WebSphere Application Server

Caching Proxy Administration Guide

Versione 6.0.2

GC13-3366-01

WebSphere Application Server

Caching Proxy Administration Guide

Versione 6.0.2

GC13-3366-01

Nota

Prima di usare questo prodotto e le relative informazioni, leggere le informazioni contenute nella sezione “Informazioni particolari” a pagina 277.

Terza edizione (Giugno 2005)

Questa edizione si applica a:
WebSphere Application Server, Versione 6.0.2

e a tutte le release e modifiche successive, finché non verrà diversamente indicato nelle nuove edizioni.

Ordinare le pubblicazioni mediante il rappresentante IBM o gli uffici IBM del proprio paese.

Indice

Figure

Informazioni su questa guida

Questa prefazione descrive i destinatari e lo scopo della presente guida, la sua organizzazione, le funzioni di accessibilità, le convenzioni, la terminologia e la documentazione correlata.

A chi è destinata questa guida

La *Guida alla gestione per Caching Proxy* è destinata ad amministratori di rete e di sistema esperti, con una buona conoscenza dei propri sistemi operativi e della fornitura di servizi Internet. Non è richiesta alcuna precedente esperienza con Caching Proxy.

Questa guida non è destinata a supportare release precedenti di Caching Proxy.

Terminologia e convenzioni adottate in questa guida

Questa documentazione utilizza le seguenti convenzioni tipografiche e di definizione dei tasti.

Tabella 1. Convenzioni utilizzate in questa guida

Convenzione	Significato
Grassetto	Quando si fa riferimento alle interfacce utente grafiche (GUI, Graphical User Interfaces), il grassetto evidenzia menu, voci di menu, etichette, pulsanti, icone e cartelle. Inoltre, può essere utilizzato per enfatizzare i nomi di comandi che, altrimenti, verrebbero confusi con il testo circostante.
`A spaziatura fissa`	Indica il testo da inserire davanti a un prompt di comandi. Inoltre, indica il testo su video, gli esempi di codice ed estratti di file.
Corsivo	Indica i valori delle variabili che l'utente deve inserire (ad esempio, il nome per sostituire *nomeFile* con il nome effettivo di un file). Il corsivo viene inoltre utilizzato per enfatizzare un concetto ed evidenziare i titoli di manuali.
Ctrl-*x*	Dove *x* è il nome di un tasto, indica una sequenza di caratteri di controllo. Ad esempio, Ctrl-c indica: tenere premuto il tasto Ctrl e contemporaneamente premere il tasto c.
Return	Indica il tasto etichettato con la parola Invio, Enter, Return o con una freccia verso sinistra.
`%`	Rappresenta il prompt della shell dei comandi di Linux e UNIX per un comando che non richiede i privilegi di root.
`#`	Rappresenta il prompt della shell dei comandi di Linux e UNIX per un comando che richiede i privilegi di root.
`C:\`	Rappresenta il prompt dei comandi di Windows.
Immissione di comandi	Quando si invita l'utente a "immettere" o "inserire" un comando, digitare il comando e premere Invio. Ad esempio, l'istruzione "Immettere il comando **ls**" indica: digitare **ls** al prompt dei comandi e premere Invio.
[ ]	Racchiude le voci facoltative nelle descrizioni della sintassi.
{ }	Racchiude gli elenchi da cui è necessario scegliere una voce nelle descrizioni della sintassi.
|	Separa le voci in un elenco di opzioni racchiuse tra parentesi { } nelle descrizioni della sintassi.

Tabella 1. Convenzioni utilizzate in questa guida (Continua)

Convenzione	Significato
...	I puntini di sospensione nelle descrizioni della sintassi indicano che è possibile ripetere la voce precedente una o più volte. Negli esempi, indicano che le informazioni sono state omesse dall'esempio per motivi di brevità.

