguiente formatea una partición de disco llamada lv02 en AIX.

```
htcformat /dev/r1v02
```

El ejemplo siguiente formatea una partición de disco llamada d en Windows.

```
htcformat \\.\d:
```

El siguiente ejemplo formatea un archivo denominado filecache para que tenga un tamaño de 1 GB.

```
htcformat -file /opt/ibm/edge/cp/filecache -blocks 131072
```

---

## Mandato **ibmproxy**

### Propósito

Utilice el mandato **ibmproxy** para iniciar el servidor.

Puede establecer todos estos distintivos (excepto **-r**) mediante las directivas del archivo de configuración del servidor.

Es una práctica habitual crear un archivo denominado README que contenga las instrucciones y avisos que debe leer cualquier persona que acceda por primera vez al directorio. Por omisión, el mandato **ibmproxy** incorpora cualquier archivo README en la versión de hipertexto de un directorio. Las instrucciones del archivo README también pueden establecerse con la directiva de configuración DirReadme.

### Formato

`ibmproxy [-Distintivo [-Distintivo [-Distintivo..]]]`

### Parámetros

#### **-nobg**

Ejecuta el servidor como un proceso en primer plano, no como un proceso en segundo plano. El valor por omisión es la ejecución como un proceso en segundo plano.

#### **-nosnmp**

Desactiva el soporte SNMP.

#### **-p** *número-puerto*

Escucha en este número de puerto. El número de puerto por omisión es 80. Este distintivo sobrescribe la directiva Port especificada en el archivo de configuración. Para utilizar el valor por omisión o el valor especificado en el archivo de configuración, omita este distintivo.

#### **-r** *archivo-configuración*

Especifica el archivo que se va a utilizar como archivo de configuración. Debe utilizar este distintivo para iniciar el servidor con un archivo de configuración distinto del archivo de configuración por omisión. Esto le permitirá utilizar varios archivos de configuración.

#### **-restart**

Devuelve un servidor que está actualmente en ejecución. El mandato **ibmproxy** obtiene el número de proceso del servidor a partir de PidFile y se lo envía a la señal HangUP (HUP). A continuación, vuelve a cargar los archivos de configuración y a abrir los archivos de anotaciones cronológicas. Para evitar que se dañen los datos, no ejecute dos instancias del servidor simultáneamente mediante los mismos PidFile, archivos de anotaciones cronológicas y antememoria de proxy.

Como el daemon **http** debe leer el archivo de configuración que el servidor está utilizando actualmente para acceder al PidFile, debe especificar el mismo archivo de configuración durante el reinicio. Si ha utilizado el distintivo **-r** y un archivo de configuración específico al iniciar el servidor, debe especificar este distintivo y el mismo archivo con **-restart**.

#### **-snmp**

Activa el soporte SNMP.



### **-unload**

En Linux, elimina las normas de cortafuegos asociadas.

Las opciones del manejo de señales también existen en las plataformas Linux y UNIX. En las plataformas Linux y UNIX, están disponibles las siguientes opciones.

### **SIGTERM**

El mandato **ibmproxy** se detiene y sale al completarse. Puede utilizar SIGKILL o CANCEL para terminar inmediatamente.

### **SIGHUP**

Si se ejecuta, el mandato **ibmproxy** se reinicia, vuelve a cargar el archivo de configuración y continúa el proceso.

## **Ejemplos**

- Para iniciar el servidor en el puerto 8080 mediante el archivo de configuración /usr/etc/ibmproxy.conf en lugar del archivo de configuración por omisión, especifique:

```
ibmproxy -p 8080 -r /usr/etc/ibmproxy.conf
```

- En AIX, para iniciar un servidor con el archivo de configuración por omisión mediante System Resource Controller, especifique:

```
startsrc -s ibmproxy
```

Si el archivo de configuración por omisión no existe, el mandato **ibmproxy** exporta el árbol de directorios /Public. Este árbol contiene enlaces con otros árboles de directorios.



---

## Apéndice B. Directivas del archivo de configuración

Este apéndice describe las directivas que se incluyen en el archivo de configuración `ibmproxy.conf`.

- **En los sistemas Linux y UNIX.** Estas directivas están ubicadas en el archivo de configuración `ibmproxy.conf` del directorio `/etc/`.
- **En los sistemas Windows.** Estas directivas están ubicadas en `C:\Archivos de programa\IBM\edge\cp\` generalmente.

Utilice esta información como referencia si configura el servidor mediante la edición del archivo `ibmproxy.conf`. Si utiliza los formularios de Configuración y Administración, es necesario que consulte este capítulo.

Las directivas se enumeran por orden alfabético.

---

### Directivas que no se modifican durante el reinicio

Algunas directivas no se renuevan cuando el servidor se reinicia. Si las siguientes directivas se modifican mientras se está ejecutando el servidor, debe detener y reiniciar el servidor manualmente. (Consulte el Capítulo 5, “Inicio y detención de Caching Proxy”, en la página 15.)

*Tabla 6. Directivas que no se renuevan durante el reinicio*

| Grupo de directivas              | Directivas                                                      |
|----------------------------------|-----------------------------------------------------------------|
| CGI                              | DisinheritEnv, InheritEnv                                       |
| Colocación en antememoria        | Caching                                                         |
| Registro cronológico             | AccessLog, CacheAccessLog, ErrorLog, ProxyAccessLog, ServerRoot |
| Acceso a red                     | BindSpecific, Hostname, ListenBacklog, Port                     |
| Rendimiento                      | MaxActiveThreads                                                |
| RTSP                             | Todas las directivas RTSP                                       |
| SSL                              | Todas las directivas SSL                                        |
| Control de procesos Linux y UNIX | GroupId, UserId                                                 |
| Varios                           | TransparentProxy                                                |

---

### Visión general de las directivas

Este apéndice proporciona la siguiente información sobre todas las directivas:

- Una cabecera con el nombre y una breve descripción de la directiva
- Instrucciones de uso
- El formato de la directiva, que sigue la sintaxis general:  
*NombreDirectiva valor*
- Cuando sea apropiado, un ejemplo del posible valor de la directiva en el archivo de configuración

**Nota:** Los ejemplos de las directivas con vías de acceso específicas para Windows a veces contienen *raíz\_servidor*, que es el directorio raíz del servidor seleccionado durante la instalación.

- El valor o valores por omisión de la directiva.

Estos son los valores originales codificados en el archivo de configuración por omisión. Modifique sólo las partes del archivo de configuración que desee que sean distintas de los valores por omisión. Una directiva que no tiene un valor por omisión codificado inicialmente aparece en el archivo precedida por un marcador de comentario (#). Si desea especificar un valor para la directiva, elimine el marcador de comentario y añada el valor a la línea del archivo de configuración.

## Valores aceptables

La siguiente lista incluye los valores que se aceptan en el archivo de configuración:

- En la información de referencia de algunas directivas, la parte *valor* contiene las plantillas de peticiones, los nombres de vía de acceso y los nombres de sistema principal. Excepto cuando se indique lo contrario, puede utilizar el carácter de asterisco (\*) en las plantillas. Para hacer coincidir una plantilla, se puede sustituir un asterisco por cualquier serie de caracteres o carácter único.
- Las directivas de configuración que le permiten especificar una serie positiva aceptan estos valores:
  - Yes
  - On
  - OK
  - Enable
- Las directivas de configuración que le permiten especificar una serie negativa aceptan estos valores:
  - No
  - Off
  - None
  - Disable
- Las directivas de configuración que le permiten especificar un periodo de tiempo aceptan cualquier combinación de los siguientes valores:
  - *hh*: horas
  - *hh:mm*: horas y minutos
  - *hh:mm:ss*: horas, minutos y segundos
  - *n years*: número de años de 365 días
  - *n months*: número de meses de 30 días
  - *n weeks*: número de semanas de 7 días
  - *n days*: número de días de 24 horas
  - *n hours*: número de horas de 60 minutos
  - *n minutes*: número de minutos de 60 segundos
  - *n seconds*: número de segundos
  - *n fortnights*: número de intervalos de 14 díasTodas las entradas se convierten a segundos y éstos se suman.
- Los caracteres en blanco no se permiten en un nombre de archivo especificado en el archivo de configuración. Los espacios en blanco son tratados como delimitadores

---

## Sintaxis de los registros del archivo de configuración

Al editar el archivo de configuración, recuerde los siguientes requisitos:

- Todas las directivas deben empezar en una línea nueva.
- Los valores se separan mediante uno o más espacios en blanco. No se realiza ninguna distinción entre el carácter de espacio y el carácter de tabulador.
- El inicio de un comentario se indica mediante el símbolo #. Todos los caracteres que van desde el símbolo # hasta el final de la línea se ignoran.
- Si es necesario especificar un símbolo de almohadilla o un espacio en blanco para una directiva, utilice el carácter de barra inclinada invertida (\) como carácter de escape delante de él. Un carácter de escape indica que el siguiente carácter va a interpretarse como un carácter en lugar de como un mandato; por ejemplo, si aparece \# en una línea, el servidor lo interpreta como un símbolo #, no como el principio de un comentario, y continúa leyendo los caracteres. Si aparece el carácter \ en una línea, el servidor lo interpreta como un espacio en blanco, no como un delimitador de valor, y continúa leyendo los caracteres para crear el valor.

---

## Directivas de Caching Proxy

A continuación aparecen las directivas de Caching Proxy.

### AcceptAnything: servir todos los archivos

Utilice esta directiva para servir los archivos al cliente incluso si el tipo MIME del archivo no coincide con una cabecera ACCEPT: enviada por el cliente. Si esta directiva se establece en OFF, no se visualizan los archivos cuyos tipos MIME son distintos de los tipos que el cliente puede aceptar. En su lugar se visualiza una página de error.

#### Formato

AcceptAnything {on | off}

#### Ejemplo

AcceptAnything off

#### Valor por omisión

AcceptAnything on

### AccessLog: nombrar la vía de acceso del archivo de anotaciones cronológicas de acceso

Utilice esta directiva para especificar el directorio y el archivo donde desea que el servidor anote cronológicamente las estadísticas de acceso. Por ejemplo, el servidor escribe una entrada en estas anotaciones cronológicas cada vez que un cliente envía al servidor una petición de datos almacenados en el servidor local. Generalmente, estas entradas sólo incluyen las peticiones del cliente de configuración o accesos cuando la máquina de Caching Proxy se utiliza como un servidor de origen. Estas anotaciones cronológicas no contienen la información de acceso a la antememoria o al proxy.

Utilice la directiva NoLog para especificar los clientes cuyas peticiones no desea anotar cronológicamente. Para obtener una descripción de la directiva NoLog, consulte “NoLog: suprimir las entradas de anotaciones cronológicas de los sistemas principales o dominios específicos que coinciden con una plantilla” en la página 248.

El servidor inicia un nuevo archivo de anotaciones cronológicas cada día a las doce de la noche si se está ejecutando. De lo contrario, el servidor inicia un nuevo archivo de anotaciones cronológicas la primera vez que se inicia en un día cualquiera. Al crear el archivo, el servidor utiliza el nombre de archivo que especifique y añadirá un sufijo de fecha. El sufijo de fecha aparece en el formato *Mmmddaaaa*, donde *Mmm* son las tres primeras letras del mes, *dd* es el día del mes y *aaaa* es el año.

**Nota:** Si cambia los valores por omisión del servidor para el ID de usuario, el ID de grupo o las vías de acceso de directorios de anotaciones cronológicas, cree los nuevos directorios y actualice los permisos y propiedad de éstos. Para permitir que el servidor escriba la información en un directorio de anotaciones cronológicas definidas por el usuario, establezca el permiso para ese directorio como 755 y el ID de usuario del servidor definido por el usuario como el propietario. Por ejemplo, si cambia el ID de usuario del servidor del valor por omisión a *jdoe* y el directorio de anotaciones cronológicas por omisión a *server\_root/account*, el directorio *server\_root/account* debe tener el permiso 755 y ser propiedad de *jdoe*.

Se recomienda eliminar los archivos de anotaciones cronológicas antiguos ya que pueden utilizar una cantidad significativa de espacio de la unidad de disco duro.

### Formato

`AccessLog /vía_acceso_directorio/nombre_archivo_anotaciones_cronológicas`

### Ejemplo

`AccessLog /logs/accesslog`

### Valores por omisión

- **En los sistemas Linux y UNIX:** `AccessLog /opt/ibm/edge/cp/server_root/logs/local`
- **En los sistemas Windows:** `AccessLog unidad:\Archivos de programa\IBM\edge\cp\logs\local`

## AccessLogExcludeMethod: suprimir las entradas de anotaciones cronológicas de los archivos y directorios solicitados por un método específico

Utilice esta directiva para evitar el registro cronológico de peticiones realizadas por un determinado método para acceder a los archivos o directorios. Por ejemplo, es posible que no desee anotar cronológicamente las peticiones DELETE de los archivos y directorios.

Pueden darse varias apariciones de esta directiva en el archivo de configuración. Asimismo, puede colocar varios métodos en la misma directiva si los separa por uno o más espacios.

### Formato

`AccessLogExcludeMethod método`  
`[ ...]`

### Ejemplos

`AccessLogExcludeMethod GET`  
`AccessLogExcludeMethod PUT`  
`AccessLogExcludeMethod POST`  
`AccessLogExcludeMethod DELETE`  
`AccessLogExcludeMethod GET PUT`

### Valor por omisión

Ninguno. El servidor incluye en las anotaciones cronológicas de acceso los archivos y directorios solicitados por todos los tipos de métodos.

## AccessLogExcludeMimeType: suprimir las entradas de anotaciones cronológicas de acceso al proxy para tipos MIME específicos

Utilice esta directiva para especificar que no desea registrar en el proxy las peticiones de anotaciones cronológicas de acceso para acceder a los directorios o archivos de un tipo MIME especificado. (Ejemplos de tipos MIME son text/html, image/gif e image/jpeg.) Por ejemplo, es posible que no desee anotar cronológicamente las peticiones de acceso de las imágenes GIF.

Pueden darse varias apariciones de esta directiva en el archivo de configuración. Asimismo, puede colocar varios tipos MIME en la misma directiva si los separa por uno o más espacios.

**Nota:** Esta directiva sólo afecta a las anotaciones cronológicas de acceso al proxy. No es posible filtrar las anotaciones cronológicas que enumeren estos objetos en antememoria a partir del tipo MIME. Utilice AccessLogExcludeURL para realizar esta acción.

### Formato

AccessLogExcludeMimeType *tipo\_MIME* [...]

### Ejemplo

```
AccessLogExcludeMimeType image/gif
AccessLogExcludeMimeType text/html
AccessLogExcludeMimeType image/gif text/html
```

### Valor por omisión

Ninguno. Las anotaciones cronológicas de acceso incluyen las peticiones al servidor de archivos y directorios de todos los tipos MIME.

## AccessLogExcludeReturnCode: suprimir las entradas de anotaciones cronológicas de códigos de retorno específicos

Utilice esta directiva para especificar que no desea anotar cronológicamente las peticiones de acceso que se incluyen dentro de un rango especificado de números de código de error. Estos números de código de error son códigos de estado del servidor proxy. No puede especificar los códigos individuales. La especificación de 300 indica que desea excluir las peticiones de acceso con códigos de retorno de redirección (301, 302, 303 y 304).

Pueden darse varias apariciones de esta directiva en el archivo de configuración. Asimismo, puede colocar varios códigos de retorno en la misma directiva si los separa por uno o más espacios.

### Formato

AccessLogExcludeReturnCode *rango*

### Ejemplo

```
AccessLogExcludeReturnCode 300
```

### Valor por omisión

Ninguno. Las anotaciones cronológicas de acceso incluyen todas las peticiones al servidor, independientemente del código.

## AccessLogExcludeURL: suprimir las entradas de anotaciones cronológicas de archivos o directorios específicos

Utilice esta directiva para especificar que no desea anotar cronológicamente las peticiones de acceso a los archivos o directorios específicos que coincidan con una plantilla de URL especificada. Por ejemplo, es posible que no desee anotar cronológicamente las peticiones de acceso de los archivos GIF o las peticiones de acceso a un determinado archivo o directorio del servidor.

Pueden darse varias apariciones de esta directiva en el archivo de configuración. Asimismo, puede colocar varias entradas de la misma directiva si las separa por uno o más espacios.

### Formato

```
AccessLogExcludeURL archivo_o_tipo [...]
```

### Ejemplos

```
AccessLogExcludeURL *.gif
AccessLogExcludeURL /Freebies/*
AccessLogExcludeURL *.gif /Freebies/*
```

### Valor por omisión

Ninguno. El servidor anota cronológicamente las peticiones de acceso a todos los archivos y directorios.

## AccessLogExcludeUserAgent: suprimir las entradas de anotaciones cronológicas de navegadores específicos

Utilice esta directiva para especificar que no desea anotar cronológicamente las peticiones de acceso realizadas por agentes de usuario específicos (por ejemplo, Internet Explorer 5.0).

Pueden darse varias apariciones de esta directiva en el archivo de configuración. Asimismo, puede colocar varias entradas de la misma directiva si las separa por uno o más espacios.

### Formato

```
AccessLogExcludeUserAgent agente_usuario [...]
```

### Ejemplo

```
AccessLogExcludeUserAgent *Mozilla/2.0
AccessLogExcludeUserAgent *MSIE 5*
```

### Valor por omisión

Por omisión, el archivo `ibmproxy.conf` contiene las siguientes definiciones de la directiva `AccessLogExcludeUserAgent`:

```
AccessLogExcludeUserAgent IBM_Network_Dispatcher_HTTP_Advisor
AccessLogExcludeUserAgent IBM_Network_Dispatcher_WTE_Advisor
```

Los agentes de usuario enumerados anteriormente son aquellos definidos para ciertos asesores de Load Balancer que generalmente trabajan delante del servidor de Caching Proxy. Para mejorar el rendimiento minimizando el número de escrituras en las anotaciones cronológicas, estos agentes de usuario no se anotan



cronológicamente. Por omisión, el servidor anota cronológicamente las peticiones de acceso realizadas por todos los agentes de usuario.

## **AddBlankIcon: especificar el URL del icono utilizado para alinear las cabeceras de los listados de directorios**

Utilice esta directiva para especificar un icono que alinee las cabeceras o listados de directorios que se devuelven cuando el servidor actúa como proxy para las peticiones FTP. Los iconos aparecen junto a los archivos asociados para ayudar a los usuarios a diferenciar los archivos.

El icono puede ser un icono en blanco u otro icono que se especifique para que aparezca en las cabeceras de los listados de directorios. Para una alineación adecuada, el icono que se utilice debe tener el mismo tamaño que los demás iconos que se están utilizando en los listados de directorios.

### **Formato**

`AddBlankIcon URL_icono texto_alternativo`

*URL\_icono*

Especifica la última parte del URL del icono. El servidor añade este valor al directorio `/icons/` para crear la petición URL completa. Si la petición es para un archivo local, el servidor traduce la petición mediante las directivas de correlación. Para recuperar el icono, las directivas de correlación deben permitir que se pase la petición.

Si está utilizando el servidor como proxy, la petición completa debe ser un URL plenamente cualificado que señale al servidor.

*texto\_alternativo*

Especifica el texto alternativo que se va a utilizar con el icono si el navegador que lo solicita no muestra ningún gráfico.

### **Ejemplo**

`AddBlankIcon logo.gif logo`

### **Valores por omisión**

- **Linux y UNIX:** `AddBlankIcon blank.m.pm.gif`
- **Windows:** `AddBlankIcon blank.gif`

El valor por omisión no especifica el texto alternativo porque el icono está en blanco.

## **AddDirIcon: especificar el URL de icono de los directorios en los listados de directorios**

Utilice esta directiva para especificar un icono que represente un directorio en un listado de directorios.

### **Formato**

`AddDirIcon URL_icono texto_alternativo`

*URL\_icono*

Especifica la última parte del URL del icono. El servidor añade este valor al directorio `/icons/` para crear la petición URL completa. Si la petición es para

un archivo local, el servidor traduce la petición mediante las directivas de correlación. Para recuperar el icono, las directivas de correlación deben permitir que se pase la petición.

Si está utilizando el servidor como proxy, la petición completa debe ser un URL plenamente cualificado que señale al servidor. Debe correlacionar el URL con un archivo local y asegurarse de que las directivas de correlación permitan que se pase el URL.

#### *texto\_alternativo*

Especifica el texto alternativo que se va a utilizar con el icono si el navegador que lo solicita no muestra ningún gráfico.

### **Ejemplo**

```
AddDirIcon direct.gif DIR
```

### **Valores por omisión**

- **Linux y UNIX:** AddDirIcon dir.m.pm.gif DIR
- **Windows:** AddDirIcon dir.gif DIR

## **AddEncoding: especificar la codificación del contenido MIME de los archivos con sufijos determinados**

Utilice esta directiva para enlazar archivos con un determinado sufijo a un tipo de codificación MIME. Esta directiva se utiliza raras veces.

### **Formato**

```
AddEncoding .extensión codificación
```

#### *.extensión*

Especifica el patrón de sufijo de archivo.

#### *codificación*

Especifica el tipo de codificación MIME que desea enlazar con los archivos que coinciden con el patrón de sufijo correspondiente.

### **Ejemplo**

```
AddEncoding .qp quoted_printable
```

### **Valor por omisión**

```
AddEncoding .Z x-compress
```

## **AddIcon: enlazar un icono con un tipo de contenido o de codificación MIME**

Utilice esta directiva para especificar los iconos que representen a los archivos con un tipo específico de codificación o de contenido MIME. El servidor utiliza los iconos en los listados de directorios, incluidos los listados de directorios FTP.

### **Formato**

```
AddIcon URL_icono texto_alternativo plantilla_tipo_MIME
```

#### *URL\_icono*

Especifica la última parte del URL del icono. El servidor añade este valor al directorio /icons/ para crear la petición URL completa. Si la petición es para un archivo local, el servidor traduce la petición mediante las directivas de correlación. Para recuperar el icono, las directivas de correlación deben permitir que se pase la petición.

Si está utilizando el servidor como proxy, la petición completa debe ser un URL plenamente cualificado que señale al servidor. Debe correlacionar el URL con un archivo local y asegurarse de que las directivas de correlación permitan que se pase el URL.

#### *texto\_alternativo*

Especifica el texto alternativo que se va a utilizar con el icono si el navegador que lo solicita no muestra ningún gráfico.

#### *plantilla\_tipo*

Especifica una plantilla de tipo de codificación o de tipo de contenido MIME. Las plantillas de tipo de contenido siempre contienen una barra inclinada (/). Las plantillas de tipo de codificación nunca tienen una barra inclinada.

### Ejemplo

```
AddIcon    video_file.m.pm.gif    MOV    video/*
```

### Valores por omisión

Numerosos valores por omisión se establecen para la directiva AddIcon en el archivo de configuración ibmproxy.conf.

## AddParentIcon: especificar el URL del icono que representa el directorio padre en los listados de directorios

Utilice esta directiva para especificar un icono que represente un directorio padre en los listados de directorios.

### Formato

```
AddParentIcon    URL_icono    texto_alternativo
```

#### *URL\_icono*

Especifica la última parte del URL del icono. El servidor añade este valor al directorio /icons/ para crear la petición URL completa. Si la petición es para un archivo local, el servidor traduce la petición mediante las directivas de correlación. Para recuperar el icono, las directivas de correlación deben permitir que se pase la petición.

Si está utilizando el servidor como proxy, la petición completa debe ser un URL plenamente cualificado que señale al servidor. Debe correlacionar el URL con un archivo local y asegurarse de que las directivas de correlación permitan que se pase el URL.

#### *texto\_alternativo*

Especifica el texto alternativo que se va a utilizar con el icono si el navegador que lo solicita no muestra ningún gráfico.

### Ejemplo

```
AddParentIcon    parent.gif    UP
```

### Valor por omisión

```
AddParentIcon    dir-up.gif    UP
```

## AddType: especificar el tipo de datos de los archivos con sufijos determinados

Utilice esta directiva para enlazar archivos con un determinado sufijo a un tipo y subtipo MIME. Pueden darse varias apariciones de esta directiva en el archivo de configuración. El servidor proporciona los valores por omisión para los sufijos utilizados con mayor frecuencia.

## Formato

AddType *.extensión tipo/subtipo codificación[calidad[ conjunto\_de\_caracteres]]*

### *.extensión*

El patrón de sufijo de archivo. Sólo puede utilizar el carácter comodín (\*) en los dos patrones de sufijo especiales siguientes:

- \*.\*** Coincide con todos los nombres de archivo que contienen un carácter de punto (.) y no coinciden con ninguna otra norma.
- \*** Coincide con todos los nombres de archivo que no contienen un carácter de punto (.) y no coinciden con ninguna otra norma.

### *tipo/subtipo*

El tipo y subtipo MIME que desee enlazar con los archivos que coincidan con el correspondiente patrón de sufijo.

### *codificación*

La codificación de contenido MIME a la que se han convertido los datos. La codificación también la utiliza un servidor proxy FTP para determinar si el archivo se recupera en modalidad binaria. En la mayoría de los casos, la codificación adecuada es 7bit, 8bit o binary y se determina del siguiente modo:

- 7bit** Todos los datos se representan como líneas cortas (de menos de 1000 caracteres) de datos 8859-1 ASCII. Los archivos de código de origen o de texto plano generalmente pertenecen a esta categoría. Son excepciones los archivos que contengan caracteres de dibujos de líneas o acentuados.
- 8bit** Los datos se representan mediante líneas cortas, pero pueden contener caracteres con el conjunto de bits alto, por ejemplo, caracteres de dibujos de líneas o acentuados. Los archivos de texto y PostScript de los sitios europeos normalmente pertenecen a esta categoría.
- binary** Esta codificación puede utilizarse con todos los tipos de datos. Los datos no sólo pueden contener caracteres que no sean ASCII sino también líneas largas (de más de 1000 caracteres). Casi todos los archivos de tipo image/\*, audio/\* y video/\* pertenecen a esta categoría, del mismo modo que lo hacen los archivos de datos binarios de tipo application/\*.

Cualquier otro valor de codificación recibe el mismo tratamiento que binary y se pasa en las cabeceras MIME como una cabecera MIME de codificación de contenido. Las especificaciones 7bit y 8bit no se envían en las cabeceras MIME.

### *calidad*

Especifica un indicador opcional de valor relativo (en una escala de 0 a 1) para el tipo de contenido. El valor de calidad se utiliza si varias representaciones de un archivo coinciden con una petición. El servidor selecciona el archivo que se asocia con el valor de calidad más alto. Por ejemplo, si se solicita el archivo internet.ps y el servidor tiene establecidas las siguientes directivas AddType, el servidor utiliza la línea application/postscript porque el número de calidad es más alto.

```
AddType .ps application/postscript 8bit 1.0
AddType *.* application/binary binary 0.3
```

### *conjunto\_de\_caracteres*

Indicador opcional del conjunto de caracteres que desea asociar con los archivos de texto. Para aquellos archivos a los que se asigna un conjunto de

caracteres, el servidor indica a los navegadores de cliente qué conjunto de caracteres debe utilizarse cuando se visualiza el archivo. Si establece un valor para el campo *conjunto\_de\_caracteres*, también debe incluir un valor para el campo *calidad*.

### Ejemplo

```
AddType .bin application/octet-stream binary 0.8
```

### Valores por omisión

Los numerosos valores por omisión de la directiva AddType se encuentran en el archivo de configuración (ibmproxy.conf).

## AddUnknownIcon: especificar el URL de icono de los tipos de archivo desconocidos en los listados de directorios

Utilice esta directiva para especificar un icono que represente los archivos con un tipo de archivo desconocido en un listado de directorios.

### Formato

```
AddUnknownIcon URL_icono texto_alternativo
```

*URL\_icono*

Especifica la última parte del URL del icono. El servidor añade este valor a /icons/ para crear la petición URL completa. Si la petición es para un archivo local, el servidor traduce la petición mediante las directivas de correlación. Para recuperar el icono, las directivas de correlación deben permitir que se pase la petición.

Si está utilizando el servidor como proxy, la petición completa debe ser un URL plenamente cualificado que señale al servidor. Debe correlacionar el URL con un archivo local y asegurarse de que las directivas de correlación permitan que se pase el URL.

*texto\_alternativo*

Especifica el texto alternativo que se va a utilizar con el icono si el navegador que lo solicita no muestra ningún gráfico.

### Ejemplo

```
AddUnknownIcon saywhat.gif unknown
```

### Valores por omisión

- **Linux y UNIX:** AddUnknownIcon unknown.gif ???
- **Windows:** AddUnknownIcon unknown.gif ???

## AdminPort: especifica el puerto para solicitar las páginas administrativas o formularios

Utilice esta directiva para especificar un puerto que puedan utilizar los administradores para acceder a las páginas de estado del servidor o los formularios de configuración. Las peticiones dirigidas a este puerto no se colocan en la cola con las demás peticiones de entrada en el puerto o puertos estándar que se definen con la directiva Port. No obstante, las peticiones de AdminPort observan las mismas normas de correlaciones de peticiones y de control de accesos normales que, por ejemplo, Exec y Protect.

**Nota:** El puerto de administración *no* debe coincidir con el puerto o puertos estándar definidos con la directiva Port.

## Formato

AdminPort *número\_puerto*

## Ejemplo

AdminPort 2001

## Valor por omisión

AdminPort 8008

## AggressiveCaching: especificar la colocación en antememoria de los archivos que no se colocan en antememoria

Utilice esta directiva para especificar si los archivos devueltos por el servidor de origen y marcados como que no se colocan en antememoria se van a colocar en antememoria de todos modos. Los archivos que no se pueden colocar en antememoria que se colocan en antememoria de acuerdo con esta directiva se marcan como deben revalidarse. Siempre que se solicita el archivo, el servidor proxy envía una petición If-Modified-Since al servidor de origen para volver a validar la respuesta antes de que se sirva la respuesta desde la antememoria. En la actualidad, los únicos archivos que no se colocan en antememoria afectados por esta directiva son respuestas del servidor de origen que contienen una cabecera cache-control: no-cache. Esta directiva puede especificarse varias veces.

## Formato

AggressiveCaching *patrón\_url*

## Ejemplos

AggressiveCaching http://www.hosta.com/\*

AggressiveCaching http://www.hostb.com/\*

Para que sea compatible con versiones anteriores, la sintaxis anterior de esta directiva ( AggressiveCaching {on | off}) se trata del siguiente modo:

AggressiveCaching on se trata como AggressiveCaching \* .

AggressiveCaching off se ignora.

**Nota:** Si se especifican AggressiveCaching off y AggressiveCaching *patrón\_url*, AggressiveCaching off se ignora y se muestra un mensaje de aviso.

## Valor por omisión

Ninguno

## AlwaysWelcome: especificar si desea buscar los archivos de bienvenida en el directorio solicitado

Para las peticiones que contienen un nombre de directorio pero carecen de un nombre de archivo, la directiva AlwaysWelcome controla si el servidor busca en el directorio un archivo de bienvenida que se devuelva. Por omisión, AlwaysWelcome se establece en un valor de on. Esto significa que el servidor siempre busca en el directorio solicitado un archivo que coincida con un nombre especificado en una directiva Welcome. Si se encuentra una coincidencia, el archivo se devuelve al solicitante. Si el servidor encuentra más de una coincidencia entre los archivos de un directorio y los nombres de archivo de las directivas Welcome, el orden de las directivas Welcome determina qué archivo se devuelve. El servidor utiliza la directiva Welcome más cercana a la parte superior del archivo de configuración.

### Formato

AlwaysWelcome on | off

### Valor por omisión

AlwaysWelcome on

### Directivas relacionadas

- “Welcome: especificar los nombres de los archivos de bienvenida” en la página 295

## appendCRLFtoPost: añadir CRLF a las peticiones POST

Utilice esta directiva para especificar los URL para los que Caching Proxy añade los caracteres de retorno de carro y de salto de línea al final del cuerpo de una petición POST. Esta directiva se puede especificar varias veces.

**Nota:** Especifique esta directiva sólo para los URL que hayan tenido un problema durante el proceso de las peticiones POST.

### Formato

appendCRLFtoPost *patrón\_url*

### Ejemplo

appendCRLFtoPost http://www.hosta.com/

### Valor por omisión

Ninguno

## ArrayName: nombrar la matriz de antememoria remota

Utilice esta directiva para especificar la matriz de antememoria remota que van a compartir los servidores.

**Nota:** Al configurar una matriz, configure la directiva Hostname en todos los miembros de la matriz de modo idéntico.

### Formato

ArrayName *nombre\_matriz*

### Valor por omisión

Ninguno

## Authentication: personalizar el paso de autenticación

Utilice esta directiva para especificar una función de aplicación personalizada a la que desee que llame el servidor durante el paso de autenticación del proceso de peticiones del servidor. Este código se ejecuta de acuerdo con el esquema de autenticación. Sólo se da soporte a la autenticación BASIC.

**Nota:** La autenticación forma parte del proceso de autorización; sólo ocurre cuando es necesaria la autorización.

### Formato

Authentication *tipo /vía\_acceso/archivo:nombre\_función*

*tipo*

Especifica un esquema de autenticación que determina adicionalmente si se llama a la función de aplicación. Tanto un asterisco (\*) como BASIC son valores aceptados.

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre que se da a la función de aplicación del programa.

### **Ejemplo**

Authentication BASIC /ics/api/bin/icsextpgm.so:basic\_authentication

### **Valor por omisión**

Ninguno

## **Authorization: personalizar el paso de autorización**

Utilice esta directiva para especificar una función de aplicación personalizada a la que llama el servidor durante el paso de autorización del proceso de peticiones del servidor. Este código verifica que el objeto solicitado puede servirse al cliente.

### **Formato**

Authorization *plantilla\_petición* /*vía\_acceso/archivo:nombre\_función*

*plantilla\_petición*

Especifica una plantilla para las peticiones que determinan adicionalmente si se llama a la función de aplicación. La especificación puede incluir el protocolo, el dominio y el sistema principal; puede estar precedida por un carácter de barra inclinada (/), y puede utilizar un asterisco (\*) como carácter comodín. Por ejemplo, /front\_page.html, http://www.ics.raleigh.ibm.com, /pub\*, /\* y \* son todas válidas. La plantilla de petición debe empezar en el directorio raíz de documentos (/) al utilizar Caching Proxy como proxy de retorno.

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre que se da a la función de aplicación del programa.

### **Ejemplo**

Authorization /index.html /api/bin/icsextpgm.so:auth\_url

### **Valor por omisión**

Ninguno

## **AutoCacheRefresh: especificar si se desea utilizar la renovación de antememoria**

Utilice esta directiva para activar y desactivar la renovación de antememoria. Si la renovación está activada, el contenido de antememoria se renueva automáticamente. Si la renovación está desactivada, no se invoca el agente de antememoria y todos sus valores se ignoran. Si está iniciando el agente de antememoria mediante otro método, por ejemplo, utilizando un trabajo **cron** en los sistemas Linux y UNIX, establezca esta directiva en off.



### Formato

AutoCacheRefresh {on | off}

### Valor por omisión

AutoCacheRefresh On

## BindSpecific: especificar si el servidor se enlaza a una dirección IP o a todas

Utilice esta directiva en un sistema multiconexión para especificar si el servidor escucha en una única dirección de red. Si establece el valor en On, el servidor se enlaza con la dirección IP especificada en la directiva Hostname, en lugar de enlazarse con todas las direcciones IP locales.

Si no se especifica esta directiva, el servidor se enlaza con Hostname por omisión.

Si modifica esta directiva, debe detener y reiniciar el servidor manualmente. El servidor no realiza el cambio si sólo lo reinicia. (Consulte el Capítulo 5, “Inicio y detención de Caching Proxy”, en la página 15.)

### Formato

BindSpecific {on | off} [OutgoingSrcIp *dir\_ip* | ]

[OutgoingSrcIp *dir\_ip* | ]

Las opciones OutgoingSrcIp permiten a Caching Proxy utilizar una dirección IP de origen específica al realizar conexiones de salida. Es de gran utilidad para los valores de Caching Proxy de DMZ, y cuando las normas especiales de cortafuegos así lo requieren.

### Valor por omisión

BindSpecific Off

## BlockSize: especificar el tamaño de bloques de la antememoria

Esta directiva especifica el tamaño, en bytes, de los bloques del soporte del dispositivo de colocación en antememoria. Por omisión, es valor es 8192. Como es el único valor soportado, no cambie este valor. Para obtener más información, consulte el apartado de referencia de “Mandato htcformat” en la página 172.

### Formato

BlockSize *tamaño*

### Valor por omisión

Por omisión, no existe un valor para BlockSize en el archivo de configuración. (El valor por omisión es 8192.)

## CacheAccessLog: especificar la vía de acceso de los archivos de anotaciones cronológicas de acceso a la antememoria

Utilice esta directiva para especificar la vía de acceso y el nombre de archivo donde desea que el servidor almacene las anotaciones cronológicas de acceso a la antememoria de proxy. Esta directiva es válida sólo si el servidor se ejecuta como un proxy. Consulte “CacheRefreshTime: especificar cuándo se desea iniciar el agente de antememoria” en la página 201 para obtener más información.

Para habilitar el registro cronológico de las peticiones dirigidas a la antememoria de proxy, la directiva Caching debe establecerse en ON, a la vez que deben establecerse valores para las directivas CacheMemory y cacheAccessLog. Opcionalmente, se pueden definir uno o más dispositivos de antememoria mediante la directiva CacheDev.

El valor de CacheAccessLog puede ser una vía de acceso absoluta o una vía de acceso relativa a ServerRoot. (Se muestra un ejemplo de cada una de ellas.)

### Formato

CacheAccessLog *vía\_acceso/archivo*

### Ejemplos

CacheAccessLog /absolute/path/logfile

CacheAccessLog /logs/logfile

### Valores por omisión

- **Sistemas Linux y UNIX:** CacheAccessLog /opt/ibm/edge/cp/server\_root/logs/cache
- **Sistemas Windows:** CacheAccessLog *unidad:*\Archivos de programa\IBM\edge\cp\logs\cache

## CacheAlgorithm: especificar el algoritmo de antememoria

Utilice esta directiva para especificar el algoritmo de antememoria que el servidor utiliza durante la recogida de basura.

### Formato

CacheAlgorithm {bandwidth | responsetime | blend}

#### bandwidth

Intenta maximizar el ahorro de ancho de banda de red.

#### responsetime

Intenta minimizar el tiempo de respuesta del usuario.

#### blend

Utiliza una combinación equilibrada de bandwidth y responsetime .

### Valor por omisión

CacheAlgorithm bandwidth

## CacheByIncomingUrl: especificar la base para generar los nombres de archivo de antememoria

Utilice esta directiva para especificar si los nombres de archivo de antememoria generados están basados en el URL de entrada de la petición.

Si se establece esta directiva en on, los nombres de archivo de antememoria se generan basándose en el URL de entrada. Si esta directiva se establece en off, el URL de entrada se pasa primero a través de todos los plug-ins aplicables de traducción de nombres, normas MAP y PROXY, y el nombre de archivo de antememoria generado se basa en el URL resultante.

**Nota:** Al definir los filtros de antememoria en un escenario de proxy de retorno para los filtros de antememoria basados en URL, utilice un formato que

empiece por un directorio raíz de documentos de / (barra inclinada). Por ejemplo, /test/index.html. El formato *no* debería incluir un protocolo, por ejemplo, *http://*.

### Formato

CacheByIncomingUrl {on | off}

### Valor por omisión

CacheByIncomingURL off

## CacheClean: especificar el periodo de tiempo que se deben mantener los archivos en antememoria

Utilice esta directiva para especificar cuánto tiempo desea que el servidor mantenga los archivos en antememoria. Cuando se ejecuta la recogida de basura, el servidor suprime los archivos en antememoria que han excedido este tiempo, independientemente de la fecha de caducidad de los archivos. Siempre que se solicite un archivo que ha estado en la antememoria durante más tiempo que el especificado, el servidor volverá a validar el archivo para asegurarse de que es válido antes de servirlo.

### Formato

CacheClean *especificación\_de\_tiempo*

### Ejemplo

CacheClean 2 weeks

### Valor por omisión

CacheClean 1 month

## CacheDefaultExpiry: especificar el tiempo de caducidad por omisión de los archivos

Utilice esta directiva para establecer un tiempo de caducidad por omisión para los archivos para los que el servidor no ha proporcionado una cabecera Expires ni Last-Modified. Especifique una plantilla de URL y el tiempo de caducidad para los archivos que tengan los URL que coincidan con la plantilla. Se pueden incluir varias apariciones de esta directiva en el archivo de configuración. Incluya una directiva separada para cada plantilla. La plantilla de URL debe incluir el protocolo. Especifique el valor de tiempo mediante cualquier combinación de meses, semanas, días y horas.

### Formato

CacheDefaultExpiry *plantilla\_URL tiempo\_caducidad*

### Valores por omisión

CacheDefaultExpiry ftp:\* 1 day  
CacheDefaultExpiry gopher:\* 2 days  
CacheDefaultExpiry http:\* 0 days

**Nota:** La caducidad por omisión del protocolo HTTP es 0 days. Se recomienda la conservación de este valor ya que numerosos programas de script no proporcionan una fecha de caducidad, aunque su salida caduca inmediatamente. Un valor distinto de 0 puede provocar que los clientes vean el contenido desfasado.

## CacheDev: especificar un dispositivo de almacenamiento para la antememoria

Utilice esta directiva para especificar un dispositivo de almacenamiento de antememoria. Se puede modificar tanto un archivo como una partición de disco sin procesar. En las plataformas AIX, se puede modificar un volumen lógico sin procesar. Si no se utiliza una antememoria de memoria, la colocación en antememoria de disco sin procesar genera el mejor rendimiento.

Tenga en cuenta que los dispositivos de antememoria deben prepararse antes de especificarse. Para preparar un dispositivo de antememoria, formateéelo mediante el mandato **htcformat**. Para obtener más información, consulte “Mandato htcformat” en la página 172.

Se pueden especificar varios dispositivos de antememoria. Todos los dispositivos se asocian con mismos valores CacheMemory y BlockSize. No obstante, todos ellos incurrir en una actividad adicional de la memoria de aproximadamente 8 MB en la máquina del servidor proxy. Menos dispositivos de gran tamaño son más eficaces que un mayor número dispositivos más pequeños. Para lograr una mayor eficacia, utilice un disco entero como una partición grande sin que haya nada más en el disco. Para obtener más información sobre el almacenamiento en antememoria, consulte “Optimización del rendimiento de antememoria de disco” en la página 109.

### Formato

CacheDev {partición\_disco\_sin\_procesar | archivo}

### Ejemplos

**AIX:** CacheDev /dev/r1v02

**HP-UX:** CacheDev /dev/rdsk/c1t15d0

**Linux:** CacheDev /opt/IBMWTE/filecache1

**Solaris:** CacheDev /dev/rdsk/c1t3d0s0

**Windows:** CacheDev \\.\E:

### Valor por omisión

Ninguno

## CacheExpiryCheck: especificar si el servidor devuelve los archivos caducados

Utilice esta directiva para especificar si el servidor devuelve los archivos en antememoria que han caducado. Establezca el valor en **Off**, si desea que el servidor devuelva los archivos caducados. Utilice el valor por omisión de **On** si desea que el proxy compruebe mediante el servidor de origen si existe una versión más reciente cuando un cliente solicite un archivo caducado. Generalmente, los administradores no desean que el servidor devuelva archivos caducados, salvo, quizás, en aquellas ocasiones en que están haciendo pruebas del servidor y no les preocupa especialmente el contenido que se devuelve.

### Formato

CacheExpiryCheck {on | off}

## Valor por omisión

CacheExpiryCheck On

## CacheFileSizeLimit: especificar el tamaño máximo para que los archivos se almacenen en antememoria

Utilice esta directiva para especificar el tamaño máximo de archivos que se desea colocar en antememoria. Los archivos que sobrepasan este tamaño no se colocan en antememoria. El valor puede especificarse en bytes (B), kilobytes (K), megabytes (M) o gigabytes (G). No importa si la especificación incluye un espacio entre el número y la unidad de medida (B, K, M, G).

### Formato

CacheFileSizeLimit *máximo* {B | K | M | G}

## Valor por omisión

CacheFileSizeLimit 4000 K

## CacheLastModifiedFactor: especificar el valor para determinar las fechas de caducidad

Utilice esta directiva para especificar el valor que se desea utilizar para calcular las fechas de caducidad de URL específicos o de todos aquellos URL que coincidan con una plantilla.

Los servidores HTTP con frecuencia proporcionan la última vez que se ha modificado un archivo pero no la fecha de caducidad. De forma parecida, los archivos FTP pueden proporcionar una indicación de hora modificada por última vez pero carecer de una fecha de caducidad. Caching Proxy calcula una fecha de caducidad de estos archivos basada en la hora en que se han modificado por última vez. Utiliza la hora de última modificación para determinar el periodo de tiempo desde que se ha modificado el archivo y lo multiplica por el valor que aparece en la directiva CacheLastModifiedFactor. El resultado de este cálculo se corresponde con la duración del archivo o con el intervalo de tiempo antes de que caduque.

Puede especificar off o -1 para desactivar la directiva sin calcular la fecha de caducidad. El servidor proxy lee las directivas CacheLastModifiedFactor en el orden en el que aparecen en el archivo de configuración. Utiliza la primera directiva que puede aplicar al archivo en antememoria.

### Formato

CacheLastModifiedFactor *url factor*

*url*

Especifica el URL completo, incluido el protocolo, del archivo que se desea colocar en antememoria. Puede utilizar una plantilla de URL con asteriscos (\*) como caracteres comodín para aplicar una máscara.

*factor*

Especifica el factor que se desea utilizar para realizar el cálculo. También se puede especificar el valor off o -1.

## Ejemplos

```
CacheLastModifiedFactor *://hosta/* off
CacheLastModifiedFactor ftp://hostb/* 0.30
CacheLastModifiedFactor ftp://* 0.25
CacheLastModifiedFactor http://* 0.10
CacheLastModifiedFactor * 0.50
```

## Valores por omisión

```
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
```

El valor por omisión de 0.14 hace que los archivos modificados siete días antes caduquen en un día.

## CacheLocalDomain: especificar si se debe colocar en antememoria el dominio local

Utilice esta directiva para especificar si se desea colocar en antememoria los URL de sistemas principales pertenecientes al mismo dominio que el proxy. Generalmente no es necesario colocar en antememoria los sitios locales de una intranet porque el ancho de banda interno es suficiente para cargar los URL con rapidez. Si no colocan en antememoria los sitios locales, se ahorra espacio de antememoria para los URL cuya recuperación requiere más tiempo.

### Formato

```
CacheLocalDomain {on | off}
```

### Valor por omisión

```
CacheLocalDomain on
```

## CacheMatchLanguage: especificar la preferencia de idioma para el contenido de antememoria devuelto

Si el servidor de programa de fondo tiene la posibilidad de devolver a los clientes las variantes del idioma para el mismo URL, utilice esta directiva para dar soporte a la colocación en antememoria de diferentes idiomas para el mismo URL. La directiva permite a Caching Proxy verificar la preferencia del idioma en las peticiones con el idioma de la respuesta en antememoria.

Cuando se habilita CacheMatchLanguage, Caching Proxy compara la preferencia del idioma de la cabecera Accept-Language de la petición con el idioma del contenido en antememoria antes de que Caching Proxy cargue el contenido en antememoria. Caching Proxy también compara la distancia de preferencia. Si la distancia de preferencia es inferior a un límite especificado, Caching Proxy devuelve la copia en antememoria; de lo contrario, el proxy envía la petición al servidor de programa de fondo para obtener una copia nueva en el idioma solicitado.

## Formato

`CacheMatchLanguage {on | off}`

*límite\_distancia\_preferencia\_idioma id\_especial\_para\_todos\_idiomas*

*límite\_distancia\_preferencia\_idioma*

Especifique un valor que esté dentro del rango 0,001–0,9999.

*id\_especial\_para\_todos\_idiomas*

Especifique una serie del idioma devuelta desde el servidor de la cabecera Content-Language para informar al proxy de que la respuesta se puede utilizar para todas las preferencias del idioma.

## Ejemplos

A continuación aparece un ejemplo de configuración de la directiva, el objeto de antememoria y la petición.

`CacheMatchLanguage On 0.2`

Si el objeto de antememoria es chino simplificado (zh\_cn) y la petición es:

`GET / HTTP/1.1`

...

`Accept-Language: en_US;q=1.0, zh_cn;q=0.7, ja;q=0.3`

....

Para esta petición, el cliente solicita una página en inglés (con el código y calidad en\_US/1.0), a continuación, en chino simplificado (con el código y calidad zh\_cn/0.7) y, por último, en japonés (con el código y calidad ja/0.3). El objeto en antememoria está en chino simplificado. La distancia de preferencia entre la mejor calidad esperada y la calidad del idioma coincidente es  $1.0 - 0.7 = 0.3$ . Como el límite está establecido en 0.2 por la directiva `CacheMatchLanguage`, y 0.3 es mayor que el límite, el proxy pide al servidor una nueva copia de ese URL en lugar de devolver el objeto en antememoria.

Si el servidor no especifica un idioma ni `special-id-for-all-lang` en la cabecera Content-Language al devolver una respuesta, el proxy no coincide con la preferencia del idioma y devuelve la copia en antememoria cuando entra la siguiente petición.

## Valor por omisión

`CacheMatchLanguage off`

## CacheMaxExpiry: especificar la duración máxima de los archivos en antememoria

Utilice esta directiva para definir el periodo máximo de tiempo que los archivos pueden permanecer en la antememoria. La duración de un archivo en antememoria define el intervalo de tiempo que puede servirse desde la antememoria sin que se compruebe el origen en busca de actualizaciones. En algunos casos, la duración calculada para un archivo en antememoria puede ser superior a la deseada para que se mantenga ese archivo. La duración del archivo, ya sea especificada por el origen o calculada por Caching Proxy, no puede exceder el límite especificado por la directiva `CacheMaxExpiry`.

Se permiten varias apariciones de esta directiva en el archivo de configuración. Incluya una directiva independiente para cada plantilla.

## Formato

`CacheMaxExpiry URL duración`

#### *URL*

Especifica el URL plenamente cualificado, incluido el protocolo, del archivo que se desea colocar en antememoria. Puede utilizar una plantilla de URL con asteriscos (\*) como caracteres comodín para aplicar una máscara.

#### *duración*

Especifica la duración máxima de los archivos en antememoria que coincidan con la plantilla de URL. El tiempo se puede especificar mediante cualquier combinación de meses, semanas, días, horas, minutos y segundos.

### **Ejemplos**

CacheMaxExpiry ftp:\* 1 month

CacheMaxExpiry http://www.santaclaus.np/\* 2 days 12 hours

### **Valor por omisión**

CacheMaxExpiry 1 month

## **CacheMemory: especificar la memoria RAM de antememoria**

Utilice esta directiva para especificar la cantidad de memoria que se desea asociar con la antememoria. Para un rendimiento óptimo de las antememorias de disco, se recomienda un valor mínimo de memoria de antememoria de 64 MB para el soporte de infraestructura de antememoria, incluido el índice de antememoria. A medida que aumenta el tamaño de antememoria, aumenta el índice de antememoria y se necesita más memoria de antememoria para almacenar el índice. Un valor de memoria de antememoria de 64 MB es lo bastante grande para proporcionar el soporte de infraestructura y almacenar un índice de antememoria para una antememoria de disco de hasta 6.4 GB aproximadamente. Para antememorias de disco de mayor tamaño, la memoria de antememoria debería ser el 1% del tamaño de antememoria.

Si se utiliza la colocación en antememoria de la memoria, establezca esta directiva para que incluya la antememoria y la cantidad de memoria necesaria para el índice de antememoria.

El valor máximo recomendado para esta directiva es 1600 MB. Este límite viene determinado por el hecho de que Caching Proxy, como aplicación de 32 bits, puede utilizar un valor máximo de 2 GB de memoria. Si la cantidad de memoria necesaria para la antememoria más la cantidad de memoria utilizada para el proceso de rutina se aproxima a 2 GB o los excede, Caching Proxy no funciona con normalidad.

La cantidad puede especificarse en cualquiera de las siguientes unidades: bytes (B), kilobytes (K), megabytes (M) y gigabytes (G).

### **Formato**

CacheMemory *cantidad* {B | K | M | G}

### **Valor por omisión**

CacheMemory 64 M

## **CacheMinHold: especificar el periodo de tiempo que están disponibles los archivos**

Utilice esta directiva para especificar los URL de los archivos cuya fecha de caducidad va a sobrescribirse. Algunos sitios establecen los archivos para que caduquen antes de que finalice su duración, lo que requiere que el servidor solicite el archivo con más frecuencia. La directiva CacheMinHold hace que se retenga el



archivo caducado en la antememoria durante el periodo de tiempo especificado antes de que se solicite de nuevo. Esta directiva puede especificarse varias veces.

**Nota:** Si se escriben las fechas de caducidad, los archivos de la antememoria pueden quedarse obsoletos o desfasados.

### Ejemplo

CacheMinHold http://www.cachebusters.com/\* 1 hour

### Valor por omisión

Ninguno

## CacheNoConnect: especificar la modalidad de antememoria autónoma

Utiliza esta directiva para especificar si el servidor proxy debe recuperar los archivos de los servidores remotos. El valor por omisión (Off) habilita el servidor para que recupere los archivos de los servidores remotos. El valor On establece el servidor para que se ejecute en la modalidad de antememoria autónoma. Esto significa que el servidor sólo puede devolver los archivos ya almacenados en la antememoria. Generalmente, al ejecutar el servidor en esta modalidad, también establece la directiva CacheExpiryCheck en Off.

La ejecución del servidor en la modalidad de antememoria autónoma puede ser de utilidad si está utilizando el servidor para demostraciones. Si tiene conocimiento de que todos los archivos que desea utilizar para una demostración se almacenan en la antememoria, no es necesaria una conexión de red.

### Formato

CacheNoConnect {on | off}

### Valor por omisión

CacheNoConnect Off

## CacheOnly: colocar en antememoria sólo los archivos con los URL que coinciden con una plantilla

Utilice esta directiva para especificar que sólo los archivos con los URL que coincidan con una plantilla específica se coloquen en la antememoria. Puede utilizar varias apariciones de esta directiva en el archivo de configuración. Incluya una directiva independiente para cada plantilla. La plantilla de URL debe incluir el protocolo. Si no se establece ningún valor para esta directiva, todos los URL que no coincidan con una directiva NoCaching pueden colocarse en antememoria. Si no se incluyen las directivas CacheOnly ni NoCaching en el archivo de configuración, se puede colocar en antememoria cualquier URL.

### Formato

CacheOnly *patrón\_url*

### Ejemplo

CacheOnly http://realstuff/\*

### Valor por omisión

Ninguno

## CacheQueries: especificar las respuestas de antememoria a los URL que contienen un signo de interrogación (?)

Utilice esta directiva para especificar los URL para los que se colocan en antememoria las respuestas a las peticiones de consulta. Si se utiliza el valor `PUBLIC patrón_url`, las respuestas a las peticiones GET que contienen un signo de interrogación en el URL se colocan en antememoria si el servidor de origen incluye la cabecera `cache-control: public` y, además, la respuesta puede colocarse en antememoria. Si se especifica el valor `ALWAYS patrón_url`, las respuestas a las peticiones GET que contienen un signo de interrogación en el URL se colocan en antememoria si éstas puede colocarse en antememoria.

Esta directiva puede especificarse varias veces.

```
CacheQueries {ALWAYS | PUBLIC} patrón_url
```

### Ejemplos

```
CacheQueries ALWAYS http://www.hosta.com/*
CacheQueries PUBLIC http://www.hostb.com/*
```

**Nota:** Para obtener la compatibilidad con versiones anteriores, la sintaxis anterior de `CacheQueries {ALWAYS | PUBLIC | NEVER}` debe tratarse del siguiente modo:

- `CacheQueries ALWAYS` y `CacheQueries PUBLIC` deben tratarse como `CacheQueries ALWAYS *` y `CacheQueries PUBLIC *`.
- `CacheQueries NEVER` se ignora.
- Si se especifican `CacheQueries NEVER` y `CacheQueries patrón_url`, se ignora `CacheQueries NEVER`, pero se emite un mensaje de aviso.

### Valor por omisión

Ninguno

## CacheRefreshInterval: especificar el intervalo de tiempo para volver a validar los objetos en antememoria

Utilice esta directiva para especificar cuándo se debe realizar la comprobación con el servidor de origen para determinar si ha cambiado un archivo en antememoria.

A pesar de que la directiva `CacheClean` parece idéntica a esta directiva, existe una diferencia. `CacheRefreshInterval` sólo especifica que el proxy vuelve a validar un archivo antes de utilizarlo, mientras que la directiva `CacheClean` hace que el archivo se elimine de la antememoria después de un periodo de tiempo especificado.

### Formato

- El siguiente formato especifica el intervalo de renovación para todos los archivos que coincidan con el patrón de URL:

```
CacheRefreshInterval patrón_URL periodo_tiempo
```

- El siguiente formato especifica el intervalo de renovación para todos los archivos que *no* coincidan con un patrón de URL. Sólo se especifica un intervalo de renovación.

```
CacheRefreshInterval periodo_tiempo
```

### Ejemplos

```
CacheRefreshInterval *.gif 8 hours
CacheRefreshInterval 1 week
```

### Valor por omisión

CacheRefreshInterval 2 weeks

## CacheRefreshTime: especificar cuándo se desea iniciar el agente de antememoria

Utilice esta directiva para especificar cuándo se desea iniciar el agente de antememoria. Puede iniciar el agente de antememoria en un momento específico.

### Formato

CacheRefreshTime *HH:MM*

### Valor por omisión

CacheRefreshTime 03:00

## CacheTimeMargin: especificar la duración mínima para colocar en antememoria un archivo

La directiva CacheTimeMargin especifica la duración mínima de un archivo que es necesaria para que se pueda colocar en antememoria.

Caching Proxy calcula un tiempo de caducidad para todos los archivos. Si es improbable que se reciba otra petición para el archivo antes de que éste caduque, Caching Proxy considera que la duración del archivo es demasiado corta para que éste se coloque en antememoria. Por omisión, Caching Proxy no coloca en antememoria los archivos cuya duración es inferior a 10 minutos. Si la antememoria no está próxima a su capacidad máxima, deje esta directiva en el valor inicial. Si la antememoria está próxima a su capacidad total, se recomienda que aumente el valor de la duración mínima.

### Formato

CacheTimeMargin *duración\_mínima*

### Valor por omisión

CacheTimeMargin 10 minutes

**Nota:** El establecimiento de esta directiva a más de cuatro horas reduce dramáticamente la eficacia de la antememoria.

## CacheUnused: especificar el periodo de tiempo que se deben mantener los archivos en antememoria no utilizados

Utilice esta directiva para establecer el intervalo de tiempo máximo para que el servidor mantenga los archivos en antememoria no utilizados que tengan los URL que coincidan con una plantilla especificada. El servidor suprime los archivos no utilizados que tengan los URL que coincidan con la plantilla después de su colocación en antememoria durante el tiempo especificado, independientemente de la fecha de caducidad. Puede incluir varias apariciones de esta directiva en el archivo de configuración. Incluya una directiva independiente para cada plantilla. La plantilla de URL debe incluir el protocolo. Especifique el valor de tiempo mediante cualquier combinación de meses, semanas, días y horas.

### Formato

CacheUnused *plantilla\_URL periodo\_tiempo*

## Ejemplos

```
CacheUnused ftp:* 3 weeks
CacheUnused gopher:* 3 days 12 hours
CacheUnused * 4 weeks
```

## Valores por omisión

```
CacheUnused ftp:* 3 days
CacheUnused gopher:* 12 hours
CacheUnused http:* 2 days
```

## Caching: habilitar la colocación en antememoria de proxy

Utilice esta directiva para habilitar la colocación en antememoria de los archivos. Con la colocación en antememoria activada, el servidor proxy almacena los archivos que recupera de otros servidores en una antememoria local. A continuación, El servidor proxy responde a las peticiones posteriores de los mismos archivos sin necesidad de recuperarlos de otros servidores.

### Formato

```
Caching {on | off}
```

### Valor por omisión

```
Caching On
```

**Nota:** Si modifica la directiva Caching, debe detener e iniciar el servidor manualmente. (Consulte el Capítulo 5, “Inicio y detención de Caching Proxy”, en la página 15.)

## CompressAge: especificar cuándo comprimir las anotaciones cronológicas

Utilice esta directiva para especificar la antigüedad después de la cual se comprimen las anotaciones cronológicas. Cuando las anotaciones cronológicas son más antiguas que el valor establecido para CompressAge, se comprimen. Si CompressAge se establece en 0, no se comprimen las anotaciones cronológicas nunca. Las anotaciones cronológicas del día actual y días anteriores nunca se comprimen.

### Formato

```
CompressAge número_de_días
```

### Valor por omisión

```
CompressAge 1
```

### Directivas relacionadas

- “CompressDeleteAge: especificar cuándo suprimir las anotaciones cronológicas” en la página 204
- “CompressCommand: especificar el mandato y los parámetros de compresión” en la página 203
- “LogArchive: especificar el comportamiento del archivado de las anotaciones cronológicas” en la página 237
- “Midnight: especificar el plug-in de API utilizado para archivar las anotaciones cronológicas” en la página 246
- “PurgeAge: especificar el límite de antigüedad para las anotaciones cronológicas” en la página 271
- “PurgeSize: especificar el límite del tamaño del archivador de anotaciones cronológicas” en la página 272

## CompressCommand: especificar el mandato y los parámetros de compresión

Utilice esta directiva para crear un mandato que identifique el programa de utilidad de compresión utilizado para compactar las anotaciones cronológicas y que pasa los parámetros a ese programa de utilidad. Incluya la vía de acceso de las anotaciones cronológicas archivadas.

El programa de utilidad de compresión debe estar instalado en un directorio incluido en la vía de acceso para esa máquina.

### Formato

CompressCommand *mandato*

*mandato*

Incluye el mandato y los parámetros que desea utilizar especificados en una única línea. Generalmente, los parámetros incluyen %%LOGFILES%% y %%DATE%%.

%%LOGFILES%%

Especifica la lista de archivos de anotaciones cronológicas que están disponibles para un valor %%DATE%% determinado.

%%DATE%%

Especifica la indicación de fecha de un archivo de anotaciones cronológicas.

### Ejemplos

- **Linux y UNIX:**

```
CompressCommand tar -cf /logarchs/log%%DATE%%.tar %%LOGFILES%% ;
gzip /logarchs/log%%DATE%%.tar
CompressCommand tar -cf /logarchs/log%%DATE%%.tar %%LOGFILES%% ;
compress /logarchs/log%%DATE%%.tar
CompressCommand zip -q /logarchs/log%%DATE%%.zip %%LOGFILES%%
```

**Nota:** El mandato y todos los parámetros deben especificarse en una única línea. En los ejemplos anteriores, los dos primeros ejemplos de mandatos se han dividido por razones de claridad.

- **Windows:**

```
CompressCommand pkzip -q d:\logarchs\log%%DATE%%.tar %%LOGFILES%%
```

### Valor por omisión

Ninguno

### Directivas relacionadas

- “CompressAge: especificar cuándo comprimir las anotaciones cronológicas” en la página 202
- “CompressDeleteAge: especificar cuándo suprimir las anotaciones cronológicas” en la página 204
- “LogArchive: especificar el comportamiento del archivado de las anotaciones cronológicas” en la página 237
- “Midnight: especificar el plug-in de API utilizado para archivar las anotaciones cronológicas” en la página 246
- “PurgeAge: especificar el límite de antigüedad para las anotaciones cronológicas” en la página 271
- “PurgeSize: especificar el límite del tamaño del archivador de anotaciones cronológicas” en la página 272

## CompressDeleteAge: especificar cuándo suprimir las anotaciones cronológicas

Utilice esta directiva para especificar cuándo se desean suprimir las anotaciones cronológicas después de su compresión. Cuando las anotaciones cronológicas son más antiguas que el número de días establecido para el valor de CompressDeleteAge, se suprimen. Si CompressDeleteAge se establece en 0 o si el valor es inferior al valor establecido para la directiva CompressAge, no se suprimen las anotaciones cronológicas.

**Nota:** El plug-in de compresión nunca suprime las anotaciones cronológicas del día actual ni del día anterior.

### Formato

CompressDeleteAge *número\_de\_días*

### Valor por omisión

CompressDeleteAge 7

### Directivas relacionadas

- “CompressAge: especificar cuándo comprimir las anotaciones cronológicas” en la página 202
- “CompressCommand: especificar el mandato y los parámetros de compresión” en la página 203
- “LogArchive: especificar el comportamiento del archivado de las anotaciones cronológicas” en la página 237
- “Midnight: especificar el plug-in de API utilizado para archivar las anotaciones cronológicas” en la página 246
- “PurgeAge: especificar el límite de antigüedad para las anotaciones cronológicas” en la página 271
- “PurgeSize: especificar el límite del tamaño del archivador de anotaciones cronológicas” en la página 272

## CompressionFilterAddContentType — Especificar el tipo de contenido de la respuesta HTTP que desea comprimir

Utilice esta directiva para especificar el tipo de contenido de la respuesta HTTP que desea comprimir.

La compresión de la respuesta HTTP ayuda a reducir la carga de red y mejora el rendimiento del servidor proxy. Cuando la función de filtro de compresión está habilitada, si el navegador da soporte a la compresión HTTP y si la respuesta HTTP no está comprimida actualmente, Caching Proxy comprime la respuesta HTTP y devuelve el contenido comprimido al navegador.

### Ejemplos

Puede habilitar la función de filtro de compresión añadiendo las dos directivas siguientes en el archivo ibmproxy.conf:

- **Para sistemas HP-UX:**

```
CompressionFilterEnable /opt/ibm/edge/cp/lib/mod_z.sl  
CompressionFilterAddContentType type-1[,type-n]
```

- **Para otros sistemas UNIX® y para sistemas Linux:**

```
CompressionFilterEnable /opt/ibm/edge/cp/lib/mod_z.so  
CompressionFilterAddContentType type-1[,type-n]
```

- **Para sistemas Windows:**

```
CompressionFilterEnable C:\Progra~1\IBM\edge\cp\Bin\mod_z.dll
CompressionFilterAddContentType type-1[,type-n]
```

La biblioteca `mod_z` a la que se hace referencia en la directiva `CompressionFilterEnable` es la versión dinámica de `zlib1.1.4`.

La variable `type-n` es cualquier valor válido de la cabecera `Content-Type`; por ejemplo: `text/html` o `image/bmp`.

**Nota:** El contenido de ciertos tipos de respuestas HTTP, por ejemplo, imágenes JPEG o corrientes de vídeo, ya está muy comprimido por otras aplicaciones; por consiguiente, no deberían comprimirse con esta función.

#### Valor por omisión

Ninguno

### CompressionFilterEnable — Habilitar el filtro de compresión para comprimir las respuestas HTTP

Utilice esta directiva para habilitar el filtro de compresión a fin de comprimir las respuestas HTTP del servidor de fondo o de la antememoria del servidor proxy.

Para ver ejemplos de cómo utilizar esta directiva, consulte “`CompressionFilterAddContentType` — Especificar el tipo de contenido de la respuesta HTTP que desea comprimir” en la página 204.

#### Valor por omisión

Ninguno

### ConfigFile: especificar el nombre de un archivo de configuración adicional

Utilice esta directiva para especificar el nombre y la ubicación de un archivo de configuración adicional. Las directivas que aparecen en el archivo de configuración especificado se procesan después del archivo de configuración actual.