Accessibilità

Le funzioni di accessibilità consentono ad un utente con un svantaggi fisici, quali una mobilità o una vista limitata, di utilizzare agevolmente prodotti software. Queste sono le principali funzioni di accessibilità in WebSphere Application Server, Versione 6.0.2:

- È possibile utilizzare un software di lettura dello schermo e un sintetizzatore vocale digitale per ascoltare ciò che viene visualizzato sullo schermo. Inoltre, è possibile utilizzare un software di riconoscimento vocale, quale IBM ViaVoice, per immettere dati e spostarsi all'interno dell'interfaccia utente.
- Le funzioni possono essere utilizzate tramite la tastiera invece che tramite il mouse.
- È possibile configurare e gestire le funzioni di Application Server utilizzando editor di testo standard e interfacce della riga comandi invece delle interfacce grafiche fornite. Per ulteriori informazioni sull'accessibilità di particolari funzioni, fare riferimento alla documentazione corrispondente.

Come inviare i propri commenti

I vostri commenti risultano di estrema importanza poiché consentono di fornire informazioni della massima accuratezza e qualità. In caso di commenti su questa guida o su altra documentazione relativa a Edge Components di WebSphere Application Server:

- Inviare i commenti per e-mail a fsdoc@us.ibm.com. Accertarsi di includere il nome della guida, il numero di sezione, la versione di WebSphere Application Server e, se il caso, il punto specifico del testo che si sta commentando, quale un numero di pagina o un numero di tabella.

Informazioni correlate

- *Concepts, Planning, and Installation for Edge Components*, GC31-6855-02
- *Programming Guide for Edge Components*, GC31-6856-02
- *Guida alla gestione per Load Balancer*, GC31-6858-02
- *Architettura di IBM WebSphere Edge Services*
- Sito Web home di IBM: *www.ibm.com/*
- Sito Web del prodotto IBM WebSphere Application Server: *www.ibm.com/software/webservers/appserv/*
- Sito Web della libreria per IBM WebSphere Application Server: *www.ibm.com/software/webservers/appserv/library.html*
- Sito Web del supporto per IBM WebSphere Application Server: *www.ibm.com/software/webservers/appserv/support.html*
- Centro informazioni per IBM WebSphere Application Server: *www.ibm.com/software/webservers/appserv/infocenter.html*
- Centro informazioni per IBM WebSphere Application Server Edge Components: *www.ibm.com/software/webservers/appserv/ecinfocenter.html*

Parte 1. Informazioni relative a Caching Proxy

Questa sezione fornisce una panoramica del componente Caching Proxy, istruzioni per l'uso dei moduli di Gestione e configurazione e del wizard di configurazione, istruzioni per la modifica manuale del file ibmproxy.conf e procedure per l'avvio e l'arresto di server proxy.

Di seguito vengono forniti i titoli di ciascun capitolo di questa sezione:

Capitolo 1. Panoramica

Caching Proxy intercetta le richieste di dati da un client, recupera le informazioni desiderate dalle macchine su cui è memorizzato il contenuto e le fornisce al client. Di norma, le richieste riguardano documenti memorizzati su server Web, detti anche server di origine o host di contenuti, e fornite mediante il protocollo HTTP (Hypertext Transfer Protocol). Tuttavia, è possibile configurare Caching Proxy per la gestione di altri protocolli, quali FTP (File Transfer Protocol) e Gopher.

Caching Proxy memorizza il contenuto che può essere salvato nella cache prima di consegnarlo al richiedente. Tra gli esempi di contenuto memorizzabile nella cache sono comprese pagine Web statiche e FILE JSP (JavaServer Page) con frammenti generati in modo dinamico ma soggetti a modifiche poco frequenti. La memorizzazione nella cache consente a Caching Proxy di soddisfare le successive richieste dello stesso contenuto fornendolo direttamente dalla cache locale, con una velocità molto maggiore di quanto avverrebbe recuperandolo di nuovo dall'host dei contenuti.

IMPORTANTE: Caching Proxy è disponibile su tutte le installazioni Edge Components, con le seguenti eccezioni:

- Caching Proxy non è disponibile per le installazioni Edge Components in esecuzione su processori a 64 bit Itanium 2 o AMD Opteron.
- Caching Proxy non è disponibile per le installazioni Edge Components di Load Balancer for IPv6.

Nuove funzioni

La *Guida alla gestione per Caching Proxy* comprende nuove funzioni, nuove piattaforme supportate e aggiornamenti correttivi per la versione 6.0 e per le release successive alla versione 5.0 (5.0.1, 5.0.2, 5.1 e 5.1.1).