**Nota:** Asegúrese de que el archivo de configuración adicional tenga el permiso establecido en `Read` para que el usuario `nobody` permita al agente de antememoria leer este archivo.

#### Ejemplos

- **Linux y UNIX:** `ConfigFile /etc/rca.conf`
- **Windows:** `ConfigFile c:\WINNT\rca.conf`

#### Valor por omisión

Ninguno

### ConnThreads: especificar el número de hebras de conexión que se van a utilizar para la gestión de conexiones

Utilice esta directiva para definir el número de hebras de conexión que se van a utilizar para la gestión de conexiones.

#### Formato

`ConnThreads` *número*

## Valor por omisión

ConnThreads 5

## Directivas relacionadas

- “MaxActiveThreads: especificar el número máximo de hebras activas” en la página 242

## ContinueCaching: especificar qué cantidad de un archivo es necesaria para la colocación en antememoria

Utilice esta directiva para especificar qué cantidad de un archivo solicitado debe transferirse para que Caching Proxy complete la creación del archivo de antememoria, incluso si la conexión de cliente ha finalizado. Los valores válidos para esta variable son enteros que están en el rango de 0 – 100.

Por ejemplo, si se especifica ContinueCaching 75, Caching Proxy continúa la transferencia del archivo desde el servidor de contenido y genera el archivo de antememoria si el 75% o más del archivo ya se ha transferido antes de que Caching Proxy detecte que la conexión de cliente ha terminado.

## Formato

ContinueCaching *porcentaje*

## Valor por omisión

ContinueCaching 75

## DefinePicsRule: proporcionar una norma de filtrado de contenido

Utilice esta directiva para proporcionar al proxy la información necesaria para filtrar los URL en busca del contenido que incluya la información de servicios de tarifas. Puede especificar esta directiva varias veces.

## Formato

```
DefinePicsRule "nombre_filtro" {
```

## Valor por omisión

```
DefinePicsRule "Exemplo RSAC" {
```

## DefProt: especificar la configuración de protección por omisión de las peticiones que coinciden con una plantilla

Utilice esta directiva para asociar una configuración de protección por omisión con las peticiones que coincidan con una plantilla.

**Nota:** Para que la protección funcione correctamente, las directivas DefProt y Protect deben colocarse antes de cualquier directiva Pass o Exec del archivo de configuración.

## Formato

```
DefProt plantilla_petición nombre_configuración [FOR dirección_IP_servidor | ]
```

*plantilla\_petición*

Especifica una plantilla para las peticiones que desee asociar con una configuración de protección por omisión. El servidor compara las peticiones de cliente de entrada con la plantilla y asocia una configuración de protección si se produce una coincidencia.



La protección, de hecho, no se activa para las peticiones que coinciden con la plantilla, a menos que la petición también coincida con una plantilla de una directiva Protect posterior. Consulte “Protect: activar una configuración de protección de las peticiones que coinciden con una plantilla” en la página 258 para obtener una explicación de cómo la directiva Protect se utiliza con DefProt.

#### *configuración*

La configuración de protección con nombre que se define en el archivo de configuración y que se desea asociar con las peticiones que coinciden con *plantilla\_petición*. La configuración de protección se define mediante subdirectivas de protección. Este parámetro puede adoptar una de las tres formas siguientes:

- Una vía de acceso completa y un nombre de archivo que especifican un archivo independiente que contiene las subdirectivas de protección.
- Un nombre de etiqueta de configuración de protección que coincide con un nombre definido anteriormente en una directiva Protection. La directiva Protection contiene las subdirectivas de protección.
- Las subdirectivas de protección reales. Las subdirectivas deben aparecer entre llaves {}. El carácter de llave izquierdo debe ser el último carácter que aparece en la misma línea que la directiva DefPro. Todas las subdirectivas continúan en su propia línea. El carácter de llave derecho debe aparecer en su propia línea después de la última línea de subdirectiva. No pueden aparecer líneas de comentario entre las llaves. Para obtener una descripción de las directivas de protección, consulte:
  - “AuthType: especificar el tipo de autenticación” en la página 264
  - “DeleteMask: especificar los nombres de usuario, grupos y direcciones que pueden suprimir archivos” en la página 264
  - “GetMask: especificar los nombres de usuario, grupos y direcciones que pueden obtener archivos” en la página 264
  - “GroupFile: especificar la ubicación del archivo de grupo asociado” en la página 264
  - “Mask: especificar los nombres de usuario, grupos y direcciones que pueden realizar peticiones HTTP” en la página 265
  - “PasswdFile: especificar la ubicación del archivo de contraseñas asociado” en la página 265
  - “PostMask: especificar los nombres de usuario, grupos y direcciones que pueden enviar archivos” en la página 265
  - “PutMask: especificar los nombres de usuario, grupos y direcciones que pueden transferir archivos” en la página 265
  - “ServerID: especificar un nombre para asociarlo con el archivo de contraseñas” en la página 266

#### **[FOR dirección\_IP\_servidor | ]**

Si está utilizando varias direcciones IP o sistemas principales virtuales, utilice este parámetro para especificar una dirección IP o un nombre de sistema principal. El servidor utiliza la directiva sólo para las peticiones que llegan al servidor en esta dirección IP o para este sistema principal. Para una dirección IP, esta es la dirección de la conexión de red del servidor, no la dirección del cliente solicitante.

Puede especificar una dirección IP (por ejemplo, FOR 240.146.167.72 ) o un nombre de sistema principal (por ejemplo, FOR sistppa1A.bcd.com ).

Este parámetro es opcional. Sin este parámetro, el servidor utiliza la directiva para todas las peticiones, independientemente de la dirección IP en la que entran las peticiones o el nombre de sistema principal del URL.

**Notas:**

1. Sólo puede utilizar este parámetro con el parámetro *configuración* especificado en forma de vía de acceso y nombre de archivo o de etiqueta de configuración. No puede utilizar este parámetro con el parámetro *configuración* especificado en forma de subdirectivas de protección reales incluidas entre comillas.
2. Para utilizar este parámetro, debe colocar FOR o cualquier otra serie de caracteres (sin espacios en blanco) entre el parámetro *configuración* y *dirección\_IP* o .

No puede especificarse un carácter comodín para la dirección IP de un servidor.

**Nota:** La directiva debe escribirse en una línea.

## Ejemplos

- El siguiente ejemplo identifica un archivo independiente que contiene las subdirectivas de protección.

```
DefProt /secret/*  
/server/protect/setup1.acc
```

- El siguiente ejemplo utiliza un nombre de etiqueta para señalar a las subdirectivas de protección. El nombre de etiqueta debe coincidir con un nombre de etiqueta de una directiva Protection. La directiva Protection debe aparecer antes de la directiva DefProt.

```
DefProt /secret/* SECRET-PROT
```

- Los siguientes ejemplos incluyen las subdirectivas de protección como parte de la directiva DefProt.

```
DefProt {  
    AuthType Basic  
    ServerID restricted  
    PasswdFile /docs/etc/WWW/restrict.password  
    GroupFile /docs/etc/WWW/restrict.group  
    GetMask authors  
    PutMask authors  
}
```

- Los siguientes ejemplos utilizan el parámetro de dirección IP opcional. Si el servidor recibe peticiones que empiecen por /secret/, asocia una configuración de protección por omisión distinta con la petición basándose en la dirección IP de la conexión de red que la petición utiliza para entrar. Para las peticiones que entran en 0.67.106.79, el servidor asocia la petición con la protección por omisión definida en una directiva Protection con la etiqueta ClienteA-PROT. Para las peticiones que entran en 0.83.100.45, el servidor asocia la petición con la protección por omisión definida en una directiva Protection con la etiqueta ClienteB-PROT.

```
DefProt /secret/* ClienteA-PROT 0.67.106.79  
DefProt /secret/* ClienteB-PROT 0.83.100.45
```

- Los siguientes ejemplos utilizan el parámetro de nombre de sistema principal opcional. Si el servidor recibe peticiones que empiecen por /secret/, asocia una configuración de protección por omisión distinta con la petición basándose en el nombre de sistema principal del URL. Para las peticiones que entran para sistppalA, el servidor asocia la petición con la protección por omisión definida en una directiva Protection con la etiqueta ClienteA-PROT. Para las peticiones

que entran para sistppalB, el servidor asocia la petición con la protección por omisión definida en una directiva Protection con la etiqueta ClienteB-PROT.

```
DefProt /secret/* ClienteA-PROT sistppalA.bcd.com
DefProt /secret/* ClienteB-PROT sistppalB.bcd.com
```

### Valor por omisión

Ninguno

## DelayPeriod: especificar si debe haber una pausa entre peticiones

Utilice esta directiva para especificar si el agente de antememoria debe esperar entre los envíos de peticiones a los servidores de destino. La especificación de un retraso entre las peticiones reduce la carga en la máquina proxy y el enlace de red, además de en los servidores de destino. Si no se especifican retrasos, deje que el agente de antememoria se ejecute a la máxima velocidad. Para las conexiones de Internet lentas, se recomienda que no se especifique ningún periodo de retraso para lograr la máxima utilización de la red.

**Nota:** Si la red de Internet es más rápida que 128 kbps, establezca DelayPeriod en On para evitar el envío de demasiadas peticiones con demasiada rapidez a los sitios que se están renovando.

### Formato

DelayPeriod {on | off}

### Valor por omisión

DelayPeriod On

## DelveAcrossHosts: especificar la colocación en antememoria entre dominios

Utilice esta directiva para especificar si el agente de antememoria debe seguir los enlaces de hipertexto en los distintos sistemas principales. Si un URL en antememoria contiene enlaces con otros servidores, el servidor puede ignorar el enlace o seguirlo. Si la directiva DelveInto está establecida en never, no se aplica esta directiva.

### Formato

DelveAcrossHosts {on | off}

### Valor por omisión

DelveAcrossHosts Off

## DelveDepth: especificar hasta dónde se deben seguir los enlaces durante la colocación en antememoria

Utilice esta directiva para especificar el número de niveles de enlace que se deben seguir al buscar las páginas que se vayan a cargar en la antememoria. Si la directiva DelveInto está establecida en never, no se aplica esta directiva.

### Formato

DelveDepth *número\_de\_niveles*

### Valor por omisión

DelveDepth 2

## DelveInto: especificar si el agente de antememoria debe seguir los enlaces

Utilice esta directiva para especificar si el agente de antememoria debe cargar las páginas enlazadas desde los URL en antememoria.

### Formato

`DelveInto {always | never | admin | topn}`

#### **always**

El agente de antememoria sigue los enlaces de todos los URL colocados en antememoria anteriormente.

#### **never**

El agente de antememoria ignora todos los enlaces de los URL.

#### **admin**

El agente de antememoria sólo sigue los enlaces de los URL especificados en las directivas LoadURL

#### **topn**

El agente de antememoria sólo sigue los enlaces de los archivos recuperados con mayor frecuencia de la antememoria.

### Valor por omisión

`DelveInto always`

## DirBackgroundImage: especificar una imagen de fondo para los listados de directorios

Utilice esta directiva para aplicar una imagen de fondo a los listados de directorio generados por el servidor proxy. Los listados de directorios se generan cuando el servidor proxy se utiliza para examinar los sitios FTP.

Especifique una vía de acceso absoluta para la imagen de fondo. Si la imagen se ubica en otro servidor, la imagen de fondo debe especificarse como un URL completo. Si no se especifica ninguna imagen de fondo, se utiliza un fondo en blanco.

### Formato

`DirBackgroundImage /vía_acceso/archivo`

### Ejemplos

`DirBackgroundImage /images/corplogo.png`

`DirBackgroundimage http://www.somehost.com/graphics/embossed.gif`

### Valor por omisión

Ninguno

## DirShowBytes: mostrar el recuento en bytes de los archivos pequeños en los listados de directorios

Utilice esta directiva para especificar si los listados de directorios incluyen el recuento exacto de bytes para los archivos más pequeños que 1 KB. Un valor de Off indica que el listado de directorios muestra un tamaño de 1 KB para todos los archivos de 1 KB o menores.

### Formato

`DirShowBytes {on | off}`

### Valor por omisión

`DirShowBytes Off`

## **DirShowCase: utilizar las mayúsculas y minúsculas al ordenar los archivos en los listados de directorios**

Utilice esta directiva para especificar si los listados de directorios distinguen entre las mayúsculas y minúsculas al ordenar los nombres de archivo.

Un valor de `On` indica que las mayúsculas aparecen antes que las minúsculas en la lista de archivos.

### Formato

`DirShowCase {on | off}`

### Valor por omisión

`DirShowCase On`

## **DirShowDate: mostrar la fecha de última modificación en los listados de directorios**

Utilice esta directiva para especificar si los listados de directorios incluyen la fecha en que cada archivo fue modificado por última vez.

### Formato

`DirShowDate {on | off}`

### Valor por omisión

`DirShowDate On`

## **DirShowDescription: mostrar las descripciones de los archivos en los listados de directorios**

Utilice esta directiva para especificar si los listados de directorios incluyen las descripciones de los archivos HTML. Las descripciones se toman de los distintivos `<title>` HTML de los archivos.

Las descripciones de los listados de directorios FTP muestran los tipos MIME de los archivos si pueden determinarse.

### Formato

`DirShowDescription {on | off}`

### Valor por omisión

`DirShowDescription On`

## **DirShowHidden: mostrar los archivos ocultos en los listados de directorios**

Utilice esta directiva para especificar si los listados de directorios incluyen cualquier archivo oculto del directorio. El servidor considera cualquier archivo que tenga un nombre que empiece por un punto (.) como un archivo oculto.

### Formato

`DirShowHidden {on | off}`

### Valor por omisión

`DirShowHidden On`

## DirShowIcons: mostrar los iconos en los listados de directorios

Utilice esta directiva para especificar si el servidor incluye iconos en los listados de directorios. Los iconos pueden utilizarse para proporcionar una representación gráfica del tipo de contenido de los archivos del listado. Los iconos mismos se definen mediante las directivas `AddBlankIcon`, `AddDirIcon`, `AddIcon`, `AddParentIcon` y `AddUnknownIcon`.

### Formato

`DirShowIcons {on | off}`

### Valor por omisión

`DirShowIcons On`

## DirShowMaxDescrLength: especificar la longitud máxima de las descripciones en los listados de directorios

Utilice esta directiva para establecer el número máximo de caracteres que debe mostrarse en el campo de descripción de los listados de directorios.

### Formato

`DirShowMaxDescrLength`  
*número\_de\_caracteres*

### Valor por omisión

`DirShowMaxDescrLength 25`

## DirShowMaxLength: especificar la longitud máxima de los nombres de archivos en los listados de directorios

Utilice esta directiva para establecer el número máximo de caracteres que debe utilizarse para los nombres de archivo de los listados de directorios.

### Formato

`DirShowMaxDescrLength`  
*número\_de\_caracteres*

### Valor por omisión

`DirShowMaxLength 25`

## DirShowMinLength: especificar la longitud mínima de los nombres de archivos en los listados de directorios

Utilice esta directiva para establecer el número mínimo de caracteres que siempre está reservado para los nombres de archivo en los listados de directorios. Los nombres de archivo del directorio pueden exceder este número. No obstante, los nombres de archivo no pueden ser de mayor longitud que el número especificado en la directiva `DirShowMaxLength`.

### Formato

`DirShowMinLength` *número\_de\_caracteres*

### Valor por omisión

`DirShowMinLength 15`

## DirShowSize: mostrar el tamaño de archivo en los listados de directorios

Utilice esta directiva para especificar si los listados de directorios incluyen el tamaño de todos los archivos.

### Formato

`DirShowSize {on | off}`

### Valor por omisión

`DirShowSize On`

## Disable: inhabilitar los métodos HTTP

Utilice esta directiva para especificar qué métodos HTTP no acepta el servidor. Para cada método que el servidor vaya a rechazar, especifique una directiva `Disable` independiente.

En el archivo de configuración por omisión, los métodos GET, HEAD, OPTIONS, POST y TRACE están habilitados y todos los demás métodos HTTP soportados están inhabilitados. Para inhabilitar un método que esté habilitado en ese momento, suprimalo de la directiva `Enable` y añádalo en la directiva `Disable`.

### Formato

`Disable método`

**Nota:** Los formularios de Configuración y Administración utilizan el método POST para realizar actualizaciones de la configuración de servidor. Si inhabilita el método POST, no podrá utilizar los formularios de Configuración y Administración.

### Valores por omisión

```
Disable  PUT
Disable  DELETE
Disable  CONNECT
```

## DisInheritEnv: especificar las variables de entorno que no heredan los programas CGI

Utilice esta directiva para especificar qué variables de entorno no desea que los programas CGI hereden, además de las variables de entorno CGI que son específicas del proceso CGI.

Por omisión, los programas CGI heredan todas las variables de entorno. Utilice esta directiva para evitar que las variables de entorno individuales se hereden.

### Formato

`DisInheritEnv variable_entorno`

### Ejemplos

```
DisInheritEnv PATH
DisInheritEnv LANG
```

En este ejemplo, los programas CGI heredan todas las variables de entorno, excepto PATH y LANG.

## Valor por omisión

Ninguno

## DNS-Lookup: especificar si el servidor debe buscar los nombres de nombre de sistema principal de cliente

Utilice esta directiva para especificar si el servidor debe buscar los nombres de sistema principal de los clientes solicitantes.

### Formato

DNS-Lookup {on | off}

El valor que utilice afecta a los siguientes aspectos del funcionamiento del servidor:

- Rendimiento del servidor. La utilización del valor por omisión de Off mejora el rendimiento y el tiempo de respuesta de los servidores ya que éste no utiliza los recursos para realizar la búsqueda de nombres de sistema principal.
- Información que el servidor registra sobre los clientes al escribir en los archivos de anotaciones cronológicas.
  - Off: los clientes se identifican mediante la dirección IP.
  - On: los clientes se identifican mediante el nombre de sistema principal.
- Si puede utilizar los nombres de sistema principal en las plantillas de dirección de las configuraciones de protección, archivos de grupo de servidor y archivos ACL (Lista de control de acceso).
  - Off: no puede utilizar los nombres de sistema principal en las plantillas de dirección; debe utilizar las direcciones IP.
  - On: puede utilizar los nombres de sistema principal en las plantillas de dirección; no puede utilizar las direcciones IP.

**Nota:** Para utilizar los nombres de dominio en las normas de protección, debe establecer la directiva DNS-Lookup en On.

## Valor por omisión

DNS-Lookup Off

## Enable: habilitar los métodos HTTP

Utilice esta directiva para especificar qué métodos HTTP acepta el servidor.

Puede habilitar tantos métodos HTTP como sea necesario. Para cada método que el servidor vaya a aceptar, especifique una directiva Enable independiente.

### Formato

Enable *método*

Si no existe ninguna directiva Service para un determinado URL, puede utilizar la directiva Enable para realizar la programación personalizada de cualquier método HTTP. El programa que especifique en esta directiva sobrescribe el proceso estándar de ese método.

Enable *método* /*vía\_acceso/archivoDLL:nombre\_función*

para obtener información sobre el formato y las opciones disponibles para el método Enable CONNECT, consulte “Configuración de túneles SSL” en la página 122.



## Valores por omisión

Enable GET  
Enable HEAD  
Enable POST  
Enable TRACE  
Enable OPTIONS

## EnableTcpNodelay: habilitar la opción de socket TCP NODELAY

Utilice esta directiva para habilitar la opción de sockets TCP NODELAY.

La directiva EnableTcpNodelay mejora el rendimiento cuando pequeños paquetes IP como, por ejemplo, un protocolo de enlace SSL o una respuesta HTTP corta se transmiten entre Caching Proxy y el cliente. Por omisión, la opción TCP NODELAY se habilita para todos los sockets.

### Formato

EnableTcpNodelay {All | HTTP | HTTPS | None}

### Valor por omisión

EnableTcpNodelay All

## Error: personalizar el paso de error

Utilice esta directiva para especificar una función de aplicación personalizada a la que desea que el servidor llame durante el paso de error. Este código se ejecuta para proporcionar rutinas de error personalizadas cuando se encuentra un error.

### Formato

Error *plantilla\_petición* /*vía\_acceso/archivo:nombre\_función*

*plantilla\_petición*

Especifica una plantilla para las peticiones que determinan adicionalmente si se llama a la función de aplicación. La especificación puede incluir el protocolo, el dominio y el sistema principal; puede estar precedida por un carácter de barra inclinada (/), y puede utilizar un asterisco (\*) como carácter comodín. Por ejemplo, /front\_page.html , http://www.ics.raleigh.ibm.com, /pub\*, /\* y \* son todas válidas.

/*vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

### Ejemplo

Error /index.html /ics/api/bin/icsext05.so:error\_rtns

### Valor por omisión

Ninguno

## ErrorLog: especificar el archivo donde se anotan cronológicamente los errores de servidor

Utilice esta directiva para especificar la vía de acceso y el nombre de archivo donde desea que el servidor anote cronológicamente los errores internos.

**Nota:** Si cambia los valores por omisión del servidor para el ID de usuario, el ID de grupo o las vías de acceso de directorios de anotaciones cronológicas, cree los nuevos directorios y actualice los permisos y la propiedad de éstos. Para permitir que el servidor escriba la información en un directorio de anotaciones cronológicas definidas por el usuario, establezca el permiso para ese directorio como 755 y el ID de usuario del servidor definido por el usuario como el propietario. Por ejemplo, si cambia el ID de usuario del servidor del valor por omisión a jdoe y el directorio de anotaciones cronológicas por omisión a server\_root/account, el directorio server\_root/account debe tener el permiso 755 y ser propiedad de jdoe.

Si el servidor se está ejecutando, inicia un nuevo archivo de anotaciones cronológicas todos los días a las doce de la noche. De lo contrario, el servidor inicia un nuevo archivo de anotaciones cronológicas la primera vez que se inicia en un día cualquiera. Al crear el archivo, el servidor utiliza el nombre de archivo que especifica e añadirá un sufijo de fecha. El sufijo de fecha aparece en el formato *Mmmddaaaa*, donde *Mmm* representa las tres primeras letras del mes, *dd* representa el día del mes y *aaaa* representa el año.

### Formato

ErrorLog */vía\_acceso/directorio\_anotaciones\_cronológicas/nombre\_archivo*

### Valores por omisión

- **Sistemas Linux y UNIX:** ErrorLog */opt/ibm/edge/cp/server\_root/logs/error*
- **Sistemas Windows:** ErrorLog *unidad:\Archivos de programa\IBM\edge\cp\logs\error*

## ErrorPage: especificar un mensaje personalizado para una determinada condición de error

Utilice esta directiva para especificar el nombre del archivo que se envía al cliente que lo solicite cuando el servidor se encuentra con una determinada condición de error. El archivo de configuración *ibmproxy.conf* proporciona las directivas ErrorPage que asocian las palabras clave de error con los archivos de mensaje error.

Para personalizar los mensajes de error, puede modificar las directivas ErrorPage para asociar las palabras clave de error con los distintos archivos o puede modificar los archivos de mensaje de error proporcionados. Por ejemplo, puede modificar un mensaje para que incluya más información sobre la causa del problema y sugiera posibles soluciones para arreglarlo. Para las redes internas, es recomendable que proporcione una persona de contacto para puedan llamar los usuarios.

Las directivas ErrorPage pueden colocarse en cualquier lugar del archivo de configuración. Cuando se produce el error, se procesa el archivo de acuerdo con las normas de correlación definidas en el archivo de configuración. Por lo tanto, el archivo que desee enviar debe estar en una ubicación que pueda accederse mediante las normas de correlación como las definen las directivas Fail, Map, NameTrans, Pass, Redirect y Service. Como mínimo, es necesaria una directiva Pass que permita al servidor pasar el archivo de mensaje de error.

### Formato

ErrorPage *palabra\_clave /vía\_acceso/nombre\_archivo.html*

*palabra\_clave*

Especifica una de las palabras clave asociadas con una condición de error. Las

palabras clave se enumeran en las directivas `ErrorPage` del archivo `ibmproxy.conf`. No se pueden modificar las palabras clave.

#### **/vía\_acceso/archivoname.html**

Especifica el nombre Web plenamente cualificado del archivo de error como lo ve un cliente en la Web. Los archivos de mensaje de error por omisión están en `/HTML/errorpages/`.

### **Ejemplo**

```
ErrorPage scriptstart /HTML/errorpages/scriptstart.htmls
```

En este ejemplo, cuando se encuentra una condición `scriptstart`, el servidor envía al cliente el archivo `scriptstart.htmls` que se encuentra en el directorio `/HTML/errorpages/`.

El siguiente texto HTML es un ejemplo de lo que el archivo puede contener:

```
<HTML>
<HEAD>
<TITLE>Mensaje para la condición SCRIPTSTART</TITLE>
</HEAD>
<BODY>
No se ha podido iniciar el programa CGI.
<P>
<A HREF="mailto:admin@websvr.com">Notificar al administrador</A>
este problema.
</BODY>
</HTML>
```

Si la directiva que coincide con la anterior vía de acceso del archivo de configuración del servidor es `PASS /* /wwwhome/*`, entonces la vía de acceso completa es `/wwwhome/HTML/errorpages/scriptstart.htmls`.

### **Personalización de los mensajes de error que devuelve el servidor**

Todas las condiciones de error se identifican mediante una palabra clave. Para decidir qué mensajes de error desea personalizar, primero revise los archivos de mensaje de error proporcionados con Caching Proxy, que puede encontrar en `/HTML/errorpages`. La página de errores incluye el número de error, el mensaje por omisión, una explicación de la causa y una acción de recuperación apropiada.

A continuación, realice una de las acciones siguientes para cambiar un mensaje de error:

- Modifique el archivo HTML o HTMLS existente, creando primero una copia de seguridad, o bien cree un nuevo archivo HTML o HTMLS con el texto deseado. Puede utilizar un editor HTML o ASCII. Debe utilizarse un archivo HTMLS si desea utilizar inclusiones de la parte servidor.
- Si ha creado un archivo de mensaje de error con un nombre distinto o en una vía de acceso distinta, modifique la directiva `ErrorPage` para que esa palabra clave señale al archivo.

### **Condiciones de error, causas y mensajes por omisión**

Todas las palabras clave de error y los archivos de mensaje de error se enumeran en el archivo `ibmproxy.conf` del apartado de la directiva `ErrorPage`. Los archivos de mensaje de error incluyen el número de mensaje de error, la palabra clave, el mensaje por omisión, la explicación y la respuesta del usuario (acción).

## Valores por omisión

Muchos de los valores por omisión se incluyen en el archivo `ibmproxy.conf`

Si no modifica una directiva `ErrorPage` para una condición de error, se envía la página de error por omisión del servidor para esa condición.

## EventLog: especificar la vía de acceso del archivo de anotaciones cronológicas de sucesos

Utilice esta directiva para especificar el nombre de archivo y la vía de acceso de las anotaciones cronológicas de sucesos. Las anotaciones cronológicas de sucesos capturan los mensajes informativos sobre la propia antememoria.

**Nota:** Si cambia los valores por omisión del servidor para el ID de usuario, el ID de grupo o las vías de acceso de directorios de anotaciones cronológicas, cree los nuevos directorios y actualice los permisos y la propiedad de éstos. Para permitir que el servidor escriba la información en un directorio de anotaciones cronológicas definidas por el usuario, establezca el permiso para ese directorio como 755 y el ID de usuario del servidor definido por el usuario como el propietario. Por ejemplo, si cambia el ID de usuario del servidor del valor por omisión a `jdoe` y el directorio de anotaciones cronológicas por omisión a `server_root/account`, el directorio `server_root/account` debe tener el permiso 755 y ser propiedad de `jdoe`.

Si el servidor se está ejecutando, inicia un nuevo archivo de anotaciones cronológicas todos los días a las doce de la noche. De lo contrario, el servidor inicia un nuevo archivo de anotaciones cronológicas la primera vez que se inicia en un día cualquiera. Al crear el archivo, el servidor utiliza el nombre de archivo que especifica e añadirá un sufijo de fecha. El sufijo de fecha aparece en el formato *Mmmddaaaa*, donde *Mmm* representa las tres primeras letras del mes, *dd* representa el día del mes y *aaaa* representa el año.

### Formato

`EventLog /vía_acceso/directorio_anotaciones_cronológicas/nombre_archivo`

### Valores por omisión

- **Sistemas Linux y UNIX:** `EventLog /opt/ibm/edge/cp/server_root/logs/event`
- **Sistemas Windows:** `EventLog unidad:\Archivos de programa\IBM\edge\cp\logs\event`

## Exec: ejecutar un programa CGI para hacer coincidir las peticiones

Utilice esta directiva para especificar una plantilla que las peticiones acepten y a la que respondan mediante la ejecución de un programa CGI. Después de que una petición coincide con una plantilla de una directiva `Exec`, la petición no se compara con las plantillas de petición de cualquier directiva posterior.

### Formato

`Exec plantilla_petición vía_acceso_programa [dirección_IP_servidor | ]`

*plantilla\_petición*

Especifica una plantilla para las peticiones que el servidor va a aceptar y a las que va a responder mediante la ejecución de un programa CGI.

Debe utilizar un asterisco (\*) como comodín en `plantilla_petición` y `vía_acceso_programa`. La parte de la petición que coincide con el comodín `plantilla_petición` debe empezar con el nombre del archivo que contiene el programa CGI.

La petición también puede contener datos adicionales que se pasan al programa CGI de la variable de entorno `PATH_INFO`. Los datos adicionales siguen al primer carácter de barra inclinada (/) que aparece detrás del nombre de archivo del programa CGI de la respuesta. Los datos se pasan de acuerdo con las especificaciones CGI.

#### *vía\_acceso\_programa*

Especifica la vía de acceso al archivo que contiene el programa CGI que el servidor ejecuta para la petición. *vía\_acceso\_programa* también debe contener un carácter comodín. El carácter comodín se sustituye por el nombre del archivo que contiene el programa CGI.

La directiva `Exec` es recursiva y se aplica a todos los subdirectorios. No es necesaria una directiva `Exec` independiente para todos los directorios que aparecen bajo `cgi-bin` `admin-bin`.

#### *[dirección\_IP\_servidor | ]*

Si está utilizando varias direcciones IP o sistemas principales virtuales, utilice este parámetro para especificar una dirección IP o un nombre de sistema principal. El servidor utiliza la directiva sólo para las peticiones que llegan al servidor en esta dirección IP o para este sistema principal. Para una dirección IP, esta es la dirección de la conexión de red del servidor, no la dirección del cliente solicitante.

Puede especificar una dirección IP (por ejemplo, 240.146.167.72 ) o un nombre de sistema principal (por ejemplo, sistppalA.bcd.com ).

Este parámetro es opcional. Sin este parámetro, el servidor utiliza la directiva para todas las peticiones, independientemente de la dirección IP en la que entran las peticiones o el nombre de sistema principal del URL.

Los caracteres comodín no pueden utilizarse para especificar las direcciones IP de servidor.

## Ejemplos

En el siguiente ejemplo, si el servidor recibe una petición de `/idd/depts/plan/c92`, éste ejecuta el programa CGI de `/depts/bin/plan.exe` pasando `c92` al programa como entrada.

El siguiente ejemplo utiliza el parámetro de dirección IP opcional. Si el servidor recibe peticiones que empiezan por `/cgi-bin/`, sirve la petición desde un directorio distinto basándose en la dirección IP de la conexión de red en la que entra la petición. Para las peticiones que entran en 130.146.167.72, el servidor utiliza el directorio `/CGI-BIN/clienteA`. Para las peticiones que entran en cualquier conexión con una dirección de 0.83.100.45, el servidor utiliza el directorio `/CGI-BIN/clienteB`.

```
Exec    /cgi-bin/*    /CGI-BIN/clienteA/*    130.129.167.72
Exec    /cgi-bin/*    /CGI-BIN/clienteB/*    0.83.100.45
```

El siguiente ejemplo utiliza el parámetro de nombre de sistema principal opcional. Si el servidor recibe peticiones que empiezan por `/cgi-bin`, sirve la petición desde un directorio distinto basándose en el nombre de sistema principal del URL. Para las peticiones que entran para `sistppalA.bcd.com`, el servidor utiliza el directorio `/CGI-BIN/clienteA`. Para las peticiones que entran para `sistppalB.bcd.com`, el servidor utiliza el directorio `/CGI-BIN/clienteB`.

```
Exec    /cgi-bin/*      /CGI-BIN/clienteA/*  sistppa1A.bcd.com
Exec    /cgi-bin/*      /CGI-BIN/clienteB/*  sistppa1B.bcd.com
```

## Valores por omisión

- **Sistemas Linux y UNIX**

```
Exec    /cgi-bin/*      /opt/ibm/edge/cp/server_root/cgi-bin/*
Exec    /admin-bin/*    /opt/ibm/edge/cp/server_root/admin-bin/*
```

- **Sistemas Windows**

```
Exec    raíz_servidor/cgi-bin/*
Exec    raíz_servidor/admin-bin/*
Exec    raíz_servidor/DOCS/admin-bin/*
```

## ExportCacheImageTo: exportar la memoria de antememoria al disco

Utilice esta directiva para exportar el contenido de antememoria a un archivo de vuelco. Esto es útil cuando la antememoria de memoria se pierde durante el reinicio o al desplegar la misma antememoria para varios proxies.

### Formato

ExportCacheImageTo *nombre\_archivo\_exportación*

### Valor por omisión

Ninguno

## ExternalCacheManager: configurar Caching Proxy para la colocación en antememoria dinámica desde IBM WebSphere Application Server

Sólo se aplica a configuraciones de proxy de retorno.

Utilice esta directiva para configurar que Caching Proxy reconozca IBM WebSphere Application Server, que se configura con un módulo de adaptador de Caching Proxy y desde el cual puede colocar en antememoria los recursos creados dinámicamente. Caching Proxy guarda copias de los resultados de JSP que también se almacenan en la antememoria dinámica del servidor de aplicaciones. Caching Proxy coloca en antememoria sólo el contenido de un servidor IBM WebSphere Application Server cuyo ID de grupo coincida con una entrada ExternalCacheManager.

Tenga en cuenta que también es necesario añadir una directiva Service al archivo de configuración de Caching Proxy para habilitar esta característica. También son necesarios pasos de configuración adicionales en el servidor de aplicaciones. Consulte el Capítulo 22, “Colocación en antememoria de contenidos generados dinámicamente”, en la página 105 para obtener toda la información.

### Formato

ExternalCacheManager *ID\_Gestor\_Antememoria\_Externa*  
*Tiempo\_Caducidad\_Máximo*

*ID\_Gestor\_Antememoria\_Externa*

ID que se asigna al IBM WebSphere Application Server, que está sirviendo al proxy. El ID debe coincidir con el ID establecido en el atributo externalCacheGroup: group id del archivo dynacache.xml del servidor de aplicaciones.

*Tiempo\_Caducidad\_Máximo*

Fecha de caducidad por omisión establecida para los recursos en antememoria

en nombre del gestor de antememoria externo. Si el gestor de antememoria externo no invalida un recurso en antememoria en el tiempo especificado, el recurso caduca en ese tiempo. El tiempo puede especificarse en minutos o segundos.

### Ejemplo

La siguiente entrada define un gestor de antememoria externo (IBM WebSphere Application Server) que se encuentra en el dominio `www.xyz.com` y cuyos recursos caducan en 20 segundos o antes.

```
ExternalCacheManager IBM-CP-XYZ-1 20 seconds
```

### Valor por omisión

Ninguno

## Fail: rechazar peticiones coincidentes

Utilice esta directiva para especificar una plantilla para las peticiones que el servidor no va a procesar. Después de que una petición coincide con una plantilla de una directiva Fail, la petición no se compara con las plantillas de petición de ninguna directiva posterior.

### Formato

```
Fail plantilla_petición [dirección_IP_servidor |  
]
```

*plantilla\_petición*

Especifica una plantilla para las peticiones que el servidor va a rechazar. Si una petición coincide con la plantilla, el servidor envía al solicitante un mensaje de error.

Puede utilizar un asterisco como comodín en la plantilla. El carácter de tilde (~) que aparece justo después de una barra inclinada (/) debe coincidir explícitamente; no se puede utilizar un carácter comodín para que coincida con él.

[*dirección\_IP\_servidor* | ]

Si está utilizando varias direcciones IP o sistemas principales virtuales, utilice este parámetro para especificar una dirección IP o un nombre de sistema principal. El servidor utiliza la directiva sólo para las peticiones que llegan al servidor en esta dirección IP o para este sistema principal. Para una dirección IP, esta es la dirección de la conexión de red del servidor, no la dirección del cliente solicitante.

Puede especificar una dirección IP (por ejemplo, 240.146.167.72 ) o un nombre de sistema principal (por ejemplo, sistppala.bcd.com ).

Este parámetro es opcional. Sin este parámetro, el servidor utiliza la directiva para todas las peticiones, independientemente de la dirección IP en la que entran las peticiones o el nombre de sistema principal del URL.

No puede especificarse un carácter comodín para la dirección IP de un servidor.

### Ejemplos

En el siguiente ejemplo, el servidor rechaza cualquier petición que empiece por `/usr/local/private/`.

```
Fail /usr/local/private/*
```

Los siguientes ejemplos utilizan el parámetro de dirección IP opcional. El servidor rechaza cualquier petición que empiece por `/clienteB/` si la petición entra en una



conexión de red con la dirección IP 240.146.167.72. El servidor rechaza cualquier petición que empiece por /clienteA/ si la petición entra en una conexión de red con la dirección IP 0.83.100.45.

```
Fail    /clienteB/*    240.146.167.72
Fail    /clienteA/*    0.83.100.45
```

Los siguientes ejemplos utilizan el parámetro de nombre de sistema principal opcional. El servidor rechaza cualquier petición que empiece por /clienteB/ si la petición entra para sistppalA.bcd.com. El servidor rechaza cualquier petición que empiece por /clienteA/ si la petición entra para sistppalB.bcd.com.

```
Fail    /clienteB/*    sistppalA.bcd.com
Fail    /clienteA/*    sistppalB.bcd.com
```

### Valor por omisión

Ninguno

## FIPSEnable: cifrados aprobados por FIPS (Enable Federal Information Processing Standard) para SSLV3 y TLS

Utilice esta directiva para habilitar cifrados aprobados por FIPS para los protocolos SSLV3 y TLS en conexiones SSL. Si esta directiva está habilitada, se ignora la lista de especificaciones de cifrado soportadas para SSLV3 (DIRECTIVA V3CipherSpecs). Además, las especificaciones de cifrado TLS permitidas se establecerán en 352F0AFF09FE, y las especificaciones de cifrado de SSLV3 se establecerán en FFFE.

### Formato

```
FIPSEnable {on | off}
```

### Valor por omisión

```
FIPSEnable off
```

## flexibleSocks: habilitar la implementación de SOCKS flexibles

Utilice esta directiva para indicar al proxy que utilice el archivo de configuración SOCKS para determinar el tipo de conexión que desea realizar.

### Formato

```
flexibleSocks {on | off}
```

### Valor por omisión

```
flexibleSocks on
```

## FTPDDirInfo: generar un mensaje descriptivo o de bienvenida de un directorio

Utilice esta directiva para permitir que los servidores FTP generen un mensaje descriptivo o de bienvenida para un directorio. Este mensaje puede visualizarse opcionalmente como parte de los listados FTP. La directiva FTPDirInfo le permite controlar donde se visualizará el mensaje.

### Formato

```
FTPDDirInfo {top | bottom | off}
```

#### top

Muestra el mensaje de bienvenida en la parte superior de la página antes del listado de archivos del directorio.



**bottom**

Muestra el mensaje de bienvenida en la parte inferior de la página después del listado de archivos del directorio.

**off**

No muestra la página de bienvenida.

**Valor por omisión**

FTPDirInfo top

## **ftp\_proxy: especificar otro servidor proxy para las peticiones FTP**

Si el servidor proxy forma parte de una cadena de proxies, utilice esta directiva para especificar el nombre de otro proxy con el que entre en contacto este servidor para obtener las peticiones FTP. Debe especificar un URL completo, incluido el carácter de barra inclinada final (/). Para obtener más información sobre cómo utilizar una plantilla o nombre de dominio opcional, consulte “no\_proxy: especificar las plantillas para conectarse directamente con los dominios” en la página 248.

Sólo se aplica a configuraciones de proxy de reenvío.

**Formato**

```
ftp_proxy URL_completo  
[nombre_dominio_o_plantilla]
```

**Ejemplo**

```
ftp_proxy http:// servidor.proxy.externo/
```

**Valor por omisión**

Ninguno

## **FTPUrlPath: especificar cómo se interpretan los URL de FTP**

Utilice esta directiva para especificar si la información de vía de acceso de los URL de FTP ha de interpretarse como relativa al directorio de trabajo del usuario que ha iniciado la sesión o al directorio raíz.

**Formato**

```
FTPUrlPath {relative | absolute}
```

Si la directiva FTPUrlPath se establece en *absolute*, el directorio de trabajo FTP del usuario que ha iniciado la sesión debe incluirse en la vía de acceso de los URL de FTP. Si se especifica FTPUrlPath *Relative*, el directorio de trabajo de FTP del usuario que ha iniciado la sesión debe omitirse de la vías de acceso de los URL de FTP. Por ejemplo, para acceder al archivo test1.html, que se encuentra en el directorio de trabajo /export/home/user1 de un usuario que ha iniciado la sesión, son necesarias las siguientes vías de acceso de URL en función del valor de la directiva FTPUrlPath:

- Si el valor es FTPUrlPath *absolute*, la vía de acceso de URL necesaria es ftp://ftphost/export/home/user1/test1.html.
- Si el valor es FTPUrlPath *relative*, la vía de acceso de URL necesaria es ftp://ftphost/test1.html.

**Valor por omisión**

Ninguno

## Gc: especificar la recogida de basura

Utilice esta directiva para especificar si se desea utilizar la recogida de basura. Si se habilita la colocación en antememoria, el servidor utiliza el proceso de recogida de basura para suprimir los archivos que ya no deben permanecer en antememoria. Los archivos se suprimen en función de la fecha de caducidad y otros valores de las directivas de proxy. Generalmente, si se habilita la colocación en antememoria, se utiliza la recogida de basura. Si no se utiliza la recogida de basura, la antememoria de proxy se utiliza sin eficacia.

### Formato

Gc {on | off}

### Valor por omisión

Gc On

## GCAadvisor: personalizar el proceso de recogida de basura

Utilice esta directiva para especificar una aplicación personalizada que desea que el servidor utilice para la recogida de basura.

### Formato

GCAadvisor */vía\_acceso/archivo:nombre\_función*

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

### Ejemplo

GCAadvisor /api/bin/customadvise.so:gcadv

## GcHighWater: especificar cuándo empieza la recogida de basura

Utilice esta directiva para especificar el porcentaje de la capacidad de antememoria total que debe rellenarse para desencadenar la recogida de basura. Este porcentaje se llama *marca alta*. La marca alta se especifica como un porcentaje de la capacidad de antememoria total. La recogida de basura continúa hasta que se ha alcanzado la marca baja; consulte “GcLowWater: especificar cuándo termina la recogida de basura” para obtener información sobre cómo se establece ésta. El porcentaje para la marca alta puede establecerse entre 50 y 95.

### Formato

GcHighWater *porcentaje*

### Valor por omisión

GcHighWater 90

## GcLowWater: especificar cuándo termina la recogida de basura

Utilice esta directiva para especificar el porcentaje de la capacidad de antememoria total que desencadena la finalización de la recogida de basura. Este porcentaje se conoce como *marca baja*. La marca baja se especifica como un porcentaje de la capacidad de antememoria total. Debe establecerse en un valor inferior que el

valor establecido para la marca alta; consulte “GcHighWater: especificar cuándo empieza la recogida de basura” en la página 224 para obtener información sobre cómo establecer la marca alta.

### Formato

GcLowWater *porcentaje*

### Valor por omisión

GcLowWater 60

## **gopher\_proxy: especificar otro servidor de proxy para las peticiones Gopher**

Si el servidor proxy forma parte de una cadena de proxies, utilice esta directiva para especificar el nombre de otro proxy con el que entre en contacto este servidor para obtener las peticiones Gopher. Debe especificar un URL completo, incluida la barra inclinada final (/). Para obtener más información sobre cómo utilizar una plantilla o nombre de dominio opcional, consulte “no\_proxy: especificar las plantillas para conectarse directamente con los dominios” en la página 248.

Sólo se aplica a configuraciones de proxy de reenvío.

### Formato

gopher\_proxy  
*URL\_completo*[*nombre\_dominio\_o\_plantilla*]

### Ejemplo

gopher\_proxy http://servidor.proxy.externo/

### Valor por omisión

Ninguno

## **GroupId: especificar el ID de grupo**

Utilice esta directiva para especificar el nombre o número de grupo al que cambia el servidor antes de acceder a los archivos.

Si modifica esta directiva, debe detener y reiniciar el servidor manualmente para que el cambio entre en vigor. El cambio no entra en vigor si únicamente reinicia el servidor. (Consulte el Capítulo 5, “Inicio y detención de Caching Proxy”, en la página 15.)

**Nota:** Si cambia los valores por omisión del servidor para el ID de usuario, el ID de grupo o las vías de acceso de directorios de anotaciones cronológicas, cree los nuevos directorios y actualice los permisos y la propiedad de éstos. Para permitir que el servidor escriba la información en un directorio de anotaciones cronológicas definidas por el usuario, establezca el permiso para ese directorio como 755 y el ID de usuario del servidor definido por el usuario como el propietario. Por ejemplo, si cambia el ID de usuario del servidor del valor por omisión a jdoe y el directorio de anotaciones cronológicas por omisión a server\_root/account, el directorio server\_root/account debe tener el permiso 755 y ser propiedad de jdoe.

### Formato

GroupId { *nombre\_grupo* |  
*número\_grupo*}

### Valores por omisión

AIX: GroupId nobody

HP-UX: GroupId other

#### Linux:

Red Hat: GroupId nobody

SUSE: GroupId nogroup

Solaris: GroupId nobody

## HeaderServerName: especificar el nombre del servidor proxy devuelto en la cabecera HTTP

Utilice esta directiva para especificar el nombre del servidor proxy devuelto en la cabecera HTTP.

### Formato

HeaderServerName *nombre*

### Valor por omisión

Ninguno

## Hostname: especificar el nombre de dominio plenamente cualificado o dirección IP del servidor

Utilice esta directiva para especificar el nombre de dominio o una dirección IP que se devuelve a los clientes desde las peticiones de archivo. Si especifica un nombre de archivo, un servidor de nombres de dominio debe poder resolver el nombre en una dirección IP. Si especifica una dirección IP, el servidor de nombres de dominio no es necesario ni se puede acceder a él.

**Nota:** Cuando se configura una matriz, la directiva Hostname debe configurarse de forma idéntica en todos los miembros de la matriz.

### Formato

Hostname {*nombre* | *dirección IP*}

### Valor por omisión

Por omisión, esta directiva no se especifica en el archivo de configuración inicial. Si no especifica esta directiva en el archivo de configuración, el valor toma el nombre de sistema principal definido en el servidor de nombres de dominio como valor por omisión.

## http\_proxy: especificar otro servidor proxy para las peticiones HTTP

Si el servidor proxy forma parte de una cadena de proxies, utilice esta directiva para especificar el nombre de otro proxy con el que entre en contacto este servidor para obtener las peticiones HTTP. Debe especificar un URL completo, incluida la barra inclinada final (/). Para obtener más información sobre cómo utilizar una plantilla o nombre de dominio opcional, consulte “no\_proxy: especificar las plantillas para conectarse directamente con los dominios” en la página 248.

### Formato

`http_proxy`  
`URL_completo[nombre_dominio_o_plantilla]`

### Ejemplo

`http://servidor.proxy.externo/`

### Valor por omisión

Ninguno

## HTTPSCheckRoot: filtrar las peticiones HTTPS

Utilice esta directiva para especificar si Caching Proxy recupera la página de inicio desprotegida del URL e intenta buscar etiquetas en ella. Si se encuentra alguna etiqueta, éstas se aplican a la petición segura. Por ejemplo, se solicita `https://www.ibm.com/`, Caching Proxy recupera `http://www.ibm.com/`, busca etiquetas en ella y utiliza todas las que encuentra para filtrar `https://www.ibm.com/`.

Si `HTTPSCheckRoot` se establece en `off`, Caching Proxy no recupera la página de inicio desprotegida y busca etiquetas en ella.

### Formato

`HTTPSCheckRoot {on | off}`

### Valor por omisión

`HTTPSCheckRoot on`

## ICP\_Address: especificar la dirección IP para las consultas ICP

Utilice esta subdirectiva para especificar una dirección IP que se utilice para enviar y recibir las consultas ICP. Debe incluirse dentro de las directivas `<MODULEBEGIN> ICP` y `<MODULEEND>`.

### Formato

`ICP_Address dirección_IP`

### Valor por omisión

Por omisión, esta directiva no se especifica en el archivo de configuración inicial. Si no especifica esta directiva en el archivo de configuración, el valor toma la aceptación y el envío de consultas ICP en cualquier interfaz como valor por omisión.

## ICP\_MaxThreads: especificar el número de hebras para las consultas ICP

Utilice esta subdirectiva para especificar el número de hebras generadas para escuchar las consultas ICP. Debe incluirse dentro de las directivas `<MODULEBEGIN> ICP` y `<MODULEEND>`.

**Nota:** En Redhat Linux 6.2 e inferiores, este número debe ser bajo porque el número máximo de hebras que pueden crearse por proceso es pequeño. Es posible que la especificación de un gran número de hebras para que ICP las utilice limite el número de hebras disponibles para su uso en el servicio de las peticiones.

## Formato

ICP\_MaxThreads *número\_de\_hebras*

## Valor por omisión

ICP\_MaxThreads 5

## Occupier: especificar un miembro de un clúster ICP

Si el servidor proxy forma parte de un clúster ICP, utilice esta subdirectiva para especificar los iguales ICP. Debe incluirse dentro de las directivas `<MODULEBEGIN> ICP` y `<MODULEEND>`.

Cuando se añade un nuevo igual al clúster ICP, la información de igual ICP debe añadirse al archivo de configuración de todos los iguales existentes. Utilice una línea para cada igual. Tenga en cuenta que el sistema principal actual también puede incluirse en la lista de iguales. Cuando se inicializa ICP, éste ignora la entrada del sistema principal actual. Esta acción hace posible que exista un único archivo de configuración que se pueda copiar en las demás máquinas de igual sin necesidad de editarlo para eliminar el sistema principal actual.

## Formato

ICP\_Peer *nombre\_sistppal puerto\_http puerto\_icp*

### **nombre\_sistppal**

Nombre del igual

### **puerto\_http**

Puerto proxy del igual

### **puerto\_icp**

Puerto del servidor ICP del igual

## Ejemplo

La siguiente línea añade el sistema principal `abc.xcompany.com`, cuyo puerto proxy es 80 y el puerto ICP 3128 como igual.

```
ICP_Peer abc.xcompany.com 80 3128
```

## Valor por omisión

Ninguno

## ICP\_Port: especificar el número de puerto para las consultas ICP

Utilice esta subdirectiva para especificar el número de puerto en el que el servidor ICP escucha las consultas ICP. Debe incluirse dentro de las directivas `<MODULEBEGIN> ICP` y `<MODULEEND>`.

## Formato

ICP\_Port *número\_puerto*

## Valor por omisión

ICP\_Port 3128

## ICP\_Timeout: especificar el tiempo de espera máximo para las consultas ICP

Utilice esta subdirectiva para especificar el periodo de tiempo máximo durante el que Caching Proxy espera las respuestas a las consultas ICP. Este periodo de

tiempo se especifica en milisegundos. Debe incluirse dentro de las directivas `<MODULEBEGIN> ICP` y `<MODULEEND>`.

### Formato

`ICP_Timeout tiempo_de_espera_en_milisegundos`

### Valor por omisión

`ICP_Timeout 2000`

## IgnoreURL: especificar los URL que no se van a renovar

Utilice esta directiva para especificar los URL que el agente de antememoria no va a cargar. Esta directiva es de gran utilidad cuando el agente de antememoria está cargando páginas enlazadas desde los URL en antememoria. Puede utilizar varias apariciones de la directiva `IgnoreURL` para especificar distintos URL o máscaras de URL. El valor de esta directiva puede contener asteriscos (\*) como comodines para aplicar una máscara.

### Formato

`IgnoreURL URL`

### Ejemplos

`IgnoreURL http://www.yahoo.com/`

`IgnoreURL http://*.ibm.com/*`

### Valor por omisión

`IgnoreURL */cgi-bin/*`

## imbeds: especificar si se va a utilizar el proceso de inclusión de la parte servidor

Utilice esta directiva para especificar si desea que el proceso de inclusión de la parte servidor se realice para los archivos servidos desde el sistema de archivos, los programas CGI o ambos. El proceso de inclusión de la parte servidor se realiza en los archivos con un tipo de contenido de `ext/x-ssi-html`. Opcionalmente, puede especificar que el proceso de inclusión de la parte servidor se realice para los archivos con un tipo de contenido de `text/html`. Para obtener más información sobre los tipos de contenido, consulte “AddType: especificar el tipo de datos de los archivos con sufijos determinados” en la página 185.

Puede utilizar el proceso de inclusión de la parte servidor para insertar dinámicamente información en el archivo que se devuelva. Esta información puede incluir la fecha, el tamaño de un archivo, la última fecha de modificación de un archivo, las variables de entorno CGI o de inclusión de la parte servidor, o archivos de texto. El proceso de inclusión de la parte servidor sólo se realiza en los archivos que se originan localmente. Caching Proxy no realiza el proceso de inclusión de la parte servidor en los objetos en antememoria o que han pasado por el proxy.

El proceso de inclusión de la parte servidor hace que el servidor examine los archivos en busca de mandatos especiales cada vez que se sirven. Esto puede afectar al rendimiento del servidor y ralentizar el tiempo de respuesta a los clientes.

### Formato

`imbeds {on | off | files | cgi | noexec} {SSIOnly | html}`

**on** El proceso de inclusión de la parte servidor se realiza para los archivos del sistema de archivos o de los programas CGI.

**off**

El proceso de inclusión de la parte servidor no se realiza para ningún perfil.

**archivos**

El proceso de inclusión de la parte servidor sólo se realiza para los archivos del sistema de archivos.

**cgi**

El proceso de inclusión de la parte servidor sólo se realiza para los archivos devueltos por los programas CGI.

**noexec**

**SSIOnly**

El proceso de inclusión de la parte servidor se realiza para los archivos con un tipo de contenido de text/x-ssi-html.

**html**

El proceso de inclusión de la parte servidor se realiza para los archivos con un tipo de contenido de text/x-ssi-html.

El servidor comprueba el tipo de contenido de todos los archivos que recupera y la salida de todos los programas CGI que procesa.

El proceso de inclusión de la parte servidor generalmente sólo se realiza para los archivos con un tipo de contenido de text/x-ssi-html. No obstante, puede especificar que los archivos con un tipo de contenido de text/html se procesen para las inclusiones de la parte servidor.

**Nota:** El servidor trata html, .html y .htm como html. El resto se trata como SSIOnly.

Todos los sufijos deben tener una directiva AddType definida con el tipo de contenido correcto. Si utiliza sufijos distintos a .htm o .html, asegúrese de que la directiva AddType se define mediante un tipo de contenido de text/x-ssi/html.

**Valor por omisión**

imbeds on SSIOnly

## **ImportCacheImageFrom: importar la memoria de antememoria de un archivo**

Utilice esta directiva para importar el contenido de antememoria de un archivo de vuelco. Esto es útil cuando la antememoria de memoria se pierde durante el reinicio o al desplegar la misma antememoria para varios proxies.

**Formato**

ImportCacheImageFrom  
*nombre\_archivo\_importación*

**Valor por omisión**

Ninguno



## InheritEnv: especificar qué variables de entorno heredan los programas CGI

Utilice esta directiva para especificar qué variables de entorno desea que los programas CGI hereden, además de las variables de entorno CGI que son específicas del proceso CGI.

Si no incluye una directiva InheritEnv, los programas CGI heredan todas las variables de entorno. Si incluye cualquier directiva InheritEnv, sólo aquellas variables de entorno especificadas en las directivas InheritEnv se heredan junto con las variables de entorno específicas de CGI. La directiva permite inicializar opcionalmente el valor de las variables que se heredan.

### Formato

InheritEnv *variable\_entorno*

### Ejemplos

```
InheritEnv PATH
InheritEnv LANG=ENUS
```

En este ejemplo, las variables de entorno PATH y LANG sólo las heredan los programas CGI y la variable de entorno LANG se inicializa con el valor de ENUS.

### Valor por omisión

Ninguno. Por omisión, los programas CGI heredan todas las variables de entorno.

## InputTimeout: especificar el tiempo de espera de la entrada

Utilice esta directiva para establecer el tiempo permitido para que un cliente envíe una petición después de realizar una conexión con el servidor. Un cliente primero se conecta al servidor y, a continuación, envía una petición. Si el cliente no envía una petición durante el especificado mediante esta directiva, el servidor cierra la conexión. Especifique el valor de tiempo mediante cualquier combinación de horas, minutos (o mins) y segundos (o secs).

### Formato

InputTimeout *tiempo*

### Ejemplo

```
InputTimeout 3 mins 30 secs
```

### Valor por omisión

```
InputTimeout 2 minutes
```

## JunctionReplaceUrlPrefix: sustituir el URL en lugar de insertar un prefijo cuando se utiliza con el plug-in JunctionRewrite

Esta directiva sobrescribirá la acción por omisión del plug-in JunctionRewrite, lo que permitirá que el proxy corrija ciertos enlaces URL de la página html. Se utiliza junto con la directiva JunctionRewrite.

Sólo se aplica a configuraciones de proxy de retorno.

La directiva JunctionReplaceUrlPrefix indicará al plug-in JunctionRewrite que cambie el URL de *patrón\_url\_1* a *patrón\_url\_2*, en lugar de insertar un prefijo al principio del URL.

## Formato

`JunctionReplaceUrlPrefix patrón_url_1 patrón_url_2`

## Ejemplo

`JunctionReplaceUrlPrefix /server1.internaldomain.com/* /server1/*`

En este ejemplo, asuma que el URL es `/server1.internaldomain.com/notes.nsf` y que el prefijo es `/server1`. En lugar de insertar el prefijo para reescribir el URL como `/server1/server1.internaldomain.com/notes.nsf`, el plug-in `JunctionRewrite` plug-in cambiará el URL a `/server1/notes.nsf`.

## Valor por omisión

Ninguno

## JunctionRewrite: habilitar la reescritura de URL

Esta directiva habilita la rutina de reescritura de unión en Caching Proxy para reescribir las respuestas de los servidores de origen para garantizar que los URL relativos al servidor se correlacionen correctamente con el servidor de origen correcto cuando se utilizan uniones.

Sólo se aplica a configuraciones de proxy de retorno.

El plug-in de reescritura de unión también debe habilitarse si establece **JunctionRewrite on** sin la opción `UseCookie`. Las uniones se definen mediante normas de correlación del proxy.

Consulte “`UseCookie` como alternativa a `JunctionRewrite`” en la página 49 y “Ejemplo de plug-in de transformación rápida para ampliar la funcionalidad de `JunctionRewrite`” en la página 50 para obtener información adicional sobre `JunctionRewrite`.

## Formato

`JunctionRewrite {on | on UseCookie | off}`

## Valor por omisión

`JunctionRewrite off`

## JunctionRewriteSetCookiePath: reescribir la opción de vía de acceso en la cabecera Set-Cookie cuando se utiliza con el plug-in JunctionRewrite

La directiva permitirá al proxy reescribir la opción de vía de acceso en la cabecera `Set-Cookie` cuando se produzca una coincidencia con el nombre de cookie. Si la respuesta necesita uniones y no se ha definido un prefijo de uniones, el prefijo insertará delante de todas las vías de acceso. Puede utilizarse con el plug-in `JunctionRewrite` o puede utilizarse con la directiva `RewriteSetCookieDomain`.

Sólo se aplica a configuraciones de proxy de retorno.

## Formato

`JunctionRewriteSetCookiePath  
nombre-cookie1 nombre-cookie2...`

`nombre-cookie`

Nombre de cookie de una cabecera `Set-Cookie`.

### Valor por omisión

Ninguno

## **JunctionSkipUrlPrefix: omitir la reescritura de los URL que ya contienen el prefijo cuando se utiliza con el plug-in JunctionRewrite**

Esta directiva sobrescribirá la acción por omisión del plug-in JunctionRewrite, lo que evitará la reescritura de URL si ya hay coincidencia con patrón de URL. Funciona con el plug-in JunctionRewrite plug-in y proporciona un modo de corregir algunos de los enlaces URL de la página URL. Generalmente, la directiva se utiliza para evitar los URL que ya incluyen un prefijo.

Sólo se aplica a configuraciones de proxy de retorno.

### Formato

`JunctionSkipUrlPrefix patrón_url`

### Ejemplo

`JunctionSkipUrlPrefix /server1/*`

En este ejemplo, asuma que el URL es `/server1/notes.nsf` y que el prefijo de unión es `/server1/`. En lugar de reescribir el URL como `/server1/server1/notes.nsf`, el plug-in JunctionRewrite plug-in omitirá la reescritura del URL, que permanecerá sin modificar como `/server1/notes.nsf`.

### Valor por omisión

Ninguno

## **KeepExpired: especificar la devolución de la copia caducada del recurso si se está actualizando el recurso en el proxy**

Utilice esta directiva para impedir que los servidores de programa de fondo se vean saturados con peticiones mientras se vuelve a validar un objeto de antememoria.

Cuando se vuelve a validar un objeto de antememoria con el contenido del servidor de programa de fondo, las peticiones de ese mismo recurso se enviarán al servidor de programa de fondo a través del proxy. En ocasiones, la avalancha de peticiones iguales provocará la caída del servidor del programa de fondo. Habilitar esta directiva puede ayudar a evitar que se produzca esta situación. Si la directiva está habilitada, se devolverán las copias caducadas u obsoletas del recurso si el recurso se está actualizando en el proxy.

### Formato

`KeepExpired {on | off}`

### Valor por omisión

`KeepExpired off`

## KeyRing: especificar la vía de acceso del archivo a la base de datos de conjunto de claves

Utilice esta directiva para especificar la vía de acceso del archivo a la base de datos de conjunto de claves que el servidor utiliza para las peticiones SSL. Los archivos de conjunto de claves se generan mediante el programa de utilidad del gestor de claves iKeyman.

**Nota:** Las directivas SSL no reciben soporte en SUSE Linux.

### Formato

`KeyRing nombre_archivo`

### Ejemplos

**Windows:** `KeyRing c:\Archivos de programa\IBM\edge\cp\key.kdb`

**Linux y UNIX:** `KeyRing /etc/key.kdb`

### Valor por omisión

Ninguno

## KeyRingStash: especificar la vía de acceso del archivo al archivo de contraseñas de la base de datos de conjunto de claves

Utilice esta directiva para especificar la vía de acceso del archivo al archivo de contraseñas de la base de datos de conjunto de claves. El archivo de contraseñas se genera mediante el programa de utilidad del gestor de claves iKeyman cuando se crea un archivo de base de datos de conjunto de claves.

**Nota:** Las directivas SSL no reciben soporte en SUSE Linux.

### Formato

`KeyRingStash vía_acceso_archivo`

### Ejemplos

**Windows:** `KeyRingStash c:\Archivos de programa\IBM\edge\cp\key.sth`

**Linux y UNIX:** `KeyRingStash /etc/key.sth`

### Valor por omisión

Ninguno

## LimitRequestBody: especificar el tamaño máximo de cuerpo de las peticiones PUT o POST

Utilice esta directiva para controlar el tamaño máximo del cuerpo de las peticiones PUT o POST. Las directivas LimitRequest se utilizan para proteger al proxy de posibles ataques.

El valor puede especificarse en kilobytes (K), megabytes (M) o gigabytes (G).

### Formato

`LimitRequestBody`  
`tamaño_cuerpo_máximo {K | M | G}`

### Valor por omisión

`LimitRequestBody 10 M`

## LimitRequestFields: especificar el número máximo de cabeceras de las peticiones de cliente

Utilice esta directiva para especificar el número máximo de cabeceras que se pueden enviar en las peticiones de cliente. Las directivas `LimitRequest` se utilizan para proteger al proxy de posibles ataques.

### Formato

`LimitRequestFields número_cabeceras`

### Valor por omisión

`LimitRequestFields 32`

## LimitRequestFieldSize: especificar la longitud máxima de cabecera y de la línea de petición

Utilice esta directiva para especificar la longitud máxima de la línea de petición y de todas las cabeceras de una petición. Las directivas `LimitRequest` se utilizan para proteger al proxy de posibles ataques.

El valor puede especificarse en bytes (B) o kilobytes (K).

### Formato

`LimitRequestFieldSize`  
`longitud_máx_cabeceras {B | K}`

### Valor por omisión

`LimitRequestFieldSize 4096 B`

## ListenBacklog: especificar el número de conexiones de cliente del registro de reserva de escucha que puede transportar el servidor

Utilice esta directiva para especificar el número de conexiones de cliente del registro de reserva de escucha que el servidor transporta antes de enviar mensajes de conexiones rechazadas a los clientes. Este número depende del número de peticiones que el servidor puede procesar en pocos segundos. No lo establezca en un valor superior al número que el servidor puede procesar antes de que finalice el tiempo de espera de los clientes y éstos terminen anormalmente la conexión.

**Nota:** Si el valor `ListenBacklog` es superior al valor `SOMAXCONN` soportado por TCP/IP, se utiliza este último en su lugar.

### Formato

`ListenBacklog`  
`número_de_peticiones`

### Valor por omisión

`ListenBacklog 128`

## LoadInlineImages: controlar la renovación de imágenes anidadas

Utilice esta directiva para especificar si el agente de antememoria debe recuperar las imágenes en línea. Si LoadInlineImages se establece en on, también se colocarán en antememoria las imágenes que estén anidadas en una página que se esté colocando en antememoria. Si se establece en off, las imágenes anidadas no se colocan en antememoria.

### Formato

LoadInlineImages {on | off}

### Valor por omisión

LoadInlineImages on

## LoadTopCached: especificar el número de páginas más solicitadas que se van a renovar

Utilice esta directiva para indicar al agente de antememoria que acceda a las anotaciones cronológicas de acceso a la antememoria de la noche anterior y cargue los URL más solicitados.

La directiva Caching debe establecerse en On y debe establecerse un valor para la directiva CacheAccessLog cuando se establece un valor para la directiva LoadTopCached.

### Formato

LoadTopCached *número\_de\_páginas*

### Valor por omisión

LoadTopCached 100

## LoadURL: especificar los URL que se van a renovar

Utilice esta directiva para especificar los URL que se desea cargar en la antememoria mediante el agente de antememoria. Pueden incluirse varias directivas LoadURL en el archivo de configuración, pero no se pueden utilizar los caracteres comodín.

### Formato

LoadURL *url*

### Ejemplo

LoadURL http://www.ibm.com/

### Valor por omisión

Ninguno

## Log: personalizar el paso de anotación cronológica

Utilice esta directiva para especificar una función de aplicación personalizada a la que el servidor llama durante el paso de anotación cronológica. Este código proporciona el registro cronológico y demás procesos que se realizan después de cerrar la conexión.

### Formato

Log *plantilla\_petición /vía\_acceso/archivo:nombre\_función*

#### *plantilla\_petición*

Especifica una plantilla para las peticiones que determinan adicionalmente si se llama a la función de aplicación. La especificación puede incluir el protocolo, el dominio y el sistema principal; puede estar precedida por una barra inclinada (/), y puede utilizar un asterisco (\*) como carácter comodín. Por ejemplo, /front\_page.html , http://www.ics.raleigh.ibm.com, /pub\*, /\* y \* son todas válidas.