Le nuove funzioni più significative per V6.0.2 sono:

- **Direttiva di abilitazione FIPS**

  Questa nuova direttiva abilita le codifiche approvate di FIPS per il protocollo SSLV3 e TLS nelle connessioni SSL. Per ulteriori informazioni, vedere "FIPSEnable — Indica di abilitare la crittografia approvata FIPS (Federal Information Processing Standard) per SSLV3 e TLS" a pagina 208.
- **Direttive per abilitare Caching Proxy alla memorizzazione nella cache di più varianti di una risorsa (URI)**

  Due nuove direttive consentono a Caching Proxy di memorizzare nella cache e richiamare più varianti di un URI basato sulle intestazioni HTTP Vary e Cookie.

  Per maggiori informazioni, consultare "SupportVaryHeader — Indica di memorizzare nella cache più di una variante di una risorsa, in base all'intestazione HTTP Vary" a pagina 268 e "RegisterCacheIdTransformer — Indica di memorizzare più di una variante di una risorsa, in base all'intestazione Cookie" a pagina 255.

Le nuove funzioni più significative per V6.0, V6.0.1 e post-V5.0 sono:

- **Nuovo supporto piattaforma**

Per informazioni complete sulle piattaforme supportate per Edge Components V6, accedere alla seguente pagina Web di WebSphere Application Server, `http://www.ibm.com/software/webservers/appserv/doc/latest/prereq.html`

- **Supporto su Linux per S/390, zSeries, iSeries e pSeries**

  Oltre a supportare l'esecuzione di Caching Proxy su Linux per Intel, il proxy viene ora eseguito su Linux per S/390, zSeries, iSeries e pSeries.

- **Supporto su AIX 5.2 e AIX 5.3**

  Oltre ad AIX 5.1, Caching Proxy supporta ora AIX 5.2 e AIX 5.3.

- **Supporto su Solaris 9**

  Oltre a Solaris 8, Caching Proxy supporta ora Solaris 9.

- **Supporto su Windows Server 2003**

  Oltre a Windows 2000, Caching Proxy supporta ora Windows Server 2003.

- **Supporto su HP-UX Versione 11i**

  Oltre al supporto per i sistemi AIX, Linux, Solaris e Windows, Caching Proxy supporta HP-UX.

- **Supporto per JDK 1.4.2**

  È ora supportata una nuova versione di JDK a 32 bit: JDK 1.4.2.

- **Supporto per GSKit 7**

  Una nuova versione di GSKit viene fornita e installata per impostazione predefinita con Caching Proxy: GSKit 7.

- **Migliorie e nuove direttive per la riscrittura delle giunzioni**

  Sono presenti migliorie e nuove direttive per la riscrittura delle giunzioni. Per ulteriori informazioni, vedere:

  - "Abilitazione della riscrittura delle giunzioni (facoltativa)" a pagina 44
  - "JunctionReplaceUrlPrefix — Indica di sostituire l'URL anziché inserire il prefisso, se si utilizza il plugin JunctionRewrite" a pagina 217
  - "JunctionSkipUrlPrefix — Indica di ignorare la riscrittura degli URL che già contengono il prefisso, quando si utilizza il plugin JunctionRewrite" a pagina 219
  - "JunctionRewriteSetCookiePath — Indica di riscrivere l'opzione di percorso nell'intestazione Set-Cookie, quando si utilizza il plugin JunctionRewrite" a pagina 218
  - "RewriteSetCookieDomain — Indica di specificare un modello del dominio da riscrivere" a pagina 257
  - "Proxy — Indica di specificare i protocolli proxy o il proxy inverso" a pagina 247

  Inoltre, è prevista un'alternativa all'uso del plugin JunctionRewrite. Per ulteriori informazioni, vedere:

  - "UseCookie come alternativa a JunctionRewrite" a pagina 46
  - "JunctionRewrite — Indica di attivare la riscrittura dell'URL" a pagina 218

- **Ulteriori nuove direttive**

  Sono supportate le seguenti nuove direttive:

  - "CacheMatchLanguage — Indica di specificare la preferenza lingua per il contenuto cache restituito" a pagina 184
  - "EnableTcpNodelay — Indica di abilitare l'opzione socket TCP NODELAY" a pagina 202
  - Direttive per la limitazione delle richieste:

- "LimitRequestBody — Indica di specificare la dimensione corpo massima nelle richieste PUT o POST" a pagina 220
- "LimitRequestFields — Indica di specificare il numero massimo di intestazioni nelle richieste client" a pagina 220
- "LimitRequestFieldSize — Indica di specificare la lunghezza massima dell'intestazione e della riga della richiesta" a pagina 221

– Direttive per il salvataggio o il caricamento della memoria cache su disco:
- "ExportCacheImageTo — Indica di esportare la memoria cache su disco" a pagina 206
- "ImportCacheImageFrom — Indica di importare la memoria cache da un file" a pagina 216

• **Migliorie alle direttive esistenti**

Sono state apportate migliorie alle seguenti direttive esistenti:

– BindSpecific: l'opzione `OutgoingSrcIp` consente al proxy di utilizzare un indirizzo IP di origine specifico per l'esecuzione di connessioni in uscita.

– ReversePass: l'opzione `host:porta` consente al proxy di applicare diverse regole ReversePass a seconda del nome host e della porta del server backend.

• **Plugin Transmogrifier di esempio fornito per estendere la funzionalità JunctionRewrite**

Per JunctionRewrite, viene ora fornito del codice di esempio personalizzabile che riscrive/analizza i blocchi di tag JavaScript (SCRIPT) e applet (APPLET) nei file HTML. (Da solo, il plugin JunctionRewrite non può elaborare i collegamenti a risorse in JavaScript o nei valori dei parametri di Java). Per ulteriori informazioni, vedere "Plugin Transmogrifier di esempio per estendere la funzionalità JunctionRewrite" a pagina 47.

• **Modifiche relative alla configurazione del daemon PACD**

Per consentire associazioni anonime, vedere "Creazione di pac_ldap.cred" a pagina 137.

Per una connessione SSL tra un proxy e un server LDAP, collocare la password del database delle chiavi nel file pac_keyring.pwd. Vedere "Creazione di un nuovo database di chiavi, password e file stash" a pagina 119.

• **Modifiche alla configurazione predefinita per aumentare la sicurezza**

Nel file di configurazione (ibmproxy.conf), sono state apportate modifiche alle impostazioni predefinite per fornire una maggiore sicurezza. Ad esempio, sono state apportate modifiche per disabilitare HTTP CONNECTION e il tunneling SSL. Non sono presenti nuove direttive per questa miglioria.

Capitolo 2. Utilizzo dei moduli di Gestione e configurazione

Caching Proxy comprende moduli HTML che possono essere forniti ai client richiedenti e utilizzati per configurare il server proxy. Tali moduli eseguono programmi CGI che modificano il file di configurazione del server proxy locale, ibmproxy.conf. Per utilizzarli, il server proxy deve essere in esecuzione e configurato per passare i moduli dalla directory locale in cui risiedono.

Per impostazione predefinita, Caching Proxy viene installato con direttive Pass comprese nel file ibmproxy.conf, che consentono l'accesso ai moduli di Gestione e configurazione. Quando un client richiede la pagina iniziale predefinita da questo server proxy, viene fornita la pagina Frntpage.html. Questa contiene un collegamento ipertestuale alla pagina iniziale dei moduli di Gestione e configurazione, wte.html.

I moduli di Gestione e configurazione sono protetti e richiedono l'autenticazione del client prima della trasmissione. Per istruzioni sull'impostazione dell'ID e della password dell'amministratore, fare riferimento a "Impostazione della password dell'amministratore" a pagina 9.

Requisiti del browser

Un browser Web utilizzato per accedere ai moduli di Gestione e configurazione deve supportare quanto segue:

- *HTML 4.0*: tutti i moduli sono scritti secondo la specifica HTML 4.0. Il browser Web deve supportare HTML 4.0 e i frame.
- *Java 1.1 e JavaScript*: le applet sono scritte secondo la specifica Java 1.1. Il browser Web deve supportare una JVM (Java Virtual Machine) compatibile con Java 1.1. Le applet sono incompatibili con le JVM (Java Virtual Machine) conformi alla specifica Java 2.0. È necessario abilitare sia JavaScript che Java.
- *256 colori*: la workstation su cui viene eseguito il browser Web deve supportare almeno 256 colori.