#### */vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

#### *nombre\_función*

Especifica el nombre de la función de aplicación del programa. Debe proporcionar los nombres de las funciones open, write y close.

### **Ejemplo**

Log /index.html /api/bin/icsextpgm.so:log\_url

### **Valor por omisión**

Ninguno

## **LogArchive: especificar el comportamiento del archivado de las anotaciones cronológicas**

Utilice esta directiva para especificar el comportamiento de la rutina de archivado. Esta directiva afecta a todas las anotaciones cronológicas con valores globales. Especifica que las anotaciones cronológicas deben comprimirse o depurarse, o que no se realice nada con ellas.

Si especifica Compress, utilice las directivas CompressAge y CompressDeleteAge para especifica cuando se comprimen o se suprimen las anotaciones cronológicas. Utilice la directiva CompressCommand para especificar qué mandato y sus parámetros deben utilizarse.

Si especifica Purge, utilice las directivas PurgeAge y PurgeSize para especificar cuando se desea depurar las anotaciones cronológicas.

### **Formato**

LogArchive {Compress | Purge | none}

#### **Compress**

Especifica que la rutina de archivado comprima las anotaciones cronológicas.

#### **Purge**

Especifica que la rutina de archivado borre las anotaciones cronológicas.

#### **none**

Especifica que la rutina de archivado no realice nada.

### **Valor por omisión**

LogArchive Purge

### **Directivas relacionadas**

- “CompressAge: especificar cuándo comprimir las anotaciones cronológicas” en la página 202
- “CompressDeleteAge: especificar cuándo suprimir las anotaciones cronológicas” en la página 204

- “CompressCommand: especificar el mandato y los parámetros de compresión” en la página 203
- “Midnight: especificar el plug-in de API utilizado para archivar las anotaciones cronológicas” en la página 246
- “PurgeAge: especificar el límite de antigüedad para las anotaciones cronológicas” en la página 271
- “PurgeSize: especificar el límite del tamaño del archivador de anotaciones cronológicas” en la página 272

## LogFileFormat: especificar el formato de las anotaciones cronológicas de acceso

Utilice esta directiva para especificar el formato de archivo de los archivos de anotaciones cronológicas de acceso.

### Formato

```
LogFileFormat {common | combined}
```

Por omisión, las anotaciones cronológicas se muestran en el formato de archivo de anotaciones cronológicas común de NCSA. Especifique `combined` para mostrar las anotaciones cronológicas en el formato de archivo de anotaciones cronológicas combinado de NCSA. El formato combinado añade campos para el URL de referencia, el agente de usuario y el cookie (si aparecen en la petición).

### Valor por omisión

```
LogFileFormat common
```

## LogToGUI (Windows sólo): visualizar las entradas de anotaciones cronológicas en la ventana del servidor

**Sistema Windows sólo.** Al ejecutar el proxy mediante la línea de mandatos, utilice esta directiva para que se envíe la salida a las anotaciones cronológicas de acceso. Para optimizar el rendimiento del servidor, esta directiva se establece en `off` (inhabilitado) por omisión.

**Nota:** Esta directiva no tiene ningún efecto al ejecutarse el proxy como un servicio.

### Formato

```
LogToGUI {on | off}
```

### Valor por omisión

```
LogToGUI off
```

## LogToSyslog: especificar si se va a enviar la información de acceso a las anotaciones cronológicas del sistema (Linux y UNIX sólo)

**Sistemas Linux y UNIX sólo.** Utilice esta directiva para especificar si el servidor va a anotar cronológicamente las peticiones y errores de acceso en las anotaciones cronológicas del sistema además de en los archivos de anotaciones cronológicas de error y de acceso.

### Formato

```
LogToSyslog {on | off}
```



El archivo de anotaciones cronológicas de error debe estar presente en el servidor antes de especificar que la información de anotaciones cronológicas de error se escriba en él. Puede escoger si desea anotar cronológicamente la información de acceso, la información de error o ambas.

Para enviar sólo la información de error a las anotaciones cronológicas del sistema, añada la siguiente línea al archivo `/etc/syslog.conf`:

```
user.err
archivo_salida_syslog_para_información_errores
```

Para enviar sólo la información de acceso a las anotaciones cronológicas del sistema, añada la siguiente línea al archivo `/etc/syslog.conf`:

```
user.info
archivo_info_syslog_para_información_acceso
```

Para enviar la información de error y la información de acceso a las anotaciones cronológicas del sistema, añada ambas líneas al archivo `/etc/syslog.conf`:

Especifique `archivo_salida_syslog` y `archivo_info_syslog` en los siguientes formatos:

- **AIX:** `/var/adm/nombre_de_archivo_syslog`
- **HP-UX:** `/var/adm/syslog/syslog.log`
- **Linux:** `/var/adm/messages`
- **Solaris:** `/var/adm/messages`

Después de crear el archivo de anotaciones cronológicas del sistema, puede reiniciarlo con el siguiente mandato:

```
kill -HUP 'cat /etc/syslog.pid'
```

### Valor por omisión

```
LogToSyslog Off
```

## Map — Cambiar las peticiones coincidentes a una nueva serie de petición, utilizando la serie de vía de acceso de petición para cumplir la regla

Utilice esta directiva para especificar una plantilla para las peticiones que desea cambiar a una nueva serie de petición. Después de que el servidor modifica la petición, éste toma la nueva serie de petición y la compara con las plantillas de petición de las directivas posteriores.

La directiva Map utiliza la serie de la vía de acceso de petición entrante para cumplir la regla. Consulte también “MapQuery — Cambiar las peticiones coincidentes a una nueva serie de petición, utilizando la serie de vía de acceso de petición y consulta para cumplir la regla” en la página 241.

### Formato

```
Map plantilla_petición petición_nueva [dirección_IP_servidor | ]
```

*plantilla\_petición*

Especifica una plantilla para las peticiones que modifica el servidor, el cual compara posteriormente la nueva serie de petición con las demás plantillas.

Puede utilizar un asterisco (\*) como comodín en la plantilla. El carácter de tilde (~) que aparece justo después de una barra inclinada (/) debe coincidir explícitamente; no se puede utilizar un carácter comodín para que coincida con él.

### *nueva\_petición*

Especifica la nueva serie de petición con la que el servidor sigue comparando las plantillas de petición en las directivas posteriores. La serie especificada con *nueva\_petición* puede contener un carácter de comodín si *plantilla\_petición* tiene uno. La parte de la petición que coincide con el comodín de *plantilla\_petición* se inserta en lugar del comodín de *nueva\_petición*.

### [*dirección\_IP\_servidor* | *nombre\_sistppal*]

Si está utilizando varias direcciones IP o sistemas principales virtuales, utilice este parámetro para especificar una dirección IP o un nombre de sistema principal. El servidor utiliza la directiva sólo para las peticiones que llegan al servidor en esta dirección IP o para este sistema principal. Para una dirección IP, esta es la dirección de la conexión de red del servidor, no la dirección del cliente solicitante.

Puede especificar una dirección IP (por ejemplo, 240.146.167.72 ) o un nombre de sistema principal (por ejemplo, sistppalA.raleigh.ibm.com).

Este parámetro es opcional. Sin este parámetro, el servidor utiliza la directiva para todas las peticiones, independientemente de la dirección IP en la que entran las peticiones o el nombre de sistema principal del URL.

No puede especificarse un carácter comodín para la dirección IP de un servidor.

## Ejemplos

- En el siguiente ejemplo, el servidor toma todas las peticiones que empiezan por /stuff/ y cambia la parte /stuff/ de las peticiones a /good/stuff/. Todo lo que aparezca después de /stuff/ en la petición original también se incluye en la nueva serie de petición. Por lo tanto, /stuff/whatsup/ cambia a /good/stuff/whatsup/. El servidor toma la nueva serie de petición y seguidamente la compara con las plantillas de petición de directivas posteriores.

```
Map /stuff/* /good/stuff/*
```

- Los siguientes ejemplos utilizan el parámetro de dirección IP opcional. Si el servidor recibe peticiones que empiezan por /stuff/, cambia la petición a una serie de petición distinta basándose en la dirección IP de la conexión de red en la que entra la petición. Para las peticiones que entran en 240.146.167.72, el servidor cambia la parte /stuff/ de la petición a /clienteA/good/stuff/. Para las peticiones que entran en cualquier conexión con una dirección de 0.83.100.45, el servidor cambia la parte /stuff/ de la petición a /clienteB/good/stuff/.

```
Map /stuff/* /clienteA/good/stuff/* 240.146.167.72
```

```
Map /stuff/* /clienteB/good/stuff/* 0.83.100.45
```

- Los siguientes ejemplos utilizan el parámetro de nombre de sistema principal opcional. Si el servidor recibe peticiones que empiezan por /stuff/, cambia la petición a una serie de petición distinta basándose en el nombre de sistema principal del URL. Para las peticiones que entran para sistppalA, el servidor cambia la parte /stuff/ de la petición a /clienteA/good/stuff/. Para las peticiones que entran para sistppalB, el servidor cambia la parte /stuff/ de la petición a /clienteB/good/stuff/.

```
Map /stuff/* /clienteA/good/stuff/* sistppalA.bcd.com
```

```
Map /stuff/* /clienteB/good/stuff/* sistppalB.bcd.com
```

## Valor por omisión

Ninguno

## MapQuery — Cambiar las peticiones coincidentes a una nueva serie de petición, utilizando la serie de vía de acceso de petición y consulta para cumplir la regla

Utilice esta directiva para especificar una plantilla para las peticiones que desea cambiar a una nueva serie de petición. Después de que el servidor modifica la petición, éste toma la nueva serie de petición y la compara con las plantillas de petición de las directivas posteriores.

La funcionalidad de la directiva es casi idéntica a la de la regla Map (“Map — Cambiar las peticiones coincidentes a una nueva serie de petición, utilizando la serie de vía de acceso de petición para cumplir la regla” en la página 239). Sin embargo, para manejar un URL con una serie de consulta, MapQuery utiliza la vía de acceso y la serie de consulta para cumplir la regla. Si el URL cumple una regla MapQuery, se utilizará el URL traducido para cumplir el resto de las reglas.

MapQuery también puede traducir un URL con una serie de consulta a otro URL con una vía de acceso o una serie de consulta distinta. Sin embargo, debido a que todas las demás directivas de correlación sólo utilizan la vía de acceso de petición, la serie de consulta modificada sólo se añadirá (no se utilizará para patrones de coincidencia) al URL traducido cuando coincida la vía de acceso de petición.

### Formato

MapQuery *plantilla\_petición* *petición\_nueva*  
[*dirección\_IP\_servidor* | ]

#### *plantilla\_petición*

Especifica una plantilla para las peticiones que modifica el servidor, el cual compara posteriormente la nueva serie de petición con las demás plantillas.

Puede utilizar un asterisco (\*) como comodín en la plantilla. El carácter de tilde (~) que aparece justo después de una barra inclinada (/) debe coincidir explícitamente; no se puede utilizar un carácter comodín para que coincida con él.

#### *nueva\_petición*

Especifica la nueva serie de petición con la que el servidor sigue comparando las plantillas de petición en las directivas posteriores. La serie especificada con *nueva\_petición* puede contener un carácter de comodín si *plantilla\_petición* tiene uno. La parte de la petición que coincide con el comodín de *plantilla\_petición* se inserta en lugar del comodín de *nueva\_petición*.

#### [*dirección\_IP\_servidor* | *nombre\_sistppal*]

Si está utilizando varias direcciones IP o sistemas principales virtuales, utilice este parámetro para especificar una dirección IP o un nombre de sistema principal. El servidor utiliza la directiva sólo para las peticiones que llegan al servidor en esta dirección IP o para este sistema principal. Para una dirección IP, esta es la dirección de la conexión de red del servidor, no la dirección del cliente solicitante.

Puede especificar una dirección IP (por ejemplo, 240.146.167.72 ) o un nombre de sistema principal (por ejemplo, sistppalA.raleigh.ibm.com).

Este parámetro es opcional. Sin este parámetro, el servidor utiliza la directiva para todas las peticiones, independientemente de la dirección IP en la que entran las peticiones o el nombre de sistema principal del URL.

No puede especificarse un carácter comodín para la dirección IP de un servidor.

## Ejemplos

Suponiendo que el URL entrante es el siguiente,  
`/getsomthing?type=1`

y que la regla MapQuery es la siguiente,  
`MapQuery /getsomthing?type=* /gettype/*`

El URL traducido será `/gettype/1` y se utilizará en la siguiente correlación de regla.

`Proxy /gettype/* http://server/gettype/*`

El URL traducido será `http://server/gettype/1`.

## Valor por omisión

Ninguno

## MaxActiveThreads: especificar el número máximo de hebras activas

Utilice esta directiva para establecer el número máximo de hebras que estarán activas simultáneamente. Si se alcanza este máximo, el servidor retiene las nuevas peticiones hasta que termina otra petición y las hebras están disponibles. Generalmente, cuanto más potencia tiene una máquina, mayor es el valor que se establece para esta directiva. Si una máquina empieza a pasar demasiado tiempo realizando tareas de actividad adicional como, por ejemplo, el intercambio de memorias intente reducir este valor.

### Formato

`MaxActiveThreads`  
*número\_de\_hebras*

### Valor por omisión

`MaxActiveThreads 100`

## MaxContentLengthBuffer: especificar el tamaño del almacenamiento intermedio para los datos dinámicos

Utilice esta directiva para establecer el tamaño del almacenamiento intermedio de los datos dinámicos generados por el servidor. Son datos dinámicos la salida de los programas CGI, las inclusiones de la parte servidor y los programas de API.

El valor puede especificarse en bytes (B), kilobytes (K), megabytes (M) o gigabytes (G). No importa si hay un espacio entre el número y el valor (B, K, M, G).

### Formato

`MaxContentLengthBuffer` *tamaño*

### Valor por omisión

`MaxContentLengthBuffer 100 K`

## MaxLogFileSize: especificar el tamaño máximo para todos los archivos de anotaciones cronológicas

Utilice esta directiva para especificar el tamaño máximo de todos los archivos de anotaciones cronológicas. Todos los archivos de anotaciones cronológicas no pueden sobrepasar el tamaño definido por esta directiva. Una vez que un archivo

de anotaciones cronológicas alcanza el tamaño máximo definido, se cierra el archivo de anotaciones cronológicas actual y se crea uno nuevo con el mismo nombre añadido por el siguiente valor entero incremental.

**Notas:**

1. Caching Proxy es una aplicación de 32 bits y abre los archivos de anotaciones cronológicas con una función de 32 bits. Debido a esta restricción, *no* especifique un valor de MaxLogFileSize mayor que 2 GB. Caching Proxy puede colgarse si el archivo de anotaciones cronológicas excede los 2 GB de tamaño cuando Caching Proxy intente escribir en el archivo de anotaciones cronológicas mientras todavía esté procesando activamente las peticiones.
2. En las plataformas Linux y UNIX, los archivos de anotaciones cronológicas no se crearán si el directorio donde residen los archivos de anotaciones cronológicas no tiene definidos permisos de escritura al menos para el grupo bajo en el que se ejecuta el daemon como mínimo. En otras palabras, las ubicaciones de los archivos de anotaciones cronológicas para las directivas de registro cronológico del archivo ibmproxy.conf deben tener permisos de lectura para el grupo definido por la directiva GroupId del archivo ibmproxy.conf como mínimo. Esta situación sólo es un problema cuando se ha modificado la ubicación por omisión de los archivos de anotaciones cronológicas o se han modificado las directivas UserId o GroupId por omisión en el archivo ibmproxy.conf.

El valor recomendado para establecer la directiva MaxLogFileSize es como mínimo de 10 M, pero de menos de 200 M. El tamaño real del archivo de anotaciones cronológicas es ligeramente superior al tamaño que ha establecido. Establecer un valor demasiado bajo afecta al rendimiento del proxy, porque el servidor proxy cierra y abre el archivo de anotaciones cronológicas más a menudo. En algunas plataformas, establecer un valor demasiado alto hace que el proxy utilice memoria para almacenamiento intermedio de E/S. Cuando el tamaño del archivo de anotaciones cronológicas se vuelve más grande, puede hacer que el proxy agote la memoria o aparente una pérdida de memoria, aunque el sistema operativo controle los almacenamientos intermedios de E/S.

El tamaño máximo puede especificarse en cualquiera de las siguientes unidades: bytes (B), kilobytes (K), megabytes (M) y gigabytes (G).

**Formato**

MaxLogFileSize *máximo* {B | K | M | G}

**Valor por omisión**

MaxLogfileSize 128 M

## **MaxPersistRequest: especificar el número máximo de peticiones que se van a recibir en una conexión persistente**

Utilice esta directiva para especificar el número máximo de solicitantes que el servidor recibe en una conexión persistente. Al determinar este número, tenga en cuenta el número de imágenes utilizado en las páginas. Cada imagen requiere una petición independiente.

**Formato**

MaxPersistRequest *número*

**Valor por omisión**

MaxPersistRequest 5

## MaxQueueDepth: especificar el número máximo de los URL que se van a colocar en cola

Utilice esta directiva para especificar la profundidad máxima de la cola de peticiones de recuperación de página pendientes del agente de antememoria. Si tiene un sistema de tamaño considerable con una gran cantidad de memoria, puede definir una cola de peticiones de recuperación de páginas mayor sin consumir toda la memoria disponible.

La cola de los URL que se va a colocar en antememoria se determina al principio de todas las ejecuciones del agente de antememoria. Si indica al agente de antememoria que siga los enlaces de hipertexto a otros URL, estos URL no se cuentan en la profundidad de la cola de antememoria. Después de que se alcance el valor especificado en la directiva MaxURLs, el agente de antememoria se detiene, incluso si quedan más URL en la cola.

### Formato

MaxQueueDepth *longitud\_máxima*

### Valor por omisión

MaxQueueDepth 250

## MaxRuntime: especificar el tiempo máximo de ejecución de un agente de antememoria

Utilice esta directiva para especificar el periodo máximo de tiempo para que el agente de antememoria recupere los URL durante una ejecución determinada. Un valor de 0 significa que el agente de antememoria se ejecuta hasta que se complete.

### Formato

MaxRuntime {0 | *tiempo\_máximo*}

### Ejemplo

MaxRuntime 2 hours 10 minutes

### Valor por omisión

MaxRuntime 2 hours

## MaxSocketPerServer — Especificar el número máximo de sockets desocupados abiertos para el servidor

Utilice esta directiva para establecer el número máximo de sockets desocupados abiertos que mantener para cualquier servidor de origen. Utilice esta directiva sólo si la directiva ServerConnPool está establecida en on.

### Formato

MaxSocketPerServer *núm*

### Ejemplo

MaxSocketPerServer 10

### Valor por omisión

MaxSocketPerServer 5

## MaxUrls: especificar el número máximo de los URL que se van a renovar

Utilice esta directiva para especificar el número máximo de los URL que el agente de antememoria recupera durante una ejecución determinada. Un valor de 0 significa que no hay ningún límite. Cuando se utiliza la modalidad automática del agente de antememoria, las directivas LoadURL y LoadTopCached tienen prioridad ante MaxURLs.

### Formato

MaxURLs *número\_máximo*

### Valor por omisión

MaxURLs 2000

## Member: especificar un miembro de una matriz

Utilice esta directiva para especificar los miembros de las matrices que comparten los servidores mediante el acceso a antememoria remota.

**Nota:** Al configurar una matriz, configure la directiva Hostname en todos los miembros de esa matriz de modo idéntico.

### Formato

```
Member nombre {  
  subdirectiva  
  subdirectiva  
  .  
  .  
}
```

Se incluyen las siguientes subdirectivas:

#### RCAAddr

Esta subdirectiva obligatoria identifica la dirección IP o el nombre de sistema principal para la comunicación RCA.

#### RCAPort

Esta subdirectiva obligatoria identifica el puerto para la comunicación RCA. El número de puerto debe ser mayor que 1024 y menor que 65535.

#### CacheSize {*n bytes* | *n Kbytes* | *n Mbytes* | *n Gbytes*}

Esta subdirectiva obligatoria identifica el tamaño de la antememoria de este miembro, que debe ser un valor positivo.

#### [Timeout *n milliseconds* | *n seconds* | *n hours* | *n days* | *n months* | *n years* | **forever**]

Identifica cuánto tiempo se debe esperar a este miembro. *n* debe ser un entero positivo. Timeout es opcional. El valor por omisión es 1000 milliseconds. Los valores del tiempo de espera generalmente se establecen en segundos o milisegundos.

#### [BindSpecific {**on** | **off**}]

Permite que las comunicaciones se realicen en una subred privada proporcionando alguna medida de seguridad. BindSpecific es opcional; el valor por omisión es On.

#### [ReuseAddr {**on** | **off**}]

Permite que se vuelva a unir la matriz con más rapidez. Su establecimiento en On permite que otros procesos roben el puerto, que puede provocar un comportamiento indefinido. ReuseAddr es opcional. El valor por omisión es Off.



## Ejemplo

```
Member bittersweet.chocolate.ibm.com {  
  RCAAddr      127.0.0.1  
  RCAPort      6294  
  CacheSize    25G  
  Timeout      500 milliseconds  
  BindSpecific On  
  ReuseAddr    Off  
}
```

## Valor por omisión

Ninguno

## Midnight: especificar el plug-in de API utilizado para archivar las anotaciones cronológicas

Utilice esta directiva para especificar el plug-in de aplicación que se ejecuta a medianoche para archivar las anotaciones cronológicas. Esta directiva se inicializa durante la instalación. Si no incluye esta directiva en el archivo de configuración, no se realizan las funciones de archivado.

### Formato

Midnight */vía\_acceso/archivo:nombre\_función*

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

### Valores por omisión

- **Linux y UNIX:** Midnight /usr/lib/archive.so:begin
- **Windows:** Midnight C:\Archivos de programa\IBM\edge\cp\\bin\archive.dll:begin

## NameTrans: personalizar el paso de traducción de nombres

Utilice esta directiva para especificar una función de aplicación personalizada a la que el servidor llama durante el paso de traducción de nombre. Este código proporciona el mecanismo para traducir la vía de acceso virtual de la petición a la vía de acceso física del servidor, lo que permite correlacionar los URL a objetos específicos.

**Nota:** No se trata de una norma de correlación de terminal. El URL transformado debe coincidir a continuación con una de las directivas de norma de correlación de terminal como, por ejemplo, Exec, Fail, Map, Pass, Redirect y Service.

### Formato

NameTrans *plantilla\_petición* */vía\_acceso/archivo:nombre\_función*  
[*dirección\_IP\_servidor* | ]

*plantilla\_petición*

Especifica una plantilla para las peticiones que determinan adicionalmente si se llama a la función de aplicación. La especificación puede incluir el protocolo, el dominio y el sistema principal; puede estar precedida por una barra inclinada



(/), y puede utilizar un asterisco (\*) como carácter comodín. Por ejemplo, /front\_page.html , http://www.ics.raleigh.ibm.com, /pub\*, /\* y \* son todas válidas.

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

*[dirección\_IP\_servidor | ]*

Si está utilizando varias direcciones IP o sistemas principales virtuales, determina si sólo se llama a la función de aplicación para las peticiones que entren en una dirección IP específica o para un sistema principal específico.

No puede especificarse un carácter comodín para la dirección IP de un servidor.

**Nota:** La directiva debe escribirse en una línea, aunque aquí se muestre en dos líneas por razones de claridad.

### Ejemplo

NameTrans /index.html /api/bin/icsextpgm.so:trans\_url

### Valor por omisión

Ninguno

## NoBG: ejecutar el proceso de Caching Proxy en primer lugar

En las plataformas Linux y UNIX, utilice esta directiva para evitar que el proceso de servidor de Caching Proxy se ejecute automáticamente de fondo. La directiva, que se establece en off por omisión, tiene el siguiente formato:

NoBG [on | off]

**Nota:** La opción **-nobg** del mandato **ibmproxy** no es válida para los sistemas Windows.

### Ejemplo

NoBG on

### Valor por omisión

NoBG off

## NoCaching: especificar que no se coloquen en antememoria los archivos con los URL que coinciden con una plantilla

Utilice esta directiva para especificar que el servidor no coloque en antememoria los archivos con los URL que coincidan con la plantilla especificada. Puede incluir varias apariciones de esta directiva en el archivo de configuración. Incluya una directiva separada para cada plantilla. La plantilla de URL debe incluir el protocolo.

Si no están establecidas las directivas CacheOnly ni NoCaching, cualquier URL es un candidato para la colocación en antememoria.

### Formato

NoCaching *patrón\_URL*

### Ejemplo

NoCaching http://joke/\*

### Valor por omisión

Ninguno

## NoLog: suprimir las entradas de anotaciones cronológicas de los sistemas principales o dominios específicos que coinciden con una plantilla

Utilice esta directiva para especificar que no coloque en antememoria las peticiones de acceso realizadas desde sistemas principales o dominios específicos que coincidan con una plantilla especificada. Por ejemplo, es posible que no desee anotar cronológicamente las peticiones de acceso de los sistemas principales locales.

Puede incluir varias apariciones de esta directiva en el archivo de configuración. Asimismo, puede colocar varias plantillas en la misma directiva si las separa por uno o más espacios. Puede utilizar los nombres de sistema principal o direcciones de número IP en las plantillas.

**Nota:** Para utilizar las plantillas de nombre de sistema principal, debe establecer la directiva DNS-Lookup en On. Si la directiva DNS-Lookup se establece en Off (valor por omisión), puede utilizar las plantillas de dirección IP únicamente.

### Formato

NoLog { | *dirección\_IP* } [...]

### Ejemplo

NoLog 128.0.\* \*.edu localhost.\*

### Valor por omisión

Ninguno

## no\_proxy: especificar las plantillas para conectarse directamente con los dominios

Si está utilizando la directiva http\_proxy, ftp\_proxy o gopher\_proxy para el encadenamiento de proxy, puede utilizar esta directiva para especificar los dominios con los que se conecta el servidor directamente en lugar de ir a través de un proxy.

Especifique el valor como un serie de nombres de dominio o plantillas de nombre de dominio. Separe cada entrada de la serie con una coma (,). *No* utilice ningún espacio en la serie.

Las plantillas de esta directiva se especifican de modo distinto a las demás directivas. Y lo más importante, *no* puede utilizar el carácter comodín (\*). *Puede* especificar una plantilla incluyendo sólo la última parte de un nombre de dominio. El servidor se conecta directamente con cualquier dominio que termine con una serie que coincida con las plantillas que se especifiquen. Esta directiva sólo se aplica al encadenamiento de proxy y es equivalente a una línea @/= directa del archivo de configuración SOCKS.

### Formato

no\_proxy *nombre\_dominio\_o\_plantilla*[,...]

## Ejemplo

`no_proxy www.someco.com,.raleigh.ibm.com,.some.host.org:8080`

En este ejemplo, el servidor no va a través de un proxy para las siguientes peticiones:

- Cualquier petición a los dominios que terminen en `www.someco.com`
- Cualquier petición a los dominios que terminen en `.raleigh.ibm.com` como, por ejemplo, `blugrass.raleigh.ibm.com` o `keystone.raleigh.ibm.com`
- Cualquier petición al puerto 8080 de los dominios que terminen en `.some.host.org` como, por ejemplo, `myname.some.host.org:8080`. No se incluyen las peticiones a cualquier otro puerto del mismo dominio como, por ejemplo, `myname.some.host.org`, que asume el puerto por omisión 80.

## Valor por omisión

Ninguno

## NoCacheOnRange — Especificar sin colocación en antememoria para peticiones de rango

Por omisión, cuando se recibe de los navegadores una petición de rango, Caching Proxy requiere una respuesta completa del servidor de fondo. Caching Proxy elimina la cabecera Rango de la petición y, a continuación, reenvía la petición al servidor de fondo. Una vez que la respuesta se coloca en la antememoria en el servidor proxy, las peticiones posteriores de los mismos recursos se sirven desde el servidor proxy independientemente de si las peticiones son peticiones de rango o no. Habitualmente, la acción por omisión de Caching Proxy mejorará el rendimiento y dará a los clientes tiempos de respuesta más cortos. Sin embargo, si la respuesta no puede colocarse en la antememoria, o si es muy grande, la acción por omisión disminuirá el rendimiento.

Utilice la directiva `NoCacheOnRange`, que especifica que no hay colocación en antememoria para las peticiones de rango, a fin de solucionar el problema que se describe al utilizar la configuración por omisión.

Cuando habilite globalmente la directiva en el archivo `ibmproxy.conf`, o si la habilita como una opción para la regla de correlación `PROXY`, Caching Proxy reenvía la cabecera Petición de rango al servidor de fondo. Sin embargo, Caching Proxy no coloca en antememoria la respuesta 206 (contenido parcial) del servidor de fondo.

Habilitar la directiva `NoCacheOnRange` puede mejorar el rendimiento del proxy en los casos siguientes:

- Las respuestas no se pueden colocar en la antememoria ni actualizar frecuentemente.
- El tiempo de respuesta es crítico para la aplicación.

## Formato

`NoCacheOnRange [on | off]`

## Ejemplo

También puede habilitar `NoCacheOnRange` en una regla de correlación de proxy:

`Proxy /not-cachable/* http://server.com/no-cachable-resources/* NoCacheOnRange`

## Valor por omisión

`NoCacheOnRange off`

## NoProxyHeader: especificar las cabeceras de cliente que se desea bloquear

Utilice esta directiva para especificar las cabeceras URL que se desea bloquear. Cualquier cabecera HTTP enviada por un cliente puede bloquearse, incluidas las cabeceras necesarias. Se requiere extrema precaución al bloquear las cabeceras. Las cabeceras comunes son:

- **Pragma:**—generalmente se utiliza para indicar a los navegadores y servidores con antememorias que capture el archivo del servidor original siempre que se solicite éste archivo.
- **Referer:**—URL del archivo del cual se ha obtenido Request-URI.

Consulte la especificación de protocolo HTTP para obtener información detallada de estas y otras cabeceras. Puede especificar esta directiva varias veces.

### Formato

NoProxyHeader *cabecera*

### Ejemplo

NoProxyHeader Referer:

### Valor por omisión

Ninguno

## NumClients: especificar el número de hebras del agente de antememoria que se van a utilizar

Utilice esta directiva para especificar el número de hebras que el agente de antememoria utiliza para recuperar las páginas de la cola. Base el número de hebras en la velocidad de red interna y la conexión a Internet. El rango permitido es de 1 a 100.

**Nota:** La utilización de más de seis hebras posiblemente puede dar lugar a peticiones excesivamente rápidas en los servidores de contenido.

### Formato

NumClients *número*

### Valor por omisión

NumClients 4

## ObjectType: personalizar el paso de tipo de objeto

Utilice esta directiva para especificar una función de aplicación personalizada a la que el servidor llama durante el paso de tipo de objeto. Este código localiza el objeto solicitado en el sistema de archivos y especifica el tipo MIME que le corresponde.

### Formato

ObjectType *plantilla\_petición* /*vía\_acceso/archivo:nombre\_función*

*plantilla\_petición*

Especifica una plantilla para las peticiones que determinan adicionalmente si se llama a la función de aplicación. La especificación puede incluir el protocolo, el dominio y el sistema principal; puede estar precedida por una barra inclinada (/), y puede utilizar un asterisco (\*) como carácter comodín. Por ejemplo, /front\_page.html , http://www.ics.raleigh.ibm.com, /pub\*, /\* y \* son todas válidas.

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

### Ejemplo

ObjectType /index.html /api/bin/icsextpgm.so:obj\_type

### Valor por omisión

Ninguno

## OptimizeRuleMapping — Optimizar el proceso de correlación de regla para las peticiones entrantes cuando aumenta el número de reglas

Esta directiva acelera el proceso de correlación de reglas para peticiones entrantes cuando aumenta el número de reglas.

Cuando se habilita la directiva OptimizeRuleMapping, en vez de correlacionar las peticiones de URI entrantes con cada regla de una en una, el proxy correlaciona el URI con un árbol de prefijos. El árbol de prefijos ayuda al proxy a eliminar la comparación redundante de series entre las reglas de correlación. Como resultado, Caching Proxy consigue un rendimiento mejor cuando el número de reglas de la configuración es mayor que 300.

### Formato

OptimizeRuleMapping [on | off ]

### Valor por omisión

OptimizeRuleMapping off

## OutputTimeout: especificar el tiempo de espera de la salida

Utilice esta directiva para establecer el intervalo de tiempo máximo permitido al servidor para que envíe la salida a un cliente. El límite de tiempo se aplica a las peticiones de los archivos locales y las peticiones para las cuales el servidor actúa como un proxy. El límite de tiempo no se aplica a las peticiones que inician un programa CGI local.

Si el servidor no envía la respuesta completa dentro del límite de tiempo especificado en esta directiva, el servidor elimina la conexión. Especifique el valor de tiempo mediante cualquier combinación de horas, minutos (o mins) y segundos (o segs).

### Formato

OutputTimeout *tiempo*

### Valor por omisión

OutputTimeout 30 minutes

## PacFilePath: especificar el directorio que contiene los archivos PAC

Utilice esta directiva para especificar el directorio que contiene los archivos de autoconfiguración de proxy generados mediante el formulario de configuración remota de archivos PAC.

### Formato

PacFilePath *vía\_acceso\_directorio*

### Valores por omisión

- **Windows:** PacFilePath c:\Archivos de programa\IBM\edge\cp\HTML\pacfiles
- **Linux y UNIX:** PacFilePath /opt/ibm/edge/cp/server\_root/pub/pacfiles

## Pass: especificar la plantilla para aceptar peticiones

Utilice esta directiva para especificar una plantilla para las peticiones que desea aceptar y a las que desea responder con un archivo del servidor. Después de que una petición coincide con una plantilla de una directiva Pass, la petición no se compara con las plantillas de petición de cualquier directiva posterior.

### Formato

Pass *plantilla\_petición* [*vía\_acceso\_archivo* [*dirección\_IP\_servidor* | ]]

*plantilla\_petición*

Especifica una plantilla para las peticiones que desea que el servidor acepte y a las que responda con un archivo.

Puede utilizar un asterisco (\*) como comodín en la plantilla. El carácter de tilde (~) que aparece justo después de una barra inclinada (/) debe coincidir explícitamente; no se puede utilizar un carácter comodín para que coincida con él.

[*vía\_acceso\_archivo*]

Especifica la vía de acceso al archivo que el servidor va a devolver.

*vía\_acceso\_archivo* puede contener un carácter comodín si *plantilla\_petición* tiene uno. La parte de la petición que coincide con el comodín de *plantilla\_petición* se inserta en lugar del comodín de *vía\_acceso\_archivo*.

Este parámetro es opcional. Si no especifica la vía de acceso, la petición misma se utiliza como la vía de acceso.

[*dirección\_IP\_servidor* | *nombre\_sistppal*]

Si está utilizando varias direcciones IP o sistemas principales virtuales, utilice este parámetro para especificar una dirección IP o un nombre de sistema principal. El servidor utiliza la directiva sólo para las peticiones que llegan al servidor en esta dirección IP o para este sistema principal. Para una dirección IP, esta es la dirección de la conexión de red del servidor, no la dirección del cliente solicitante.

Puede especificar una dirección IP (por ejemplo, 240.146.167.72 ) o un nombre de sistema principal (por ejemplo, sistppalA.raleigh.ibm.com).

Este parámetro es opcional. Sin este parámetro, el servidor utiliza la directiva para todas las peticiones, independientemente de la dirección IP en la que entran las peticiones o el nombre de sistema principal del URL.

No puede especificarse un carácter comodín para la dirección IP de un servidor.

## Ejemplos

- En los siguientes ejemplos, el servidor responde a una petición que empieza con /updates/parts/ con un archivo de la vía de acceso enumerada, dependiendo del sistema operativo. Cualquier elemento que siga a /updates/parts/ también se utiliza para especificar el archivo.

**Sistemas Linux y UNIX:** Pass /updates/parts/\* /opt/ibm/edge/cp/server\_root/pub/\*

**Sistemas Windows:** Pass /updates/parts/\* c:\Archivos de programa\IBM\edge\cp\pub\\*

- En el siguiente ejemplo, el servidor responde a una petición que empieza con /gooddoc/ con un archivo del directorio /gooddoc. De este modo el servidor responde a la petición /gooddoc/volume1/issue2/newsletter4.html con un documento del archivo /gooddoc/volume1/issue2/newsletter4.html.

Pass /gooddoc/\*

- Los siguientes ejemplos utilizan el parámetro de dirección IP opcional. Si el servidor recibe peticiones que empiezan por /parts/, éste devuelve un archivo de un directorio distinto basándose en la dirección IP de la conexión de red en la que entra la petición. Para las peticiones que entran en 240.146.167.72, el servidor devuelve un archivo de /clienteA/catalog. Para las peticiones que entran en cualquier conexión con una dirección 0.83.100.45, el servidor devuelve un archivo de /clienteB/catalog/.

Pass /parts/\* /clienteA/catalog/\* 240.146.167.72

Pass /parts/\* /clienteB/catalog/\* 0.83.100.45

- Los siguientes ejemplos utilizan el parámetro de nombre de sistema principal opcional. Si el servidor recibe peticiones que empiezan por /parts/, devuelve un archivo de un directorio distinto basándose en el nombre de sistema principal del URL. Para las peticiones que entran para sistppalA, el servidor devuelve un archivo de /clienteA/catalog. Para las peticiones que entran para sistppalB, el servidor devuelve un archivo de /clienteB/catalog.

### Sistemas 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/\*

### Sistemas Solaris, HP-UX y Linux

Pass /Admin/\* /opt/ibm/edge/cp/server\_root/Admin/\*

Pass /Docs/\* /opt/ibm/edge/cp/server\_root/Docs/\*

Pass /errorpages/\* /opt/ibm/edge/cp/server\_root/pub/errorpages/\*

Pass /\* /opt/ibm/edge/cp/server\_root/pub/\*

## Valores por omisión

### Sistemas 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/\*

### Sistemas HP-UX, Linux y Solaris

Pass /Admin/\* /opt/ibm/edge/cp/server\_root/Admin/\*

Pass /Docs/\* /opt/ibm/edge/cp/server\_root/Docs/\*

Pass /errorpages/\* /opt/ibm/edge/cp/server\_root/pub/errorpages/\*

Pass /\* /opt/ibm/edge/cp/server\_root/pub/\*

### Sistemas Windows

Pass	/icons/*	C:\Archivos de programa\IBM\edge\cp\icons\*
Pass	/Admin/*	C:\Archivos de programa\IBM\edge\cp\Admin\*
Pass	/Docs/*	C:\Archivos de programa\IBM\edge\cp\Docs\*
Pass	/errorpages/*	C:\Archivos de programa\IBM\edge\cp\pub\errorpages\*
Pass	/*	C:\Archivos de programa\IBM\edge\cp\pub\*

## PersistTimeout: especificar el tiempo de espera para que el cliente envíe otra petición

Utilice esta directiva para especificar el periodo de tiempo que el servidor espera entre las peticiones del cliente antes de cancelar una conexión persistente. El tiempo puede especificarse en cualquier incremento de tiempo válido, pero generalmente se especifica en segundos o minutos.

El servidor utiliza una directiva de tiempo de espera distinta, InputTimeout, para determinar cuánto tiempo debe esperar el cliente para enviar la primera petición después del establecimiento de la conexión. Para obtener más información sobre el tiempo de espera de la entrada, consulte “InputTimeout: especificar el tiempo de espera de la entrada” en la página 231.

Después de que el servidor envíe la primera respuesta, éste utiliza el valor establecido de la directiva PersistTimeout para determinar cuánto tiempo se debe esperar a las peticiones posteriores antes de cancelar la conexión persistente.

### Formato

PersistTimeout *tiempo*

### Valor por omisión

PersistTimeout 4 seconds

## PICSDBLookup: personalizar el paso de recuperación de etiquetas PICS

Utilice esta directiva para especificar una función de aplicación personalizada a la que el servidor llama para recuperar las etiquetas PICS para un URL especificado. La función puede crear dinámicamente una etiqueta PICS para el archivo solicitado o bien buscar una etiqueta PICS en un archivo o base de datos alternativos.

### Formato

PICSDBLookup */vía\_acceso/archivo:nombre\_función*

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

### Ejemplo

PICSDBLookup /api/bin/icsext05.so:get\_pics

### Valor por omisión

Ninguno



## **PidFile (Linux y UNIX sólo): especificar el archivo donde se va a almacenar el ID de proceso de Caching Proxy**

**Linux y UNIX sólo.** Utilice esta directiva para especificar la ubicación del archivo que contiene el ID de proceso de Caching Proxy. Cuando se inicia el proceso de servidor, registra el ID de proceso ID (PID) en un archivo. Si varias instancias del servidor se ejecutan en un único sistema, todas las instancias deben tener su propia directiva PidFile.

### **Formato**

PidFile  
*vía\_acceso\_a\_info\_archivo\_pid*

### **Ejemplo**

PidFile /usr/pidinfo

### **Valores por omisión**

- Si se especifica una directiva ServerRoot: PidFile *raíz\_servidor* /ibmproxy-pid
- Si no se especifica una directiva ServerRoot: PidFile /tmp/ibmproxy-pid

## **PKCS11DefaultCert, PKCS11DriverPath, PKCS11TokenPassword — Da soporte a la tarjeta IBM 4960 PCI Cryptographic Accelerator Card (sólo AIX)**

En los sistemas AIX, se proporcionan directivas adicionales para dar soporte a la tarjeta IBM 4960 PCI Cryptographic Accelerator Card.

Utilice estas tres directivas para que el proxy pueda: cargar el controlador de dispositivo, abrir el dispositivo de señal y acceder a los certificados almacenados en el dispositivo. Cuando se carga el controlador de dispositivo, el servidor proxy utilizará automáticamente el dispositivo para aumentar la velocidad de comunicación de SSL.

Consulte también “SSLCryptoCard: especificar la tarjeta criptográfica instalada” en la página 286.

### **Formato**

PKCS11DefaultCert *etiqueta\_cert\_por\_omisión*

Especifique la etiqueta del certificado SSL por omisión en el dispositivo de señal.

PKCS11DriverPath *vía\_absoluta\_al\_controlador\_de\_tarjeta*

Especifique la vía de acceso absoluta al controlador de dispositivo de la tarjeta Cryptographic Accelerator Card.

PKCS11TokenPassword *contraseña*

Especifique la contraseña para abrir el dispositivo de señal.

### **Ejemplo**

PKCS11DefaultCert MyDefaultCertInTheToken  
PKCS11DriverPath /usr/lib/pkcs11/PKCS11\_API.so  
PKCS11TokenPassword MyPasswordToOpenTheToken

### **Valor por omisión**

Ninguno

## Directivas de módulos de plug-in

Las directivas enumeradas a continuación se han añadido al archivo `ibmproxy.conf` de Caching Proxy para habilitar nuevas características y plug-ins. Los formularios de Configuración y Administración no están disponibles para la edición de la mayoría de estas directivas. Se debe utilizar un editor de texto estándar como vi o emacs para editarlas manualmente. Encontrará información adicional sobre estas nuevas directivas por orden alfabético en este capítulo.

- “ExternalCacheManager: configurar Caching Proxy para la colocación en antememoria dinámica desde IBM WebSphere Application Server” en la página 220
- “ICP\_Address: especificar la dirección IP para las consultas ICP” en la página 227
- “ICP\_Port: especificar el número de puerto para las consultas ICP” en la página 228
- “ICP\_Timeout: especificar el tiempo de espera máximo para las consultas ICP” en la página 228
- “Occupier: especificar un miembro de un clúster ICP” en la página 228
- “ICP\_MaxThreads: especificar el número de hebras para las consultas ICP” en la página 227
- “SignificantURLTerminator; especificar un código de terminación para las peticiones URL” en la página 283
- “SSLCertificate — Especificar etiquetas de clave para certificados” en la página 284
- “SSLOnly — Inhabilitar hebras de receptor para peticiones HTTP” en la página 286

En el archivo `ibmproxy.conf`, las directivas utilizadas para configurar los módulos de plug-in de Caching Proxy deben especificarse con el siguiente formato:

```
<MODULEBEGIN> nombre plug-in
subdirectiva1
subdirectiva2

<MODULEEND>
```

Todos los programas de plug-in analizan el archivo `ibmproxy.conf` y leen únicamente su propio bloque de subdirectivas. El analizador de Caching Proxy ignora todo lo que aparece entre `<MODULEBEGIN>` y `<MODULEEND>`.

Los módulos de plug-in de Caching Proxy y algunas características nuevas requieren que las directivas API se añadan al archivo `ibmproxy.conf`. Como el servidor proxy interactúa con los módulos de plug-in en el orden en el que aparecen enumerados, tenga cuidado al ordenar las directivas en el archivo de configuración de proxy. Las directivas de prototipo (en forma de comentarios) se han añadido al apartado API del archivo `ibmproxy.conf`. Estas directivas API aparecen en un orden determinado. Al añadir las directivas API para habilitar nuevas características y módulos de plug-in, ordene las directivas como se muestran en la parte de prototipo del archivo de configuración. Alternativamente, elimine los comentarios de las directivas API y édítelas, si es necesario, para incluir el soporte de todas las funciones o plug-ins deseados. Añada los módulos de plug-in generados por el usuario después de los que se proporcionan con el producto.

## Port: especificar el puerto donde el servidor escucha las peticiones

Utilice esta directiva para especificar el número del puerto donde el servidor escucha las peticiones. El número de puerto estándar para HTTP es 80. Los demás números de puertos inferiores a 1024 se reservan para otras aplicaciones TCP/IP y no deben utilizarse. Los puertos comunes utilizados para los servidores Web de proxy son 8080 y 8008.

Cuando se utiliza un puerto distinto de 80, se le solicita a los clientes que incluyan un número de puerto específico en las peticiones al servidor. El número de puerto está precedido por dos puntos (:) y aparece colocado detrás del nombre de sistema principal del URL. Por ejemplo, desde el navegador, el URL `http://www.turfco.com:8008/` solicita la página de bienvenida por omisión de un sistema principal denominado `www.turfco.com` que escucha en el puerto 8008.

Puede utilizar la opción **-p** del mandato **ibmproxy** para sobrescribir este valor al iniciar el servidor.

### Formato

`Port número`

Si modifica esta directiva, debe detener y reiniciar el servidor manualmente para que el cambio entre en vigor. El servidor no reconoce el cambio si sólo lo reinicia. (Consulte el Capítulo 5, “Inicio y detención de Caching Proxy”, en la página 15.)

### Valor por omisión

`Port 80`

## PostAuth: personalizar el paso de PostAuth

Utilice esta directiva para especificar una función de aplicación personalizada a la que el servidor llama durante el paso de PostAuth. Este código se ejecuta independientemente de los códigos de retorno de pasos anteriores u otros manejadores PostAuth. Le permite limpiar cualquier recurso asignado para procesar la petición.

### Formato

`PostAuth /vía_acceso/archivo:nombre_función`

`/vía_acceso/archivo`

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

`nombre_función`

Especifica el nombre de la función de aplicación del programa.

### Ejemplo

`AuthExit /ics/api/bin/icsext05.so:post_exit`

### Valor por omisión

Ninguno

## PostExit: personalizar el paso de PostExit

Utilice esta directiva para especificar una función de aplicación personalizada a la que el servidor llama durante el paso de PostExit. Este código se ejecuta

independientemente de los códigos de retorno de pasos anteriores u otros manejadores PostExit. Le permite limpiar cualquier recurso asignado para procesar la petición.

### Formato

PostExit */vía\_acceso/archivo:nombre\_función*

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

### Ejemplo

PostExit /ics/api/bin/icsext05.so:post\_exit

### Valor por omisión

Ninguno

## PreExit: personalizar el paso de PreExit

Utilice esta directiva para especificar una función de aplicación personalizada a la que el servidor llama durante el paso de PreExit. Este código se ejecuta después de la lectura de una petición de cliente pero antes de que ocurra cualquier otro proceso. Puede llamar al módulo GoServe durante este paso.

### Formato

PreExit */vía\_acceso/archivo:nombre\_función*

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del DLL compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

### Ejemplo

PreExit /ics/api/bin/icsext05.so:pre\_exit

### Valor por omisión

Ninguno

## Protect: activar una configuración de protección de las peticiones que coinciden con una plantilla

Utilice esta directiva para activar las normas de configuración de protección de las peticiones que coinciden con una plantilla.

**Nota:** Para que la protección funcione correctamente, las directivas DefProt y Protect deben colocarse antes de cualquier directiva Pass, Exec o Proxy del archivo de configuración.

Una configuración de protección se define mediante subdirectivas de protección. El formato de la directiva Protect depende de si desea señalar a una etiqueta o archivo que contenga las subdirectivas de protección o bien incluir las subdirectivas de protección en línea como parte de la directiva Protect.

## Formato

Este parámetro puede adoptar las siguientes formas:

- La directiva Protect puede especificarse como una vía de acceso completa y nombre de archivo de un archivo independiente que contiene las subdirectivas de protección. También puede especificarse mediante un nombre de etiqueta de configuración de protección que coincida con un nombre definido anteriormente en una directiva Protection, que contiene las subdirectivas de protección. Utilice este formato:

```
Protect plantilla_petición [archivo_configuración | etiqueta]  
[FOR dirección_IP_servidor | ]
```

**Nota:** La directiva debe escribirse en una línea, aunque aquí se muestre en dos líneas.

- Puede especificar las subdirectivas de protección reales en línea en la directiva Protect. Las subdirectivas deben aparecer entre llaves {}. El carácter de llave izquierdo debe ser el último carácter que aparece en la misma línea que la directiva Protect. Todas las subdirectivas continúan en su propia línea. El carácter de llave derecho debe aparecer en su propia línea después de la última línea de subdirectiva. No pueden aparecer líneas de comentario entre las llaves. Para incluir las subdirectivas de protección en línea como parte de la directiva Protect, el formato es el siguiente:

```
Protect plantilla_petición [FOR dirección_IP_servidor | h]  
    subdirectiva valor  
    subdirectiva valor  
    .  
    .  
    .  
}
```

Se utilizan los siguientes parámetros:

*plantilla\_petición*

Especifica una plantilla para las peticiones para las que se desea activar la protección. El servidor compara las peticiones de cliente de entrada con la plantilla y activa la protección si se produce una coincidencia.

[*archivo\_configuración* | *etiqueta*]

Si está señalando a una etiqueta o archivo que contenga las subdirectivas de protección, este parámetro especifica que la configuración de protección se active para las peticiones que coincidan con *plantilla\_petición*.

Este parámetro es opcional. Si se omite, la configuración de protección se define mediante la directiva DefProt más reciente que contiene una plantilla que coincida.

[FOR *dirección\_IP\_servidor* | ]

Si está utilizando varias direcciones IP o sistemas principales virtuales, utilice este parámetro para especificar una dirección IP o un nombre de sistema principal. El servidor utiliza la directiva sólo para las peticiones que llegan al servidor en esta dirección IP o para este sistema principal. Para una dirección IP, esta es la dirección de la conexión de red del servidor, no la dirección del cliente solicitante. Si protege una dirección IP, se protegen tanto la dirección IP como el nombre de sistema principal plenamente cualificado. No obstante, no se protege al servidor si se lo llama servidor desde dentro de la red mediante un nombre distinto del nombre de sistema principal plenamente cualificado, como, por ejemplo, mediante una entrada de un archivo de nombre de sistema principal.

Ejemplo:

Protect http://x.x.x.x PROT-ADMIN

En un navegador Web:

- http://x.x.x.x está protegido
- http://nombresistppal.ejemplo.com está protegido
- http://nombresistppal no está protegido

Ejemplo:

Protect http://nombresistppal.ejemplo.com PROT-ADMIN

En un navegador Web:

- http://x.x.x.x no está protegido
- http://nombresistppal.ejemplo.com está protegido
- http://nombresistppal no está protegido

Puede especificar una dirección IP (por ejemplo, FOR 240.146.167.72 ) o un nombre de sistema principal (por ejemplo, FOR sistppalA.bcd.com ).

Los caracteres comodín no pueden utilizarse para especificar las direcciones IP de servidor.

Este parámetro es opcional. Sin este parámetro, el servidor utiliza la directiva para todas las peticiones, independientemente de la dirección IP en la que entran las peticiones o el nombre de sistema principal del URL.

**Nota:** El parámetro [*dirección\_IP\_servidor* | ] se utiliza con el parámetro [*archivo\_configuración* | *etiqueta*] o el parámetro *valor subdirectiva*.

- Para utilizar [*dirección\_IP\_servidor* | ] con [*archivo\_configuración* | *etiqueta*], debe incluir FOR o cualquier otra serie de caracteres (sin espacios) entre el parámetro [*archivo\_configuración* | *etiqueta*] y los parámetros [*dirección\_IP\_servidor* | ].
- Para utilizar [*dirección\_IP\_servidor* | ] con los parámetros *valor subdirectiva*, no incluya FOR antes de *dirección\_IP* ni de *nombre\_sistppal*.

#### *valor subdirectiva*

Para incluir las subdirectivas de protección como parte de la directiva Protect, utilice este parámetro. Para obtener descripciones de las subdirectivas de protección, consulte los apartados siguientes:

- “AuthType: especificar el tipo de autenticación” en la página 264
- “DeleteMask: especificar los nombres de usuario, grupos y direcciones que pueden suprimir archivos” en la página 264
- “GetMask: especificar los nombres de usuario, grupos y direcciones que pueden obtener archivos” en la página 264
- “GroupFile: especificar la ubicación del archivo de grupo asociado” en la página 264
- “Mask: especificar los nombres de usuario, grupos y direcciones que pueden realizar peticiones HTTP” en la página 265
- “PasswdFile: especificar la ubicación del archivo de contraseñas asociado” en la página 265

- “PostMask: especificar los nombres de usuario, grupos y direcciones que pueden enviar archivos” en la página 265
- “PutMask: especificar los nombres de usuario, grupos y direcciones que pueden transferir archivos” en la página 265
- “ServerID: especificar un nombre para asociarlo con el archivo de contraseñas” en la página 266

## Ejemplos

- En el siguiente ejemplo, el servidor activa la protección del siguiente modo:
  - Las peticiones que empiezan por /secret/scoop/ activan la protección. La configuración de protección se define en el archivo de configuración de protección /server/protect/setup1.acc. Como la directiva Protect no especifica una configuración de protección, se utiliza la configuración de protección de la directiva DefProt con la que haya coincidido anteriormente.
  - Las peticiones que empiezan por /secret/business/ activan la protección. La configuración de protección se define en la directiva Protection que tiene una etiqueta de BUS-PROT.
  - Las peticiones que empiezan por /topsecret/ activan la protección. La configuración de protección se incluye directamente en la directiva Protect.

Estos ejemplos utilizan direcciones IP. Si el servidor recibe peticiones que empiecen por /secret/ o /topsecret/, activa una configuración de protección distinta de la petición basándose en la dirección IP de la conexión de red que esa petición utiliza para entrar.

- Para las peticiones /secret/ que entren en 0.67.106.79, el servidor activa la configuración de protección definida en una directiva Protection con una etiqueta de ClienteA-PROT. Para las peticiones /topsecret/ requests que entren en 0.67.106.79, el servidor activa la configuración de protección definida en línea en la directiva Protect para /topsecret/.
- Para las peticiones /secret/ que entren en 0.83.100.45, el servidor activa la configuración de protección definida en una directiva Protection con una etiqueta de ClienteB-PROT. Para las peticiones /topsecret/ que entren en 0.83.100.45, el servidor activa la configuración de protección definida en línea en la directiva Protect para /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/* ClienteA-PROT FOR 0.67.106.79
Protect /secret/* ClienteB-PROT FOR 0.83.100.45
Protect /topsecret/* 0.67.106.79 {
    AuthType Basic
    ServerID restricted
    PasswdFile /docs/WWW/cliente-A.pwd
    GroupFile /docs/WWW/cliente-A.grp
    GetMask A-brass
    PutMask A-brass
}
Protect /topsecret/* 0.83.100.45 {
    AuthType Basic
    ServerID restricted
    PasswdFile /docs/WWW/cliente-B.pwd
    GroupFile /docs/WWW/cliente-B.grp
    GetMask B-brass
    PutMask B-brass
}

```

- Los siguientes ejemplos utilizan sistemas principales virtuales. Si el servidor recibe peticiones que empiecen por /secret/ o /topsecret/, activa una configuración de protección distinta para la petición basándose el nombre de sistema principal del URL.
  - Para las peticiones /secret/ que entren para sistppalA.bcd.com, el servidor activa la configuración de protección definida en una directiva Protection con una etiqueta de ClienteA-PROT. Para las peticiones /topsecret/ que entren para sistppalA.bcd.com, el servidor activa la configuración de protección definida en línea en la directiva Protect para /topsecret/.
  - Para las peticiones /secret/ que entren para sistppalB.bcd.com, el servidor activa la configuración de protección definida en una directiva Protection con una etiqueta de ClienteB-PROT. Para las peticiones /topsecret/ que entren para sistppalB.bcd.com, el servidor activa la configuración de protección definida en línea en la directiva Protect para /topsecret/.
  - Para las peticiones que pasan por el proxy, el servidor activa la configuración de protección definida en una directiva Protection con una etiqueta de proxy-prot. Por ejemplo:

```

Protect http://host1/* proxy-prot
Protect /secret/* ClienteA-PROT FOR sistppalA.bcd.com
Protect /secret/* ClienteB-PROT FOR sistppalB.bcd.com
Protect /topsecret/* sistppalA.bcd.com {
    AuthType Basic
    ServerID restricted
    PasswdFile /docs/WWW/cliente-A.pwd
    GroupFile /docs/WWW/cliente-A.grp
    GetMask A-brass
    PutMask A-brass
}
Protect /topsecret/* sistppalB.bcd.com {
    AuthType Basic
    ServerID restricted
    PasswdFile /docs/WWW/cliente-B.pwd
    GroupFile /docs/WWW/cliente-B.grp
    GetMask B-brass
    PutMask B-brass
}

```

## Valor por omisión

Por omisión, se proporciona protección para los formularios de Configuración y Administración mediante una directiva Protect con una plantilla de petición de /admin-bin/\* .



## Protection: definir una configuración de protección con nombre dentro del archivo de configuración

Utilice esta directiva para definir una configuración de protección dentro del archivo de configuración. Debe darle un nombre a la configuración de protección y definir el tipo de protección mediante las subdirectivas de protección.

### Notas:

1. En el archivo de configuración, coloque las directivas Protection antes de cualquier directiva DefProt o Protect que señale a ellas.
2. Para utilizar los nombres de dominio en las normas de protección, establezca la directiva DNS-Lookup en on.

### Formato

```
Protection nombre_etiqueta {  
    subdirectiva valor  
    subdirectiva valor  
    .  
    .  
    .  
}
```

#### *nombre\_etiqueta*

Especifica el nombre que se debe asociar con la configuración de protección. A continuación, las directivas DefProt y Protect posteriores pueden utilizar el nombre para señalar a esta configuración de protección.

#### *valor subdirectiva*

Las subdirectivas aparecen entre llaves ({ }). El carácter de llave izquierdo debe ser el último carácter que aparece en la misma línea que *nombre\_etiqueta*. Todas las subdirectivas continúan en su propia línea. El carácter de llave derecho debe aparecer en su propia línea después de la última línea de subdirectiva. No pueden aparecer líneas de comentario entre las llaves.

Consulte “Subdirectivas de protección: especificar cómo proteger un conjunto de recursos” en la página 264 para obtener descripciones de las subdirectivas de protección.

### Ejemplo

```
Protection NAME-ME {  
    AuthType      Basic  
    ServerID      restricted  
    PasswdFile    /WWW/password.pwd  
    GroupFile     /WWW/group.grp  
    GetMask       groupname  
    PutMask       groupname  
}
```

### Valor por omisión

```
Protect /admin-bin/* {  
    ServerId      Private_Authorization  
    AuthType      Basic  
    GetMask       All@(*)  
    PutMask       All@(*)  
    PostMask      All@(*)  
    Mask          All@(*)  
    PasswdFile    /opt/ibm/edge/cp/server_root/protect/webadmin.passwd  
}
```

## Subdirectivas de protección: especificar cómo proteger un conjunto de recursos

A continuación se proporcionan las descripciones de las subdirectivas de protección que pueden utilizarse en una configuración de protección. Las subdirectivas aparecen por orden alfabético.

Las configuraciones de protección pueden estar en archivos independientes o incluidas en el archivo de configuración como parte de las directivas DefProt, Protect o Protection.

### **AuthType: especificar el tipo de autenticación**

Utilice esta subdirectiva de protección al limitar el acceso en función de los nombres de usuario y las contraseñas. Especifique el tipo de autenticación que se va a utilizar cuando el cliente envíe una contraseña al servidor. Con la autenticación básica AuthType Basic), las contraseñas se envían al servidor como texto plano. Se codifican pero no se cifran.

#### **Valor por omisión:**

AuthType Basic

### **DeleteMask: especificar los nombres de usuario, grupos y direcciones que pueden suprimir archivos**

Utilice esta subdirectiva de protección para especificar las plantillas de nombres de usuario, grupos y direcciones autorizadas para realizar peticiones DELETE a un directorio protegido.

#### **Ejemplo:**

DeleteMask authors,(niceguy,goodie)@45.96.3.1,128.0.\*.\*

### **GetMask: especificar los nombres de usuario, grupos y direcciones que pueden obtener archivos**

Utilice esta subdirectiva de protección para especificar las plantillas de nombres de usuario, grupos y direcciones autorizadas para realizar peticiones GET a un directorio protegido.

#### **Ejemplo:**

GetMask authors,(niceguy,goodie)@45.96.3.1,128.0.\*.\*

#### **Valor por omisión:**

GetMask All@(\*)

### **GroupFile: especificar la ubicación del archivo de grupo asociado**

Utilice esta subdirectiva de protección para especificar la vía de acceso y el nombre de archivo del archivo de grupo de servidor que la configuración de protección utiliza. Los grupos definidos dentro del archivo de grupo de servidor los pueden utilizar posteriormente:

- Cualquier subdirectiva de máscara que forme parte de la configuración de protección. Las subdirectivas de máscara son DeleteMask, GetMask, Mask, PostMask y PutMask.
- Cualquier archivo ACL de un directorio que este protegido mediante la configuración de protección.

#### **Ejemplo:**

GroupFile /docs/etc/WWW/restrict.group

### **Mask: especificar los nombres de usuario, grupos y direcciones que pueden realizar peticiones HTTP**

Utilice esta subdirectiva para especificar las plantillas de nombres de usuario, grupos y direcciones autorizadas para realizar peticiones HTTP que no estén cubiertas por otras subdirectivas de máscara.

#### **Ejemplos:**

```
Mask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*
```

**Nota:** Cuando utilice la directiva Mask, es importante tener en cuenta que las máscaras son sensibles a las mayúsculas y minúsculas. A continuación aparece un ejemplo de una protección de máscara especificada en un ID de usuario:

```
MASK WEBADM,webadm
```

### **PasswdFile: especificar la ubicación del archivo de contraseñas asociado**

Utilice esta subdirectiva de protección al limitar el acceso en función de los nombres de usuario y las contraseñas. Especifique la vía de acceso y nombre del archivo de contraseñas que va a utilizar esta configuración de protección.

Como algunos navegadores colocan en antememoria los ID de usuario y contraseñas según el reino de seguridad (ServerID) de un sistema principal, siga estas directrices al especificar los archivo de contraseñas y ServerID:

- Para las configuraciones de protección que utilizan el mismo archivo de contraseñas, utilice el mismo ServerID.
- Para las configuraciones de protección que utilicen distintos archivos de contraseñas, utilice ServerIDs diferentes.

#### **Ejemplo:**

```
PasswdFile /docs/etc/WWW/restrict.password
```

**Nota:** Si la vía de acceso o el nombre de archivo del archivo de contraseñas contiene blancos intercalados, la vía de acceso o el nombre de archivo debe aparecer entre comillas ("").