I browser **consigliati** sono Mozilla 1.4 o Mozilla 1.7 (per i sistemi Linux e UNIX) o Internet Explorer (per i sistemi Windows). Fare riferimento a *Informazioni di base, pianificazione e installazione per Edge Components* per ulteriori informazioni sui browser per la visualizzazione dei moduli di configurazione e amministrazione.

Note:

1. Sui sistemi Linux PowerPc a 64 bit, non sarà possibile accedere ai moduli di Gestione e configurazione con il browser Mozilla, poiché per questa architettura non è disponibile SDK. In alternativa, è possibile accedere ai moduli di Gestione e configurazione da una macchina diversa, dotata di un browser Web supportato.
2. Se viene richiesto due volte di effettuare il login all'avvio della console di gestione, è possibile che le impostazioni Java in Internet Explorer non siano corrette. Per risolvere questo problema in Internet Explorer, selezionare **Strumenti>Opzioni Internet>Avanzate** ed eliminare il segno di spunta dalla casella **Usa Java 2 v1.4.X**.

Accesso ai moduli di Gestione e configurazione

Per accedere ai moduli di Gestione e configurazione:

1. Accertarsi che il server proxy sia in esecuzione. Per istruzioni sull'avvio del server proxy, fare riferimento a Capitolo 5, "Avvio e arresto di Caching Proxy", a pagina 15.
2. Indirizzare un browser HTTP per richiedere la propria pagina iniziale del server proxy (Frntpage.html) o la pagina iniziale di Gestione e configurazione (wte.html).

   Nota: Questa pagina varia a seconda delle regole di mappatura effettive nel server proxy e può essere diversa dalle pagine predefinite indicate tra parentesi.

   `http://nome.proprio.server[:porta][/directory][/pagina.html]`

   in cui

   - *nome.proprio.server* è il percorso completo del proprio host, ad esempio `http://www.ibm.com/`.
   - [:*porta*] Se il server proxy riceve richieste di gestione su una porta diversa dalla 80, includere il numero di porta dopo il nome del server: `http://nome.proprio.server:porta`
   - [*/directory*] L'aggiunta di una directory all'interno dell'URL dipende dalla regola di mappatura.
   - [*/pagina.html*] La pagina HTML deve essere specificata solo se non è elencata come pagina iniziale. Per informazioni sulle pagine iniziali, fare riferimento a "Definizione delle pagine di benvenuto predefinite" a pagina 50.
3. Fare clic su **Moduli di Gestione e configurazione** per accedere ai moduli di configurazione del server. Viene richiesto il nome utente dell'amministratore e la password. Immettere un nome utente e una password autorizzati. Viene visualizzata la finestra del client di configurazione di Caching Proxy.

   Note:

   a. Il caricamento dei contenuti del frame di navigazione sulla sinistra può richiedere alcuni secondi dopo la visualizzazione della pagina principale.
   b. Sui sistemi Windows 2003, le connessioni che richiedono moduli di gestione (script CGI) possono essere riavviate prima del loro completamento. Di conseguenza, i browser potrebbero segnalare di non aver ricevuto dati o che la pagina da visualizzare non è disponibile. Per evitare questo problema, aumentare MaxActiveThreads a un valore maggiore di 200, o aumentare ConnThreads a un valore maggiore di 50 per risolvere il riavvio delle connessioni. Vedere "MaxActiveThreads — Indica di specificare il numero massimo di thread attivi" a pagina 226 e "ConnThreads — Indica di specificare il numero di thread di connessione da utilizzare per la gestione delle connessioni" a pagina 193 per ulteriori informazioni su queste direttive.
4. Il pannello di navigazione sulla sinistra mostra le cinque categorie principali dei moduli di configurazione:
   - **Configurazione proxy**
   - **Configurazione cache**
   - **Configurazione server**
   - **Controllo attività del server**
   - **Configurazione plug-in**

Fare clic sul puntatore triangolare sulla sinistra di un'intestazione per espandere l'elenco dei moduli di configurazione in quella categoria. Fare clic su un modulo per aprirlo. Il modulo illustra i valori di configurazione attuali (se presenti) nei campi di immissione; se la configurazione non è stata modificata dopo l'installazione, si tratta dei valori predefiniti.