```
PasswdFile "c:\test this\admin.pwd"
```

### **PostMask: especificar los nombres de usuario, grupos y direcciones que pueden enviar archivos**

Para tener un servidor protegido, utilice esta subdirectiva de protección para especificar las plantillas de usuarios, grupos y direcciones autorizadas para realizar peticiones POST a un directorio protegido.

#### **Ejemplo:**

```
PostMask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*
```

### **PutMask: especificar los nombres de usuario, grupos y direcciones que pueden transferir archivos**

Utilice esta subdirectiva de protección para especificar las plantillas de usuarios, grupos y direcciones autorizadas para realizar peticiones PUT a un directorio protegido.

#### **Ejemplo:**

```
PutMask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*
```

## **ServerID: especificar un nombre para asociarlo con el archivo de contraseñas**

Utilice esta subdirectiva de protección al limitar el acceso en función de los nombres de usuario y las contraseñas. Especifique un nombre que desee asociar con el archivo de contraseñas que se esté utilizando. No es necesario que el nombre sea el nombre real de la máquina.

El nombre se utiliza como un identificador del solicitante. Como distintas configuraciones de protección pueden utilizar archivos de contraseñas diferentes, la asociación de un nombre con la configuración de protección puede ayudar al cliente a decidir qué contraseña debe enviar. La mayoría de los clientes muestran este nombre al solicitar un nombre de usuario o contraseña.

Como algunos navegadores colocan en antememoria los ID de usuario y contraseñas según el reino de seguridad (ServerID) de un sistema principal, siga estas directrices al especificar los archivo de contraseñas y ServerID:

- Para las configuraciones de protección que utilizan el mismo archivo de contraseñas, utilice el mismo ServerID.
- Para las configuraciones de protección que utilicen distintos archivos de contraseñas, utilice ServerIDs diferentes.

### **Ejemplo:**

ServerID restricted

## **Proxy: especificar los protocolos de proxy o el proxy de retorno**

Utilice esta directiva para indicar qué protocolos va a procesar Caching Proxy y correlacionar una petición con un servidor. Los protocolos válidos son http, ftp y gopher.

La directiva de proxy pasa la petición a un servidor remoto. Por ejemplo, la siguiente directiva provoca que todas las peticiones se reenvíen al URL designado:

```
Proxy /* http://nombre.servidor.proxy/*
```

Para disponer de un servidor proxy de retorno, utilice la siguiente directiva:

```
Proxy /* https://nombre.servidor.proxy/*
```

Si desea que el servidor proxy sea menos restrictivo, elimine los comentarios de las siguientes directivas del archivo de configuración. No obstante, estas directivas pueden ocasionar un problema de seguridad cuando el proxy se configura como un proxy de retorno.

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

### **Parámetros opcionales:**

- UseSession

Sólo se aplica a configuraciones de proxy de retorno.

Esta opción indica a Caching Proxy que mantenga una correlación de uno a uno entre el socket del cliente y el socket saliente. Esta opción es útil para algunas aplicaciones como, por ejemplo, la autenticación basada en conexiones, que necesitan al proxy para mantener activo el socket del servidor y reutilizar el socket para las peticiones que vengan del mismo socket del cliente.

- NoCaching  
Si se cumple la regla del proxy, esta opción indica al proxy que no coloque en antememoria las respuestas correspondientes.
- NoCacheOnRange  
Si se cumple la regla del proxy y hay una cabecera Range en la petición, esta opción indica al proxy que no coloque en antememoria la respuesta correspondiente. Para obtener más información, consulte “NoCacheOnRange — Especificar sin colocación en antememoria para peticiones de rango” en la página 249.
- NoJunction  
Sólo se aplica a configuraciones de proxy de retorno.  
Utilice esta opción si el plug-in de reescritura de enlace está habilitado. Esta opción no permite que el proxy reescriba las respuestas correspondientes si el URL entrante coincide. Para obtener más información, consulte “Habilitación de la reescritura de unión (opcional)” en la página 47 y “Definición de la unión con la opción JunctionPrefix (método recomendado)” en la página 48.
- JunctionPrefix  
Sólo se aplica a configuraciones de proxy de retorno.  
Utilice esta opción si el plug-in de reescritura de enlace está habilitado. En vez de inferir el prefijo de enlace a partir del primer patrón de URL en la regla de proxy, la opción declara explícitamente el prefijo de reescritura de enlace. Para obtener más información, consulte “Habilitación de la reescritura de unión (opcional)” en la página 47 y “Definición de la unión con la opción JunctionPrefix (método recomendado)” en la página 48.

## Formato

Proxy *plantilla\_petición vía\_servidor\_destino* [[ip]:puerto]  
[UseSession | NoCaching | NoCacheOnRange | NoJunction | JunctionPrefix:/prefijo\_url]

## Ejemplo

A continuación aparece un ejemplo de la opción UseSession de la directiva Proxy:

```
Proxy /abc/* http://servidor1/por_omisión/abc/* :80 UseSession
```

Cuando la petición de entrada de cliente viene del puerto 80, y si el URL de la petición de cliente coincide con el patrón /abc/\*, el URL se correlaciona con http://servidor1/por\_omisión/abc/\*.

## Valores por omisión

Ninguno.

## ProxyAccessLog: nombrar la vía de acceso del archivo de anotaciones cronológicas de acceso al proxy

Utilice esta directiva para especificar la vía de acceso y el nombre del archivo donde desea que el servidor anote cronológicamente las estadísticas de acceso de las peticiones de proxy. Por ejemplo, el servidor escribe una entrada en estas anotaciones cronológicas siempre que actúa como un proxy para una petición de cliente. Puede utilizar la directiva NoLog si no desea anotar cronológicamente las peticiones de ciertos clientes.

El servidor inicia un nuevo archivo de anotaciones cronológicas cada día a las doce de la noche si se está ejecutando. De lo contrario, el servidor inicia un nuevo archivo de anotaciones cronológicas la primera vez que lo inicia en un día cualquiera. Al crear el archivo, el servidor utiliza el nombre de archivo que

especifica e añadirá una extensión o sufijo de fecha. La extensión o sufijo de fecha aparece en el formato *Mmmddaaaa*, donde *Mmm* son las tres primeras letras del mes, *dd* es el día del mes y *aaaa* es el año.

Se recomienda eliminar los archivos de anotaciones cronológicas antiguos ya que pueden consumir un cantidad significativa de espacio de la unidad de disco duro.

### Formato

*ProxyAccessLog* *vía\_acceso/archivo*

### Valores por omisión

- **Sistemas Linux y UNIX:** *ProxyAccessLog* /opt/ibm/edge/cp/server\_root/logs/proxy
- **Sistemas Windows:** *ProxyAccessLog* *unidad:*\Archivos de programa\IBM\edge\cp\logs\proxy

## ProxyAdvisor: personalizar el servicio de las peticiones de proxy

Utilice esta directiva para especificar una aplicación personalizada a la que desea que el servidor llame durante el paso de Proxy Advisor. Este código dará servicio a la petición.

### Formato

*ProxyAdvisor* /*vía\_acceso/archivo:nombre\_función*

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

### Ejemplo:

*ProxyAdvisor* /api/bin/customadvise.so:proxyadv

### Valor por omisión

Ninguno

## ProxyForwardLabels: especificar el filtrado PICS

Utilice la directiva *ProxyForwardLabels* para especificar el filtrado PICS en el servidor proxy y en el servidor, o en dos proxies de una jerarquía de proxy.

Si *ProxyForwardLabels* se establece en *on*, el servidor proxy genera cabeceras HTTP *PICS-Label*: de todas la etiquetas PICS encontradas, que incluyen las etiquetas del servidor de origen, las oficinas de etiquetas, la antememoria de etiquetas de Caching Proxy y los plug-ins de proveedor de etiquetas.

Si *ProxyForwardLabels* se establece en *off*, las cabeceras HTTP *PICS-Label*: no se generan.

### Formato

*ProxyForwardLabels* {on | off}

### Valor por omisión

*ProxyForwardLabels* Off

## ProxyFrom: especificar un cliente con una cabecera From:

Utilice esta directiva para generar una cabecera From:. Generalmente se utiliza para proporcionar una dirección de correo electrónico del administrador de proxy.

### Formato

ProxyFrom *dirección\_correo\_electrónico*

### Ejemplo

El valor ProxyFrom webmaster@proxy.ibm.com ocasiona la siguiente modificación de la cabecera:

#### Cabecera original

Location: http://www.ibm.com/  
Last Modified: Tue 5 Nov 1997 10:05:39  
GMT  
Pragma: no-cache

#### Cabecera modificada

Location: http://www.ibm.com/  
Last Modified: Tue 5 Nov 1997 10:05:39  
GMT  
**From: webmaster@proxy.ibm.com**  
Pragma: no-cache

### Valor por omisión

Ninguno

## ProxyIgnoreNoCache: ignorar una petición de recarga

Utilice esta directiva para especificar cómo reacciona el servidor cuando los usuarios pulsán **Recargar** en el navegador. Si la directiva ProxyIgnoreNoCache se establece en on, durante los periodos de carga elevada el servidor no solicita la página del servidor de destino y proporciona la copia en antememoria del archivo si está disponible. Esencialmente, el servidor hace caso omiso de la cabecera Pragma: no-cache enviada desde el navegador.

### Formato

ProxyIgnoreNoCache {on | off}

### Valor por omisión

ProxyIgnoreNoCache off

## ProxyPersistence: permitir las conexiones persistentes

Utilice esta directiva para especificar si se desea mantener una conexión persistente con el cliente. Una conexión persistente reduce el tiempo de espera para los usuarios así como la carga de la CPU del servidor proxy, pero requiere más recursos. Se requieren más hebras y, por lo tanto, más memoria del servidor proxy para una conexión persistente.

Las conexiones persistentes no deben utilizarse en una configuración de servidores proxy de varios niveles si alguno de los proxies no es compatible con HTTP 1.1.

### Formato

ProxyPersistence {on | off}

### Valor por omisión

ProxyPersistence on

## ProxySendClientAddress: generar la cabecera Client IP Address:

Utilice esta directiva para especificar si el proxy reenvía la dirección IP del cliente al servidor de destino.

### Formato

ProxySendClientAddress {*IP\_cliente*: | OFF}

### Ejemplo

La directiva ProxySendClientAddress *Client-IP*: ocasiona la siguiente modificación de la cabecera:

#### Cabecera original

Location: http://www.ibm.com/  
Last Modified: Tue 5 Nov 1997 10:05:39 GMT  
Pragma: no-cache

#### Cabecera modificada

Location: http://www.ibm.com  
Last Modified: Tue 5 Nov 1997 10:05:39 GMT  
**Client-IP: 0.67.199.5**  
Pragma: no-cache

### Valor por omisión

Ninguno

## ProxyUserAgent; modificar la serie User Agent

Utilice esta directiva para especificar la serie User Agent que sustituye a la serie que envía el cliente. Esta acción permite un mayor anonimato al visitar los sitios Web. No obstante, algunos sitios tienen páginas personalizadas basadas en la serie User Agent. La utilización de la directiva ProxyUserAgent evita que estas páginas de personalización se visualicen.

### Formato

ProxyUserAgent *nombre\_producto/versión*

### Ejemplo

La directiva ProxyUserAgent Caching Proxy/6.1 ocasiona la siguiente modificación de la cabecera:

#### Cabecera original

Location: http://www.ibm.com/  
Last Modified: Tue 5 Nov 1997 10:05:39 GMT  
**User Agent: Mozilla/ 2.02 OS2**  
Pragma: no-cache

#### Cabecera modificada

Location: http://www.ibm.com  
Last Modified: Tue 5 Nov 1997 10:05:39 GMT  
**User Agent: Caching Proxy/6.1**  
Pragma: no-cache

### Valor por omisión

Ninguno

## ProxyVia: especificar el formato de la cabecera HTTP

Utilice esta directiva para controlar el formato de la cabecera HTTP. Existen cuatro valores posibles de esta directiva. Si ProxyVia se establece en Full, Caching Proxy añade una cabecera Via a la petición o respuesta; si una cabecera Via ya está en la corriente, Caching Proxy añade la información de sistema principal al final. Si se establece en Set, Caching Proxy establece la cabecera Via en la información de sistema principal; si una cabecera Via ya está en la corriente, Caching Proxy la



elimina. Si se establece en Pass, Caching Proxy reenvía cualquier información como está. Si se establece en Block, Caching Proxy no reenvía ninguna cabecera Via.

### Formato

ProxyVia {Full | Set | Pass | Block}

### Ejemplo

ProxyVia Pass

### Valor por omisión

ProxyVia Full

## ProxyWAS: especificar que las peticiones se envíen a WebSphere Application Server

Sólo se aplica a configuraciones de proxy de retorno.

La directiva de correlación ProxyWAS funciona de modo idéntico a la directiva Proxy, pero también indica a Caching Proxy que las peticiones coincidentes se dirijan a WebSphere Application Server. Por ejemplo, para obtener información sobre cómo utilizar esta directiva, consulte “Proxy: especificar los protocolos de proxy o el proxy de retorno” en la página 266.

### Formato

ProxyWAS *plantilla\_petición vía acceso\_servidor\_destino* [[ip]:puerto]  
[UseSession | NoCaching | NoCacheOnRange | NoJunction |  
JunctionPrefix:/*prefijo\_url*]

### Valor por omisión

Ninguno

## PureProxy: inhabilitar un proxy dedicado

Utilice esta directiva para especificar si el servidor debe actuar como un servidor proxy o como un proxy y servidor de contenido. Se recomienda que utilice Caching Proxy como proxy sólo.

### Formato

PureProxy {on | off}

### Valor por omisión

PureProxy on

## PurgeAge: especificar el límite de antigüedad para las anotaciones cronológicas

Utilice esta directiva para especificar la antigüedad de las anotaciones cronológicas en días antes de que se depuren. Si PurgeAge se establece en 0, las anotaciones cronológicas no se suprimen nunca.

**Nota:** El plug-in nunca suprime las anotaciones cronológicas del día actual ni del día anterior.

### Formato

PurgeAge *número*

### Valor por omisión

PurgeAge 7

## Directivas relacionadas

- “CompressAge: especificar cuándo comprimir las anotaciones cronológicas” en la página 202
- “CompressDeleteAge: especificar cuándo suprimir las anotaciones cronológicas” en la página 204
- “CompressCommand: especificar el mandato y los parámetros de compresión” en la página 203
- “Midnight: especificar el plug-in de API utilizado para archivar las anotaciones cronológicas” en la página 246
- “LogArchive: especificar el comportamiento del archivado de las anotaciones cronológicas” en la página 237
- “PurgeSize: especificar el límite del tamaño del archivador de anotaciones cronológicas”

## PurgeSize: especificar el límite del tamaño del archivador de anotaciones cronológicas

Utilice esta directiva para especificar el tamaño en megabytes que pueden alcanzar los archivos de anotaciones cronológicas antes de que se depure el archivador de anotaciones cronológicas. Si la directiva PurgeSize se establece en 0, no existe límite de tamaño y no se suprimen archivos.

El valor de PurgeSize hace referencia a *todas* las anotaciones cronológicas de un tipo de anotaciones cronológicas. Por ejemplo, si está anotando cronológicamente los errores -es decir, si una entrada ErrorLog se ha realizado en el archivo de configuración- y PurgeSize está definido como 10 MB, Caching Proxy calcula los tamaños de todas las anotaciones cronológicas de error, las suma y, a continuación, elimina anotaciones cronológicas hasta que el tamaño total es inferior a 10 MB.

**Nota:** El plug-in nunca suprime las anotaciones cronológicas del día actual ni del día anterior. Cuando se suprimen archivos de anotaciones cronológicas, las anotaciones más antiguas se suprimen primero, hasta que el tamaño de los archivos de anotaciones cronológicas de todos los tipos de anotaciones cronológicas sea inferior o igual al valor definido por PurgeSize (en megabytes).

### Formato

PurgeSize *número\_de\_MB*

### Valor por omisión

PurgeSize 0

## Directivas relacionadas

- “CompressAge: especificar cuándo comprimir las anotaciones cronológicas” en la página 202
- “CompressDeleteAge: especificar cuándo suprimir las anotaciones cronológicas” en la página 204
- “CompressCommand: especificar el mandato y los parámetros de compresión” en la página 203
- “LogArchive: especificar el comportamiento del archivado de las anotaciones cronológicas” en la página 237
- “Midnight: especificar el plug-in de API utilizado para archivar las anotaciones cronológicas” en la página 246

- “PurgeAge: especificar el límite de antigüedad para las anotaciones cronológicas” en la página 271

## **RCAConfigFile: especificar un alias para ConfigFile**

Utilice esta directiva para especificar el nombre y la ubicación del archivo de configuración de acceso a antememoria remota.

**Nota:** El archivo de configuración RCA se ha fusionado con el archivo `ibmproxy.conf`. Para obtener la compatibilidad con versiones anteriores, se da soporte a `RCAConfigFile` como un alias para `ConfigFile`.

### **Formato**

`RCAConfigFile /etc/nombre_archivo`

### **Ejemplo**

`RCAConfigFile /etc/user2rca.conf`

### **Valor por omisión**

`RCAConfigFile /etc/rca.conf`

## **RCAThreads: especificar el número de hebras por puerto**

Utilice esta directiva para especificar el número de hebras que funcionan en un puerto RCA.

### **Formato**

`RCAThreads número_de_hebras`

### **Ejemplo**

`RCAThreads 50`

### **Valor por omisión**

`MaxActiveThreads x [(ArraySize -1) / (2 x ArraySize -1)]`

## **ReadTimeout: especificar el límite de tiempo de una conexión**

Utilice esta directiva para especificar el límite de tiempo permitido sin actividad de red antes de que se cancele una conexión.

### **Formato**

`ReadTimeout tiempo`

### **Valor por omisión**

`ReadTimeout 5 minutes`

## **Redirect: especificar una plantilla para las peticiones enviadas a un servidor distinto**

Utilice esta directiva para especificar una plantilla para las peticiones que desea aceptar y enviar a otro servidor. Después de que una petición coincida con una plantilla de una directiva `Redirect`, la petición no se compara con las plantillas de ninguna otra directiva del archivo de configuración.

### **Formato**

`Redirect plantilla_petición URL [dirección_IP_servidor | ]`

### *plantilla\_petición*

Especifica una plantilla para las peticiones que desea que el servidor envíe a otro servidor.

Puede utilizar un asterisco (\*) como comodín en la plantilla. El carácter de tilde (~) que aparece justo después de una barra inclinada (/) debe coincidir explícitamente; no se puede utilizar un carácter comodín para que coincida con él.

### *URL*

Especifica la petición de URL que el servidor envía a otro servidor. La respuesta a esta petición va al solicitante original sin ninguna indicación de que no venía de su propio servidor.

*URL* debe contener una especificación de protocolo y el nombre del servidor al se envía la petición. También debe contener una vía de acceso o un nombre de archivo. Si *plantilla\_petición* utiliza un comodín, la vía de acceso o el nombre de archivo de *URL* también puede contener un comodín. La parte de la petición original que coincide con el comodín de *plantilla\_petición* se inserta en lugar del comodín de *URL*.

### [*dirección\_IP\_servidor* | ]

Si está utilizando varias direcciones IP o sistemas principales virtuales, utilice este parámetro para especificar una dirección IP o un nombre de sistema principal. El servidor utiliza la directiva sólo para las peticiones que llegan al servidor en esta dirección IP o para este sistema principal. Para una dirección IP, esta es la dirección de la conexión de red del servidor, no la dirección del cliente solicitante.

Puede especificar una dirección IP (por ejemplo, 240.146.167.72 ) o un nombre de sistema principal (por ejemplo, sistppalA.bcd.com ).

Este parámetro es opcional. Sin este parámetro, el servidor utiliza la directiva para todas las peticiones, independientemente de la dirección IP en la que entran las peticiones o el nombre de sistema principal del URL.

No puede especificarse un carácter comodín para la dirección IP de un servidor.

## Ejemplos

- En el siguiente ejemplo, el servidor envía cualquier petición que empiece por /chief/stuff/ al directorio wahoo del servidor de www.otra.org.  
Redirect /chief/stuff/\* http://www.otra.org/wahoo/\*
- Los siguientes ejemplos utilizan el parámetro de dirección IP opcional. Si el servidor recibe peticiones que empiezan por /stuff/, redirige la petición a servidores distintos basándose en la dirección IP de la conexión de red en la que entra la petición. Para las peticiones que entran en 240.146.167.72, el servidor envía la petición al directorio wahoo del servidor www.chief.org. Para las peticiones que entran en cualquier conexión con una dirección de 0.83.100.45, el servidor envía la petición al directorio pound del servidor www.dawg.com.  
Redirect /stuff/\* http://www.chief.org/wahoo/\* 240.146.167.72  
Redirect /stuff/\* http://www.dawg.com/pound/\* 0.83.100.45
- Los siguientes ejemplos utilizan el parámetro de dirección IP opcional. Si el servidor recibe peticiones que empiezan por /stuff/, redirige la petición a servidores distintos basándose en el nombre de sistema principal del URL. Para las peticiones que entran para sistppalA, el servidor envía la petición al directorio wahoo del servidor www.chief.org. Para las peticiones que entran para sistppalB, el servidor envía la petición al directorio pound del servidor www.dawg.com.

Redirect	/stuff/*	http://www.chief.org/wahoo/*	sistppalA.bcd.com
Redirect	/stuff/*	http://www.dawg.com/pound/*	sistppalB.bcd.com

### Valor por omisión

Ninguno

## RegisterCacheIdTransformer: almacenar en antememoria más de una variante de un recurso basándose en la cabecera Cookie

Utilice esta directiva para permitir a Caching Proxy almacenar en antememoria más de una variante de un recurso (URI) basándose en la cabecera Cookie.

**Nota:** Si se inhabilitan las cookies en los navegadores del cliente, los clientes pueden acceder al mismo objeto almacenado en antememoria.

Para obtener más información, consulte “SupportVaryHeader: almacenar en antememoria más de una variante de un recurso basándose en la cabecera Vary de HTTP” en la página 289.

### Formato

RegisterCacheIdTransformer Cookie *nombre-cookie*

*nombre-cookie* es el nombre de la cabecera Cookie en la petición del cliente.

### Ejemplo

RegisterCacheIdTransformer Cookie Usergroup

Para obtener un ejemplo de utilización de esta directiva junto con SupportVaryHeader, consulte “SupportVaryHeader: almacenar en antememoria más de una variante de un recurso basándose en la cabecera Vary de HTTP” en la página 289.

### Valor por omisión

Ninguno

## ReversePass: interceptar las peticiones redirigidas automáticamente

Sólo se aplica a configuraciones de proxy de retorno.

La directiva de correlación ReversePass examina la corriente de respuestas de servidor para detectar las peticiones que se reescriben como resultado de la redirección automática. Generalmente, cuando un servidor devuelve un código HTTP de la clase 3xx (por ejemplo, 301, trasladado permanentemente, o 303, ver otro), el servidor envía un mensaje con la respuesta que indica al cliente solicitante que dirija las peticiones futuras a la dirección IP y el URL correctos. En el caso de una configuración de proxy de retorno, un mensaje de redirección desde el servidor de origen puede ocasionar que los navegadores de cliente omitan el servidor de proxy en peticiones posteriores. Para evitar que los clientes contacten con el servidor de origen directamente, utilice la directiva ReversePass para interceptar las peticiones que se realizan específicamente al servidor de origen.

A diferencia de las demás directivas de correlación, que procesan la corriente de peticiones, ReversePass hace coincidir su plantilla con la corriente de respuestas. La corriente de respuestas es la respuesta que el servidor proxy obtiene del servidor de origen y envía al cliente.

### Formato

ReversePass *URL\_reescrito* *URL\_proxy* [*sistppal:puerto*]

La opción *sistppal:puerto* permite que el proxy aplique una norma ReversePass distinta basada en el nombre de sistema principal y el puerto del servidor de programa de fondo.

### Ejemplos

- La siguiente sentencia de ejemplo evita las peticiones directas al servidor de origen:

```
ReversePass http://backend.company.com:9080/* http://edge.company.com/*
```

El puerto 9080 es el puerto por omisión de Application Service at the Edge. Este tipo de petición puede generarse si el servidor de aplicaciones de origen devuelve un código de 3xx al cliente.

- La siguiente sentencia de ejemplo captura las peticiones que se hayan redirigido mediante un código 301 desde el Servidor de aplicaciones Edge.

```
ReversePass http://edge.company.com:9080/* http://edge.company.com/*
```

**Nota:** El contenido del patrón *URL\_proxy* hasta el comodín (\*), debe coincidir exactamente con lo que el servidor de programa de fondo envía en la cabecera de ubicación; de lo contrario, se produce un error en la directiva.

### Valor por omisión

Ninguno

## RewriteSetCookieDomain: especificar el patrón de dominio que es necesario reescribir

Sólo se aplica a configuraciones de proxy de retorno.

Utilice esta directiva para especificar el patrón de dominio que es necesario reescribir. La directiva modificará el dominio de *patrón\_dominio1* a *patrón\_dominio2*.

### Formato

RewriteSetCookieDomain *patrón\_dominio1* *patrón\_dominio2*

### Ejemplo

```
RewriteSetCookieDomain .internal.com .external.com
```

### Valor por omisión

Ninguno

### Directivas relacionadas

- “JunctionRewriteSetCookiePath: reescribir la opción de vía de acceso en la cabecera Set-Cookie cuando se utiliza con el plug-in JunctionRewrite” en la página 232

## RTSPEnable: habilitar la redirección de RTSP

Sólo se aplica a configuraciones de proxy de retorno.

Esta directiva habilita o inhabilita la redirección de RTSP. Las opciones son on u off.

### Formato

RTSPEnable {on | off}

### Ejemplo

RTSPEnable on

### Valor por omisión

Ninguno

## rtsp\_proxy\_server: especificar los servidores para la redirección

Sólo se aplica a configuraciones de proxy de retorno.

Esta directiva se utiliza para especificar que los servidores proxy de RTSP reciban las peticiones redirigidas. Se pueden especificar distintos servidores para tipos de corrientes diferentes. El formato de esta directiva es:

rtsp\_proxy\_server *dirección dns servidor[:puerto]* *rango por omisión*  
[*lista de tipos mime*]

### Ejemplo

rtsp_proxy_server	rproxy.mycompany.com:554	1
rtsp_proxy_server	fw1.mycompany.com:554	2
rtsp_proxy_server	fw1.mycompany.com:555	3
rtsp_proxy_server	fw2.mycompany.com:557	4

### Valor por omisión

Ninguno

## rtsp\_proxy\_threshold: especificar el número de peticiones antes de la redirección a una antememoria

Sólo se aplica a configuraciones de proxy de retorno.

Esta directiva especifica cuántas peticiones se reciben antes de que una petición RTSP se redirija a un servidor proxy en lugar de a un servidor de origen. Los proxies RealNetworks colocan en antememoria las corrientes de la primera petición e inicialmente la colocación en antememoria se produce al doble del ancho de banda de la recepción de una corriente. La especificación de un umbral mayor que uno evita que las peticiones realizadas una vez se coloquen en antememoria. El formato de esta directiva es:

rtsp\_proxy\_threshold  
*número\_de\_coincidencias*

### Ejemplo

rtsp\_proxy\_threshold 5

### Valor por omisión

Ninguno

## rtsp\_url\_list\_size: especificar el número de los URL en la memoria proxy

Sólo se aplica a configuraciones de proxy de retorno.

Esta directiva especifica el número de los URL exclusivos que se mantienen en la memoria para la redirección. El proxy consulta esta lista para determinar si se ha encontrado un determinado URL anteriormente. Los tamaños de lista más grandes mejoran la capacidad del servidor proxy para enviar una petición posterior al mismo servidor proxy que haya recibido la petición anterior, aunque todas las entradas de lista consumen aproximadamente 16 bytes de memoria.

#### Formato

`rtsp_url_list_size tamaño_de_lista`

#### Ejemplo

`rtsp_url_list_size 8192`

#### Valor por omisión

Ninguno

### RuleCaseSense — Correlaciona peticiones de los URL de aplicación que no son sensibles a mayúsculas y minúsculas

Por omisión, cuando Caching Proxy correlaciona peticiones con reglas definidas en el archivo `ibmproxy.conf`, el proceso de coincidencia es sensible a mayúsculas y minúsculas. Sin embargo, algunos URL de aplicación no son sensibles a mayúsculas y minúsculas. Para manejar correctamente estas peticiones, se proporciona la directiva `RuleCaseSense`. Cuando la directiva se establece en `off`, el proxy emparejará peticiones independientemente de que tengan mayúsculas o minúsculas.

**Nota:** La directiva es global y se aplica a todas las reglas de correlación definidas.

#### Formato

`RuleCaseSense {on | off}`

#### Valor por omisión

`RuleCaseSense on`

### ScriptTimeout: especificar el valor de tiempo de espera de los scripts

Utilice esta directiva para establecer el tiempo permitido para que finalice un programa CGI iniciado por el servidor. Cuando caduca el tiempo, el servidor finaliza el programa. En las plataforma Linux y UNIX, esto se realiza con la señal KILL.

Especifique el valor de tiempo mediante cualquier combinación de horas, minutos (o mins) y segundos (o segs).

#### Formato

`ScriptTimeout tiempo_espera`

#### Valor por omisión

`ScriptTimeout 5 minutes`

### SendHTTP10Outbound: especificar la versión de protocolo para las peticiones que pasan por el proxy

Utilice esta directiva para especificar qué peticiones enviadas desde Caching Proxy a un servidor en sentido descendente deben utilizar el protocolo HTTP versión 1.0.



Un servidor *en sentido descendente* es otro servidor proxy de una cadena de proxies o un servidor de origen que procesa la petición.

Si se utiliza esta directiva, Caching Proxy identifica HTTP 1.0 como el protocolo de la línea de petición. Sólo las funciones específicas de HTTP 1.0 y ciertas funciones de HTTP 1.1 como, por ejemplo, las cabeceras de control de antememoria, a las que dan soporte la mayoría de los servidores HTTP 1.0, se envían al servidor en sentido descendente. Utilice esta directiva si tiene un servidor en sentido descendente que no maneja las peticiones HTTP 1.1 correctamente.

Si *no* se especifica la directiva SendHTTP10Outbound, Caching Proxy identifica HTTP 1.1 como el protocolo de la línea de petición. Las funciones de HTTP 1.1, como, por ejemplo, las conexiones persistentes, también pueden utilizarse en la petición.

### Formato

SendHTTP10Outbound *patrón\_url*

### Ejemplos

Esta directiva puede especificarse varias veces, por ejemplo:

```
SendHTTP10Outbound http://www.hosta.com/*
SendHTTP10Outbound http://www.hostb.com/*
```

Para obtener la compatibilidad con versiones anteriores, la sintaxis anterior de SendHTTP10Outbound se maneja del siguiente modo:

- SendHTTP10Outbound on se trata como si se hubiese especificado SendHTTP10Outbound \*.
- SendHTTP10Outbound off se ignora.

**Nota:** Si se especifican SendHTTP10Outbound off y SendHTTP10Outbound *patrón\_url*, SendHTTP10Outbound off se ignora, pero se emite un mensaje de aviso.

### Valor por omisión

Ninguno

## SendRevProxyName: especificar el nombre de sistema principal de Caching Proxy en la cabecera HOST

Sólo se aplica a configuraciones de proxy de retorno.

Al funcionar como un proxy de retorno, Caching Proxy recibe peticiones HTTP de un cliente y envía las peticiones al servidor de origen. Por omisión, Caching Proxy escribe el nombre de sistema principal del servidor de origen en la cabecera HOST de la petición que se envía al servidor de origen. Si esta directiva SendRevProxyName se establece en yes, Caching Proxy escribe su propio nombre de sistema principal en la cabecera HOST en su lugar. Esta directiva puede utilizarse para habilitar la configuración especial de servidores de programa de fondo, ya que permite que la petición al servidor de origen siempre aparezca si procediese del servidor proxy, incluso cuando la petición se redirige de un servidor de programa de fondo a otro.

Esta directiva difiere de las directivas de correlación ReversePass del modo siguiente: la directiva ReversePass intercepta las peticiones con una sintaxis especificada y sustituye el contenido de petición distinto que especifique. La directiva SendRevProxyName sólo puede establecerse para sustituir el nombre de

sistema principal de Caching Proxy por el nombre de sistema principal del servidor de origen. Esta directiva no es útil para configurar Application Service at the Edge.

### Formato

`SendRevProxyName {yes | no}`

## ServerConnGCRun: especificar el intervalo durante el que se ejecuta la hebra de recogida de basura

Esta directiva establece el intervalo durante el cual la hebra de recogida de basura busca las conexiones de servidor que han excedido el tiempo de espera, que se establece con la directiva `ServerConnTimeout`. Utilice esta directiva sólo si la directiva `ServerConnPool` está establecida en `on`.

### Formato

`ServerConnGCRun intervalo_tiempo`

### Ejemplo

`ServerConnGCRun 2 minutes`

### Valor por omisión

`ServerConnGCRun 2 minutes`

## ServerConnPool: especificar la agrupación de conexiones con los servidores de origen

Esta directiva permite que el proxy agrupe las conexiones de salida con los servidores de origen. El establecimiento de esta directiva en `on` mejora el rendimiento y permite aprovechar mejor los servidores de origen que permiten las conexiones persistentes. También puede especificar cuánto tiempo desea mantener una conexión en desuso a través de la directiva `ServerConnTimeout`.

**Nota:** Esta directiva se habilita mejor en un entorno controlado, ya que puede degradar el rendimiento en una situación de proxy de reenvío o en una donde los servidores no sean compatibles con HTTP 1.1.

### Formato

`ServerConnPool {on | off}`

### Valor por omisión

`ServerConnPool off`

## ServerConnTimeout: especificar el periodo máximo de inactividad

Utilice esta directiva para limitar el tiempo permitido sin actividad de red antes de cancelar la conexión. Utilice esta directiva sólo si la directiva `ServerConnPool` está establecida en `on`.

### Formato

`ServerConnTimeout especificación-tiempo`

### Ejemplo

`ServerConnTimeout 30 seconds`

## Valor por omisión

ServerConnTimeout 10 seconds

## ServerInit: personalizar el paso de inicialización de servidor

Utilice esta directiva para especificar una función de aplicación personalizada a la que el servidor llama durante las rutinas de inicialización. Este código se ejecuta antes de que se lea cualquier petición de cliente y siempre que el servidor se reinicie.

Si está utilizando los módulos GoServe en los pasos de PreExit o de servicio, es necesario que aquí llame al módulo gosclone.

### Formato

ServerInit /*vía\_acceso/archivo:nombre\_función*  
[*serie\_inicialización*]

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

*serie\_inicialización*

Es opcional y especifica una serie de texto que se pasa a la función de aplicación.

### Ejemplo

ServerInit /ics/api/bin/icsext05.so:svr\_init

## Valor por omisión

Ninguno

## ServerRoot: especificar el directorio donde se instala el programa servidor

Utilice esta directiva para especificar el directorio dónde se va a instalar el programa servidor, es decir, el directorio de trabajo actual del servidor. Las directivas de registro cronológico utilizan este directorio de trabajo actual como el directorio raíz por omisión cuando se utilizan los nombres de vías de acceso relativas.

En los sistemas Windows, el directorio se identifica durante la instalación.

### Formato

ServerRoot *vía\_acceso\_directorio*

### Valores por omisión

- **Sistemas Linux y UNIX:** ServerRoot /opt/ibm/edge/cp/server\_root/
- **Sistemas Windows:** C:\Archivos de programa\IBM\edge\cp\bin\

**Nota:** Puede modificar el valor por omisión, pero no tiene ningún efecto sobre el modo en que el servidor procesa las peticiones.

**Nota:** Las normas PASS y EXEC pueden ser independientes de este directorio.

## ServerTerm: personalizar el paso de terminación de servicio

Utilice esta directiva para especificar una función de aplicación personalizada a la que el servidor llama durante el paso de terminación de servicio. Este código se ejecuta cuando se produce una conclusión ordenada y siempre que el servidor se reinicie. Le permite liberar los recursos asignados por una función de aplicación PreExit

### Formato

ServerTerm */vía\_acceso/archivo:nombre\_función*

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

### Ejemplo

ServerTerm /ics/api/bin/icsext05.so:shut\_down

### Valor por omisión

Ninguno

## Service: personalizar el paso de servicio

Utilice esta directiva para especificar una función de aplicación personalizada a la que el servidor llama durante el paso de servicio. Este código da servicios a la petición de cliente. Por ejemplo, envía el archivo o ejecuta el programa CGI.

No existe un valor por omisión para esta directiva. Si la petición coincide con una norma Service, es decir, si se ejecuta una función de aplicación especificada en una directiva Service, pero la función devuelve HTTP\_NOACTION, el servidor genera un error y la petición no se realiza correctamente.

### Formato

Service *plantilla\_petición/vía\_acceso/archivo:nombre\_función*  
[*dirección\_IP\_servidor* | ]

*plantilla\_petición*

Especifica una plantilla para las peticiones que determinan adicionalmente si se llama a la función de aplicación. La especificación puede incluir el protocolo, el dominio y el sistema principal; puede estar precedida por una barra inclinada (/), y puede utilizar un asterisco (\*) como carácter comodín. Por ejemplo, /front\_page.html , http://www.ics.raleigh.ibm.com, /pub\*, /\* y \* son todas válidas.

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre de la función de aplicación del programa.

[*dirección\_IP\_servidor* | ]

Si utiliza varias direcciones IP o sistemas principales virtuales, este parámetro determina si sólo se llama a la función de aplicación para las peticiones que entren en una dirección IP específica o para un sistema principal específico.

No puede especificarse un carácter comodín para la dirección IP de un servidor.

## Ejemplos

```
Service /index.html /ics/api/bin/icsext05.so:serve_req
Service /cgi-bin/hexcalc* /ics/api/calculator:HEXcalc*
```

**Nota:** Si desea una traducción de la vía de acceso completa, incluido *serie\_consulta*, debe tener un asterisco (\*) tanto en *plantilla\_petición* como en *vía\_acceso/archivo:nombre\_función*, como muestra el segundo ejemplo.

## Valor por omisión

Ninguno

## SignificantURLTerminator; especificar un código de terminación para las peticiones URL

Utilice esta directiva para especificar un código de terminación de las peticiones URL. La utilización del código de terminación en una petición provoca que Caching Proxy evalúe sólo los caracteres que aparecen antes del código de terminación durante el proceso de la petición y al evaluar si el resultado ya está colocado en antememoria. Cuando se define más de un código de terminador, Caching Proxy compara los URL de entrada con los códigos de terminador en el orden en el que están definidos en el archivo ibmproxy.conf.

## Formato

SignificantURLTerminator *serie\_terminación*

## Ejemplo

SignificantURLTerminator &.

En este ejemplo, las dos peticiones que siguen aparecen a continuación se tratan de igual modo.