5. Su qualsiasi modulo, immettere le informazioni di configurazione per la funzione specifica. Ciascun modulo è corredato da istruzioni che guidano l'utente nella decisione circa le modifiche da apportare. Per ulteriori informazioni, fare clic sull'icona della guida, il punto interrogativo (**?**) sulla parte superiore di ciascun modulo. Tale icona fornisce i seguenti collegamenti:
   - **Guida per il campo**—Descrizioni dei campi in ciascun pannello della schermata
   - **Come...**—Fasi dettagliate dell'uso del modulo per svolgere operazioni specifiche
   - **Indice**—Un indice delle informazioni della guida
6. Dopo aver compilato un modulo, fare clic su **Inoltra** per aggiornare la configurazione del server con le modifiche apportate. Il pulsante **Inoltra** si trova al di sotto dei campi di immissione in ciascun modulo. Se non si desidera rendere effettive le modifiche apportate al modulo, fare clic su **Ripristina** e i campi del modulo torneranno ai valori originali.
7. Se si fa clic su **Inoltra** e i dati immessi vengono accettati, nel frame superiore viene visualizzato il seguente messaggio:

   ```
   Le modifiche alla configurazione richieste sono state completate correttamente
   ```

   Se i dati immessi non vengono accettati, nel frame superiore viene visualizzato un messaggio di errore che indica le impostazioni non accettabili.
8. Per riavviare il server proxy, fare clic sull'icona di riavvio del server (|) nel frame superiore. Quando il server proxy riceve il comando di riavvio, smette di accettare richieste dai client, ma completa eventuali richieste già in corso. Dopo aver ricaricato il file di configurazione modificato, il proxy viene avviato e ricomincia ad accettare richieste dai client.

   Nota: La modifica di determinate direttive, mediante i moduli di Gestione e configurazione o la modifica manuale del file ibmproxy.conf, richiede il completo arresto del server e il suo riavvio per rendere effettive le modifiche, anziché il solo riavvio. Tali direttive sono elencate in Tabella 6 a pagina 165.

Impostazione della password dell'amministratore

Dopo aver installato i pacchetti di Caching Proxy, è necessario creare un ID utente e una password dell'amministratore per l'accesso ai moduli di Gestione e configurazione. La configurazione predefinita del server proxy prevede l'autenticazione degli utenti che richiedono i moduli di Gestione e configurazione mediante il file di password webadmin.passwd nella directory /opt/ibm/edge/cp/server_root/protect/ su Linux e sistemi UNIX o nella directory \Programmi\IBM\edge\cp\etc\ sui sistemi Windows. L'installazione dei pacchetti non sovrascrive un file webadmin.passwd esistente.

Per aggiungere una voce amministratore al file webadmin.passwd, utilizzare i comandi seguenti:

- Su sistemi Linux e UNIX:

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

Quando richiesto, fornire al programma **htadm** un nome utente, una password e un nome completo per l'amministratore.

- Su sistemi Windows:

```
cd "\Programmi\IBM\edge\cp\root_server\protect\"
htadm -adduser webadmin.passwd"
```

  Quando richiesto, fornire al programma **htadm** un nome utente, una password e un nome completo per l'amministratore.

Nota: Il nome utente e la password per l'amministratore prevedono la distinzione tra maiuscole e minuscole, anche se il sistema operativo non la prevede. Durante l'accesso ai moduli di Gestione e configurazione, accertarsi di digitare il nome utente e la password esattamente come sono stati immessi mediante il comando `htadm`.

Per una descrizione dettagliata del comando **htadm**, fare riferimento a "Comando htadm" a pagina 157.