```
http://www.exampleURL.com/tx.asp?id=0200&. ;x=004;y=001
http://www.exampleURL.com/tx.asp?id=0200&. ;x=127;y=034
```

## Valor por omisión

Ninguno

## SMTPServer (Windows sólo): establecer un servidor SMTP para la rutina sendmail

Utilice esta directiva para establecer el servidor SMTP utilizado por la rutina sendmail de Caching Proxy para Windows. Las dos directivas siguientes también deben establecerse para esta rutina: “WebMasterEMail: establecer una dirección de correo electrónico para recibir informes de servidor seleccionados” en la página 294 y “WebMasterSocksServer (Windows sólo): establecer un servidor socks para la rutina sendmail” en la página 295.

## Formato

SMTPServer *dirección IP o nombre de sistema principal del servidor SMTP*

## Ejemplo

SMTPServer mybox.com

## Valor por omisión

Ninguno

## SNMP: habilitar e inhabilitar el soporte SNMP

Utilice esta directiva para habilitar o inhabilitar el soporte SNMP.

### Formato

SNMP {on | off}

### Valor por omisión

SNMP off

## SNMPCommunity: proporcionar una contraseña de seguridad para SNMP

Utilice esta directiva para definir la contraseña entre el subagente DPI (Distributed Protocol Interface) del servidor Web y el agente SNMP. El nombre de la comunidad SNMP autoriza a un usuario a visualizar las variables de rendimiento supervisadas por SNMP para una comunidad especificada de servidores. El administrador del sistema define qué variables de los servidores pueden visualizarse cuando se especifica una contraseña. Si modifica el nombre de la comunidad SNMP, asegúrese también de modificar el nombre de comunidad especificado en el archivo `/etc/snmpd.conf`.

### Formato

SNMPCommunity *nombre*

### Valor por omisión

SNMPCommunity public

## SSLCaching: habilitar la colocación en antememoria de una petición segura

Utilice esta directiva para colocar en antememoria el contenido de una petición segura cuando se utiliza un servidor proxy de retorno. Esta directiva configura la colocación en antememoria de todas las conexiones con el servidor proxy, tanto las conexiones de cliente como las conexiones con un servidor de contenido de programa de fondo.

**Nota:** Las directivas SSL no reciben soporte en SUSE Linux.

### Formato

SSLCaching {on | off}

### Valor por omisión

SSLCaching off

## SSLCertificate — Especificar etiquetas de clave para certificados

Utilice esta directiva para especificar las etiquetas de clave que permiten al proxy determinar qué certificado se va a enviar al cliente cuando Caching Proxy esté actuando como un único proxy de retorno para varios dominios que ofrezcan sus propios certificados SSL y para indicar al servidor proxy que recupere o no un certificado PKI de la parte cliente para la autenticación de cliente.

Utilizando la directiva SSLCertificate, Caching Proxy puede distinguir entre un certificado emitido por una autoridad de certificación (CA) o un certificado autoasignado. Sin embargo, al aceptar un certificado emitido por cualquier CA

(opción `ClientAuthRequired`), el uso de esta directiva puede permitir a los usuarios que no sean válidos obtener acceso al servidor proxy. Al utilizar la opción `ClientAuthRequired` en la directiva `SSLCertificate`, puede utilizar la opción de expresión lógica para determinar qué usuarios válidos pueden acceder al canal SSL.

Cuando se añade una expresión lógica adicional a la directiva `SSLCertificate`, `Caching Proxy` extrae valores del certificado de cliente y calcula la expresión lógica. Si los valores del certificado del cliente son satisfactorios para la expresión, `Caching Proxy` otorga al cliente el uso de la conexión SSL; en caso contrario, se cierra la conexión.

## Formato

`SSLCertificate Ipservidor/nombresistppal EtiquetaCertificado`  
`[NoClientAuth | ClientAuthRequired expresión-lógica]`

*Ipservidor/nombresistppal*

Puede especificar una dirección IP (por ejemplo, 240.146.167.72) o un nombre de sistema principal (por ejemplo, sistppalA.raleigh.ibm.com) para el servidor al que se dirige la petición SSL.

*EtiquetaCertificado*

Nombre del certificado que se va a utilizar si la autenticación de cliente es necesaria para las peticiones SSL dirigidas a la dirección IP o el nombre de sistema principal designados.

*[NoClientAuth | ClientAuthRequired expresión-lógica]*

Instrucciones dirigidas al servidor proxy para recuperar o no un certificado PKI de la parte cliente.

La opción de expresión lógica sólo es válida cuando se utiliza con la opción `ClientAuthRequired`. Cuando se añade una expresión lógica adicional a la directiva `SSLCertificate`, `Caching Proxy` extrae valores del certificado de cliente y calcula la expresión lógica. Si los valores del certificado del cliente son satisfactorios para la expresión, `Caching Proxy` otorga al cliente el uso de la conexión SSL; en caso contrario, se cierra la conexión.

- El nombre de atributo en la expresión lógica puede ser: IST, ICN, IOU, IC, IL, IO, IE, ST, CN, OU, C, L, O, E.
  - El nombre de atributo se correlaciona con los siguientes campos en el certificado de cliente: 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).
- El valor del nombre de atributo debe delimitarse con comillas.
- Los operadores lógicos válidos son: `&&` (AND), `||` (OR), `!` (NOT), `=` (EQUAL).

## Ejemplos

```
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")
```

## Valor por omisión

Ninguno

## SSLCryptoCard: especificar la tarjeta criptográfica instalada

Sólo se aplica a configuraciones de proxy de retorno.

Utilice esta directiva para indicar al servidor proxy que hay una tarjeta criptográfica instalada y para especificar la tarjeta.

En AIX, para dar soporte a la tarjeta IBM 4960 PCI Cryptographic Accelerator Card, consulte “PKCS11DefaultCert, PKCS11DriverPath, PKCS11TokenPassword — Da soporte a la tarjeta IBM 4960 PCI Cryptographic Accelerator Card (sólo AIX)” en la página 255.

### Formato

SSLCryptoCard {rainbowcs | nciphernfast} {on | off}

### Ejemplo

SSLCryptoCard rainbowcs on

### Valor por omisión

Ninguno

## SSLEnable: especificar la escucha de peticiones seguras en el puerto 443

Utilice esta directiva para especificar que Caching Proxy escucha las peticiones seguras en el puerto 443.

**Nota:** Las directivas SSL no reciben soporte en SUSE Linux.

### Formato

SSLEnable {on | off}

### Valor por omisión

SSLEnable off

## SSLForwardPort: especificar a qué puerto dirigirse para las actualizaciones HTTP SSL

Utilice esta directiva para especificar el puerto al que dirigirse para las peticiones HTTP que Caching Proxy actualiza a peticiones HTTPS mediante la implementación SSL. Especifique un puerto distinto del puerto HTTP principal 80 o el puerto SSL principal 443.

### Formato

SSLForwardPort *número de puerto*

### Ejemplo

SSLForwardPort 8888

### Valor por omisión

Ninguno

## SSLOnly — Inhabilitar hebras de receptor para peticiones HTTP

Utilice esta directiva para inhabilitar las hebras de receptor de las peticiones HTTP estándar (generalmente puertos 80 y 8080) cuando se habilita SSL (generalmente el puerto 443).



### Formato

SSLOnly {on | off}

### Valor por omisión

SSLOnly off

## SSLPort: especificar un puerto de escucha HTTPS distinto del puerto por omisión

Utilice esta directiva para especificar el puerto de escucha HTTPS distinto del puerto HTTPS por omisión 443 de ibmproxy.

**Nota:** ibmproxy da soporte a un puerto HTTPS para cada instancia, de modo que la directiva NO debe utilizarse para especificar varios puertos HTTPS. Para dar soporte a varios puertos HTTPS, debe iniciar varias instancias ibmproxy con archivos ibmproxy.conf distintos.

### Formato

SSLPort *valor de puerto*

donde *valor de puerto* es un valor entero mayor que 0. Asimismo, el sistema operativo debe permitir *valor de puerto*, que no puede utilizar ninguna otra aplicación.

### Ejemplo

SSLPort 8443

### Valor por omisión

443

## SSLTunneling: habilitar los túneles SSL

Sólo se aplica a configuraciones de proxy de reenvío.

Activar esta directiva (valor on) habilita los túneles SSL para cualquier puerto del servidor de destino. Desactivar esta directiva (valor off) sólo habilita los túneles SSL para los puertos indicados en las normas Proxy. Si no existe ninguna norma Proxy para los túneles SSL, y la directiva SSLTunneling se establece en off, no se permitirán los túneles SSL. Si la directiva SSLTunneling se establece en on, también debe habilitar el método CONNECT mediante la directiva Enable.

Debe habilitar esta directiva si utiliza Caching Proxy como proxy de reenvío. Sin embargo, al utilizar Caching Proxy como proxy de retorno, la inhabilitación de esta directiva (por omisión) protege contra los ataques a la vulnerabilidad de los túneles SSL.

Para obtener más información, consulte “Túneles SSL” en la página 121.

**Nota:** Utilice la directiva Proxy para habilitar los túneles SSL para un puerto específico del sistema principal de destino.

### Formato

SSLTunneling {on | off}

### Valor por omisión

SSLTunneling off

## SSLVersion: especificar la versión de SSL

Utilice esta directiva para especificar la versión de SSL que se va a utilizar: V2, V3 o todas las versiones. Establezca esta directiva en V2 si está utilizando servidores que no pueden dar soporte a SSL Versión 3.

**Nota:** Las directivas SSL no reciben soporte en SUSE Linux.

### Formato

SSLVersion {SSLV2 | SSLV3 | all}

### Valor por omisión

SSLVersion SSLV3

## SSLV2Timeout: especificar el tiempo de espera antes de que caduque una versión de SSLV2

Utilice esta directiva para especificar en segundos durante cuánto tiempo una sesión de SSL versión 2 espera sin actividad antes de que caduque la sesión.

**Nota:** Las directivas SSL no reciben soporte en SUSE Linux.

### Formato

SSLV2Timeout *segundos*

donde *segundos* representa un valor entre 0 y 100.

### Valor por omisión

SSLV2Timeout 100

## SSLV3Timeout: especificar el tiempo de espera antes de que caduque una versión de SSLV3

Utilice esta directiva para especificar en segundos durante cuánto tiempo una sesión de SSL versión 3 espera sin actividad antes de que caduque.

**Nota:** Las directivas SSL no reciben soporte en SUSE Linux.

### Formato

SSLV3Timeout *segundos*

donde *segundos* representa un valor entre 1 y 86400 segundos (que es 1 día en segundos).

### Valor por omisión

SSLV3Timeout 100

## SuffixCaseSense: especificar si las definiciones de sufijo son sensibles a las mayúsculas y minúsculas

Utilice esta directiva para especificar si desea que el servidor distinga entre mayúsculas y minúsculas cuando los sufijos de archivo se comparen con los patrones de sufijo de las directivas AddClient, AddCharSet, AddType, AddEncoding y AddLanguage. Por omisión, el servidor no realiza la distinción entre mayúsculas y minúsculas.

### Formato

SuffixCaseSense {on | Off}

## Valor por omisión

SuffixCaseSense Off

## SupportVaryHeader: almacenar en antememoria más de una variante de un recurso basándose en la cabecera Vary de HTTP

Utilice esta directiva para permitir a Caching Proxy almacenar en antememoria más de una variante de un recurso (URI) basándose en la cabecera Vary de HTTP.

Cuando esta habilitada la directiva SupportVaryHeader, el proxy forma un ID de antememoria basándose en el URI y los valores de cabecera seleccionados en la petición del cliente.

Los nombres de las cabeceras seleccionadas se especifican en la cabecera Vary enviada en una respuesta anterior desde el servidor. Si el servidor cambia el conjunto de nombres de cabecera de un recurso, todos los objetos de antememoria anteriores del recurso se eliminan de la antememoria del proxy.

Esta directiva se puede utilizar con la directiva RegisterCacheIdTransformer (“RegisterCacheIdTransformer: almacenar en antememoria más de una variante de un recurso basándose en la cabecera Cookie” en la página 275).

Cuando se utilizan ambas directivas, el proxy crea un transformador interno de ID de antememoria basándose en la cabecera Vary del servidor y en la cabecera de la petición del cliente. De esta forma, el proxy puede generar identificadores de antememoria exclusivos para pares de petición y respuesta distintos, aunque los URI solicitados sean los mismos.

Los objetos de antememoria del mismo URI tienen su propia vida por omisión en la antememoria, en función de las cabeceras Expire y Cache-Control de las peticiones/respuestas, u otros valores de configuración. Si se utiliza el plug-in Dynacache, todas las presentaciones asociadas al mismo URI pasan a ser no válidas en la antememoria del proxy.

### Formato

SupportVaryHeader {on | off}

### Ejemplo

En este ejemplo, se habilitan y configuran las directivas en ibmproxy.conf, tal y como se indica:

```
SupportVaryHeader on
RegisterCacheIdTransformer Cookie UserGroup
```

El cliente Guest accede al servidor proxy con

URI [`<code>`] `http://www.dot.com/group.jpg` [`</code>`]

y la siguiente petición/respuesta:

```
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
.....
```

A continuación, el cliente Admin accede al servidor proxy con el mismo URI  
`http://www.dot.com/group.jpg`

y la siguiente petición/respuesta:

```
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
.....
```

Como resultado, si las respuestas se pueden almacenar en antememoria, el servidor proxy genera dos ID de antememoria distintos:

1. `CacheID(URI, "Guest", "en_US")`
2. `CacheID(URI, "Admin", "fr_FR")`

El servidor proxy almacena dos variantes distintas de las respuestas del servidor en la antememoria. Posteriormente, cuando cualquier cliente solicita el recurso (`.../group.jpg`), con una combinación de valores de preferencia de idioma y de grupos de usuarios, el servidor proxy recupera la variante adecuada del recurso de la antememoria y la proporciona.

### Valor por omisión

`SupportVaryHeader off`

## TLSV1Enable: habilitar el protocolo TLS (Transport Layer Secure)

Utilice esta directiva para habilitar el protocolo TLS versión 1 en las conexiones SSL. Después de activar esta directiva, la conexión SSL primero comprueba el protocolo TLS, seguidamente el protocolo SSLv3 y por último el protocolo SSLv2.

**Nota:** Esta directiva funciona con Internet Explorer y otros navegadores, pero no con Netscape. (Netscape no se recomienda como navegador al utilizar Caching Proxy.)

### Formato

`TLSV1Enable {on | off}`

### Ejemplo

`TLSV1Enable on`

### Valor de configuración inicial

Ninguno

## Transmogrieff: personalizar el paso de manipulación de datos

Utilice esta directiva para especificar una función de aplicación personalizada a la que el servidor llama durante el paso de manipulación de datos. Este código proporciona tres funciones de aplicación:

- Una función *open* para realizar cualquier inicialización anterior al proceso de datos
- Una función *write* para procesar los datos
- Una función *close* para realizar cualquier actividad de limpieza

- Una función *error* para proporcionar las notificaciones de los problemas ocurridos

Puede tener varios Transmogrifiers para cada instancia del servidor.

### Formato

Transmogrifier

*/vía\_acceso/archivo: nombre\_función:nombre\_función:nombre\_función*

*/vía\_acceso/archivo*

Especifica el nombre de archivo plenamente cualificado del programa compilado, incluida la extensión.

*nombre\_función*

Especifica el nombre que se da a la función de aplicación del programa. Debe proporcionar el nombre de las funciones open, write y close.

### Ejemplo

Transmogrifier /ics/bin/icsext05.so:open\_data:write\_data:close\_data

### Valor por omisión

Ninguno

## TransmogrifiedWarning: enviar un mensaje de aviso al cliente

Utilice esta directiva para enviar un mensaje al cliente informándole de los datos:

### Formato

transmogrifiedwarning {yes|no}

### Valor por omisión

Yes

## TransparentProxy — Habilitar el proxy transparente en Linux

Sólo se aplica a configuraciones de proxy de reenvío.

Sólo para sistemas **Linux**, utilice esta directiva para especificar si el servidor puede ejecutarse o no como servidor proxy transparente.

Cuando la directiva TransparentProxy se establece en on, la directiva BindSpecific se pasa por alto y toma el valor off por omisión. Como la mayoría del tráfico HTTP fluye a través del puerto 80, se recomienda que sea uno de los puertos configurados.

### Formato

TransparentProxy {on | off}

Port 80

### Valor por omisión

TransparentProxy off

Si se utiliza el cortafuegos IPCHAIN, basta con habilitar esta directiva para configurar satisfactoriamente el proxy transparente. Si se utiliza el cortafuegos IPTABLES, tendrá que añadir manualmente la norma del cortafuegos IPTABLES.

Si utiliza el cortafuegos IPTABLES, cuando se habilite la directiva TransparentProxy y **antes de iniciar el servidor proxy**, ejecute el mandato siguiente para añadir la norma de cortafuegos a IPTABLES:

```
iptables -t nat -A PREROUTING -i interfaz-red-usuario -p tcp --dport 80 -j  
REDIRECT --to-port puerto-escucha-ibmproxy
```

Suponiendo que el cortafuegos y el servidor proxy estén en el mismo receptáculo, esta norma indica al cortafuegos IPTABLES que redirija todo el tráfico de TCP designado para el puerto 80 al puerto de escucha del proxy local. La norma también se puede añadir a la configuración de IPTABLES. Esto permite que la norma se cargue automáticamente cuando se reinicie el sistema.

**Después de iniciar el proxy transparente**, si desea detener el servidor Caching Proxy, también debe emitir el siguiente mandato como root:

```
ibmproxy -unload
```

En los sistemas Linux, este mandato elimina las normas de cortafuegos de redirección. Si no emite este mandato después de detener el servidor, la máquina aceptará las peticiones que no está dirigidas a él.

## UpdateProxy: especificar el destino de antememoria

Utilice esta directiva para especificar qué servidor proxy actualizará el agente de antememoria. Esta directiva es necesaria cuando el agente de antememoria debe actualizar un servidor proxy distinto del servidor proxy local donde está en ejecución el agente de antememoria. Opcionalmente, puede especificar el puerto.

**Nota:** En las plataformas Linux y UNIX, esta directiva es necesaria para utilizar el agente de antememoria. Si sólo está utilizando una máquina para el proxy, especifique el nombre de sistema principal.

Aunque el agente de antememoria puede actualizar la antememoria en otro servidor, no puede recuperar las anotaciones cronológicas de acceso a la antememoria desde esa máquina. Por lo tanto, si la directiva UpdateProxy especifica un sistema principal que sea distinto del sistema principal local, la directiva LoadTopCached se ignora.

### Formato

UpdateProxy *nombre\_de\_sistppal\_plenamente\_cualificado\_de\_server\_proxy*

### Ejemplo

UpdateProxy proxy15.ibm.com:1080

### Valor por omisión

Ninguno

## Userld: especificar el ID de usuario por omisión

Utilice esta directiva para especificar el nombre o número de usuario al que cambia el servidor antes de acceder a los archivos.

Si modifica esta directiva, debe detener y reiniciar el servidor manualmente para que el cambio entre en vigor. El servidor no reconoce el cambio si sólo lo reinicia. (Consulte el Capítulo 5, “Inicio y detención de Caching Proxy”, en la página 15.)

**Nota:** Si cambia los valores por omisión del servidor para el ID de usuario, el ID de grupo o las vías de acceso de directorios de anotaciones cronológicas, cree los nuevos directorios y actualice los permisos y la propiedad de éstos. Para permitir que el servidor escriba la información en un directorio de anotaciones cronológicas definidas por el usuario, establezca el permiso para

ese directorio como 755 y el ID de usuario del servidor definido por el usuario como el propietario. Por ejemplo, si cambia el ID de usuario del servidor del valor por omisión a jdoe y el directorio de anotaciones cronológicas por omisión a server\_root/account, el directorio server\_root/account debe tener el permiso 755 y ser propiedad de jdoe.

### Formato

UserId {*nombre\_ID* | *número*}

### Valor por omisión

AIX, Linux, Solaris: UserId nobody

HP-UX: UserId www

## V2CipherSpecs: enumerar las especificaciones de cifrado soportadas para SSL Versión 2

Esta directiva enumera las especificaciones de cifrado disponibles para SSL Versión 2.

**Nota:** Las directivas SSL no reciben soporte en SUSE Linux.

### Formato

V2CipherSpecs *especificación*

Los valores aceptables son cualquiera de las combinaciones siguientes. Ninguno puede utilizarse dos veces.

- 1 — RC4 US
- 2 — RC4 Export
- 3 — RC2 US
- 4 — RC2 Export
- 6 — DES 56-bit
- 7 — Triple DES US
- NULL — se utilizan las especificaciones de cifrado por omisión

### Ejemplos

- Para Estados Unidos: V2CipherSpecs '137624'
- Para exportar: V2 Cipherspecs '246'

### Valor por omisión

Ninguno (SSL está inhabilitada por omisión).

## V3CipherSpecs: enumerar las especificaciones de cifrado soportadas para SSL Versión 3

Esta directiva enumera las especificaciones de cifrado disponibles para SSL Versión 3.

**Nota:** Las directivas SSL no reciben soporte en SUSE Linux.

Si la directiva FIPSEnable está establecida en "on", se ignorará la directiva V3CipherSpecs. Para obtener más información, consulte "FIPSEnable: cifrados aprobados por FIPS (Enable Federal Information Processing Standard) para SSLV3 y TLS" en la página 222.

## Formato

V3CipherSpecs *especificación*

Los valores aceptables son los siguientes:

- 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 — se utilizan las especificaciones de cifrado por omisión.

## Ejemplos

- Para los Estados Unidos: V3CipherSpecs '0A09060564620403020100'
- Para exportar: V3Cipherspecs '0906646203020100'

## Valor por omisión

Ninguno (SSL está inhabilitada por omisión).

## WebMasterEMail: establecer una dirección de correo electrónico para recibir informes de servidor seleccionados

Utilice esta directiva para establecer una dirección de correo electrónico donde recibir informes de Caching Proxy seleccionados como, por ejemplo, un aviso 30 días antes de la fecha de caducidad de un certificado SSL. En los sistemas Linux y UNIX debe estar en ejecución un proceso sendmail. Para los sistemas Windows, el proceso sendmail se crea dentro de Caching Proxy de modo que no es necesario ningún servidor de correo externo; no obstante, deben establecerse dos directivas adicionales: “WebMasterSocksServer (Windows sólo): establecer un servidor socks para la rutina sendmail” en la página 295 y “SMTPServer (Windows sólo): establecer un servidor SMTP para la rutina sendmail” en la página 283.

**Nota:** Esta dirección de correo electrónico también se utiliza como contraseña FTP anónima.

## Formato

WebMasterEMail *direccióncorreo electrónicoWebmaster*

## Ejemplo

WebMasterEmail webmaster@computer.com

## Valor por omisión

WebMasterEmail webmaster



## WebMasterSocksServer (Windows sólo): establecer un servidor socks para la rutina sendmail

Utilice esta directiva para establecer el servidor socks utilizado por la rutina sendmail de Caching Proxy para Windows. Las dos directivas siguientes también deben establecerse para esta rutina: "WebMasterEMail: establecer una dirección de correo electrónico para recibir informes de servidor seleccionados" en la página 294 y "SMTPServer (Windows sólo): establecer un servidor SMTP para la rutina sendmail" en la página 283.

### Formato

*WebMasterSocksServer dirección IP o sistema principal de servidores socks*

### Ejemplo

*WebMasterSocksServer socks.mybox.com*

### Valor por omisión

Ninguno

## Welcome: especificar los nombres de los archivos de bienvenida

Utilice esta directiva para especificar el nombre de un archivo de bienvenida que el servidor busca para responder a las peticiones que no contienen un nombre de archivo específico. Puede crear una lista de archivos de bienvenida introduciendo varias apariciones de esta directiva en el archivo de configuración.

Para las peticiones que no contienen un nombre de archivo o nombre de directorio, el servidor siempre busca en el directorio raíz un archivo que coincida con un nombre especificado en una directiva Welcome. Si se encuentra una coincidencia, el archivo se devuelve al solicitante.

Para las peticiones que contienen un nombre de directorio pero carecen de un nombre de archivo, la directiva AlwaysWelcome controla si el servidor busca en el directorio un archivo de bienvenida para devolverlo. Por omisión, AlwaysWelcome se establece en un valor de 0n. Esto significa que el servidor siempre busca en el directorio solicitado un archivo que coincida con un nombre especificado en una directiva Welcome. Si se encuentra una coincidencia, el archivo se devuelve al solicitante.

Si el servidor encuentra más de una coincidencia entre los archivos de un directorio y los nombres de archivo de las directivas Welcome, el orden de las directivas Welcome determina qué archivo se devuelve. El servidor utiliza la directiva Welcome más cercana a la parte superior del archivo de configuración.

### Formato

*Welcome nombre\_archivo [dirección\_IP\_servidor | nombre\_sistppal]*

*nombre\_archivo*

Especifica el nombre de un archivo que desee definir como archivo de bienvenida.

*[dirección\_IP\_servidor | nombre\_sistppal]*

Si está utilizando varias direcciones IP o sistemas principales virtuales, utilice este parámetro para especificar una dirección IP o un nombre de sistema principal. El servidor utiliza la directiva sólo para las peticiones que llegan al

servidor en esta dirección IP o para este sistema principal. Para una dirección IP, esta es la dirección de la conexión de red del servidor, no la dirección del cliente solicitante.

Puede especificar una dirección IP (por ejemplo, 240.146.167.72) o un nombre de sistema principal (por ejemplo, sistppalA.bcd.com ).

Este parámetro es opcional. Sin este parámetro, el servidor utiliza la directiva para todas las peticiones, independientemente de la dirección IP en la que entran las peticiones o el nombre de sistema principal de los URL.

No puede especificarse un carácter comodín para la dirección IP de un servidor.

## Ejemplos

- En el ejemplo siguiente se definen dos páginas de bienvenida y se asume que la directiva AlwaysWelcome se establece en su valor por omisión de 0n. Para las peticiones que no contienen un nombre de archivo, el servidor intenta devolver un archivo de bienvenida desde el directorio especificado en la petición o bien el directorio raíz del archivo si la petición no especifica un nombre de archivo ni directorio. El servidor busca primero un archivo denominado letsgo.html. Si no encuentra ningún archivo con ese nombre en el directorio, el servidor busca un archivo denominado Welcome.html.

```
Welcome letsgo.html
Welcome Welcome.html
```

- En el siguiente ejemplo, el servidor busca distintos archivos de bienvenida basados en la dirección IP de la conexión de red en la que entra la petición. Para las peticiones que entren en 0.67.106.79, el servidor busca los archivos de bienvenida ClienteA.html. Para las peticiones que entren en 0.83.100.45, el servidor busca los archivos de bienvenida ClienteB.html. Si la petición entra en una dirección IP distinta, el servidor busca la dirección por omisión.

```
Welcome ClienteA.html 0.67.106.79
Welcome ClienteB.html 0.83.100.45
```

- En el siguiente ejemplo, el servidor busca distintos archivos de bienvenida basados en el nombre de sistema principal del URL. Para las peticiones que entren para sistppalA, el servidor busca los archivos de bienvenida ClienteA.html. Para las peticiones que entren para sistppalB, el servidor busca los archivos de bienvenida ClienteB.html. Si la petición entra para un sistema principal distinto, el servidor busca el nombre de sistema principal por omisión.

```
Welcome ClienteA.html sistppalA.bcd.com
Welcome ClienteB.html sistppalB.bcd.com
```

## Valores por omisión

Estos valores por omisión están en el orden utilizado por la configuración por omisión:

```
Welcome Welcome.html
Welcome welcome.html
Welcome index.html
Welcome Frntpage.html
```

---

## Avisos

### Primera edición (mayo de 2006)

Esta información se ha desarrollado para productos y servicios proporcionados en los Estados Unidos.

Es posible que IBM no ofrezca los productos, servicios o funciones que se tratan en este documento en otros países. Consulte el representante de IBM de su localidad para obtener información acerca de los productos y servicios que están disponibles actualmente en su localidad. Cualquier referencia que se haga a un producto, programa o servicio de IBM no implica que sólo se pueda utilizar dicho producto, programa o servicio de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ningún derecho de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o aplicaciones pendientes de patente que conciernan al tema descrito en este documento. El suministro de este documento no le da ninguna licencia sobre estas patentes. Puede enviar preguntas acerca de licencias por escrito a:

IBM Corporation  
Attn.: G71A/503  
P.O. box 12195  
3039 Cornwallis Rd.  
Research Triangle Park, N.C. 27709-2195  
Estados Unidos

Para preguntas acerca de licencias referentes a información de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe sus preguntas por escrito a:

IBM World Trade Asia Corporation Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106, Japón

**El siguiente párrafo no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones no coincidan con la legislación local:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTE DOCUMENTO "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS O CONDICIONES IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas legislaciones no contemplan la exclusión de garantías, explícitas o implícitas en algunas transacciones, por lo que puede haber usuarios a los que no les afecte dicha regla.

Esta publicación puede contener imprecisiones técnicas o errores tipográficos. La información que ofrece está sometida a modificaciones periódicas, las cuales se van

incorporando en ediciones posteriores. IBM se reserva el derecho de realizar mejoras y/o cambios en los productos o programas descritos en esta publicación en cualquier momento sin previo aviso.

Cualquier referencia en esta información a sitios web que no son de IBM se proporciona solamente para su comodidad y no equivale de ninguna manera a una aprobación de esos sitios web. El material de dichos sitios Web no forma parte del material correspondiente a este producto IBM y el uso de estos sitios Web se realiza bajo riesgo del usuario.

IBM puede utilizar o distribuir cualquier información que el usuario le proporcione de la manera que considere adecuada sin incurrir en ninguna obligación con el usuario.

Los usuarios autorizados de este programa que deseen tener información sobre el mismo con el propósito de posibilitar: (i) el intercambio de información entre programas creados independientemente y otros programas (incluyendo éste) y (ii) la utilización mutua de la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation  
ATTN: Software Licensing  
11 Stanwix Street  
Pittsburgh, PA 15222-9183  
Estados Unidos

Esta información puede estar disponible, bajo las condiciones y los términos adecuados, incluyendo en algunos casos, el pago de una cuota.

El programa con licencia descrito en este documento y todos los materiales con licencia disponibles para el mismo son proporcionados por IBM bajo los términos del acuerdo IBM International Program License Agreement o cualquier acuerdo equivalente entre nosotros.

Cualquier información de rendimiento contenida aquí fue determinada en un entorno controlado. Por tanto, los resultados obtenidos en otros entornos operativos pueden variar de forma significativa. Pueden haberse realizado algunas mediciones en sistemas en nivel de desarrollo y no existen garantías de que estas mediciones sean las mismas en sistemas disponibles para todos los usuarios. Además, algunas mediciones pueden haberse calculado mediante extrapolaciones. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su entorno específico.

La información referente a productos que no son de IBM se ha obtenido de los suministradores de estos productos, sus anuncios publicados u otras fuentes disponibles para el público. IBM no ha probado estos productos y no puede confirmar la precisión del rendimiento, compatibilidad y otras afirmaciones relacionadas con productos que no son de IBM. Las preguntas acerca de las posibilidades de productos que no son de IBM deben dirigirse a los suministradores de estos productos.

Todas las declaraciones referentes a acciones e intenciones futuras de IBM pueden cambiar o ser retiradas sin aviso previo y solamente representan objetivos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones diarias de negocios. Para ilustrarlos de la manera más completa posible, los ejemplos pueden incluir nombres de personas, compañías, marcas y productos.

Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones utilizadas por una empresa de negocios real es mera coincidencia.

Si accede a esta información mediante una presentación visual, las fotografías e ilustraciones en color no aparecerán.

---

## Marcas registradas

Los siguientes términos son marcas registradas IBM Corporation en Estados Unidos, otros países o en ambos:

- AIX
- IBM
- Netfinity
- RS/6000
- SecureWay
- Tivoli
- ViaVoice
- WebSphere

Java y todas las marcas basadas en Java son marcas registradas de Sun Microsystems, Inc. en los Estados Unidos u otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas de Microsoft Corporation en los Estados Unidos, en otros países o en ambos.

Intel, Intel Inside (logos), MMX y Pentium son marcas registradas de Intel Corporation en Estados Unidos, en otros países o en ambos.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos, en otros países o en ambos.

Otros nombres de empresas, productos o servicios pueden ser marcas registradas o marcas de servicio de terceros.







Printed in Denmark by IBM Danmark A/S

GC11-3239-00





Spine information:



WebSphere Application Server

Guía de administración de Caching Proxy

Versión 6.1

GC11-3239-00