Capitolo 3. Uso del Wizard di configurazione

Il Wizard di configurazione di Caching Proxy consente di configurare rapidamente un Caching Proxy installato. Questo programma imposta solo le direttive essenziali, necessarie a modificare il funzionamento di Caching Proxy perché funga da surrogato. Il server proxy può richiedere ulteriori operazioni di configurazione.

Per utilizzare il Wizard di configurazione di Caching Proxy:

1. Avviare il Wizard di configurazione.

   Sui sistemi Windows: fare clic su **Start –> Programmi –> IBM WebSphere –> Edge Components –> Caching Proxy –> Wizard di configurazione**.

   Sui sistemi Linux e UNIX: immettere il comando
   `/opt/ibm/edge/cp/cpwizard/cpwizard.sh`
2. Selezionare la porta di rete su cui il server proxy attende le richieste HTTP.
3. Digitare il nome del server di contenuti di destinazione.
4. Immettere l'ID utente e la password per l'amministratore del server proxy.

Note:

1. Il Wizard di configurazione imposta le seguenti direttive:

   ```
   Port porta
   Proxy /* http://server contenuti :porta
   ```
2. Se si utilizza il Wizard di configurazione per configurare il server proxy, per abilitare SSL è necessario creare una regola di mappatura per le richieste proxy ricevute attraverso la porta 443. Per ulteriori informazioni, fare riferimento a "Definizione delle regole di mappatura" a pagina 41.

   Esempi:

   ```
   Proxy /* http://server contenuti:443
   ```

   o

   ```
   Proxy /* https://server contenuti:443
   ```

Limitazioni: sui sistemi Linux, i tasti di scelta rapida non funzionano per il Wizard di configurazione di Caching Proxy.

Capitolo 4. Modifica manuale del file ibmproxy.conf

È possibile configurare Caching Proxy manualmente, modificando il file di configurazione ibmproxy, oppure utilizzando i moduli di Configurazione e amministrazione.

- Sui sistemi Linux e UNIX, il file ibmproxy.conf si trova nella directory /etc/.
- Sui sistemi Windows, il file ibmproxy.conf si trova in C:\Programmi\IBM\edge\cp\etc\en_US\.

Il file di configurazione è composto da istruzioni dette direttive. Per cambiare la configurazione, modificare il file di configurazione modificando le direttive, quindi salvare le modifiche apportate. È possibile utilizzare qualsiasi editor di testo, quali emacs e vi, per modificare il file di configurazione.

Nota: Non utilizzare l'editor di file di testo compreso in Solaris Common Desktop Environment (CDE). L'editor di Solaris a volte modifica il gruppo di appartenenza del file e le proprietà del suo collegamento, per cui i moduli di Gestione e configurazione non possono scrivere sul file di configurazione.

Le modifiche apportate al file di configurazione hanno effetto dopo il riavvio del server, a meno che non sia stata modificata una delle direttive identificate in Tabella 6 a pagina 165. In tal caso, è necessario arrestare il server, quindi riavviarlo. Per le istruzioni, consultare Capitolo 5, "Avvio e arresto di Caching Proxy", a pagina 15.

Appendice B, "Direttive del file di configurazione", a pagina 165 descrive ciascuna direttiva del file di configurazione e fornisce dettagli sulla relativa sintassi.

Capitolo 5. Avvio e arresto di Caching Proxy

Caching Proxy è progettato per l'esecuzione continuativa come processo in background con intervento minimo da parte dell'operatore. In genere, il server proxy viene avviato durante il ciclo di avvio della macchina e arrestato solo in caso di interventi di manutenzione. Il server proxy può essere avviato manualmente in caso di necessità. Inoltre, è possibile passare al server proxy un'istruzione di riavvio, che arresta e riavvia il server proxy senza danni per le connessioni client attive.

Avvio e arresto automatico sui sistemi Linux e UNIX

Sui sistemi Linux e UNIX, uno script di inizializzazione **ibmproxy** e i relativi collegamenti simbolici vengono collocati nelle directory /etc/ adeguate durante l'installazione di Caching Proxy. Tali script vengono quindi integrati nelle routine di avvio e arresto del sistema operativo. È possibile modificare le impostazioni di configurazione per il riavvio automatico modificando lo script **ibmproxy** e cambiando le opzioni del comando **ibmproxy**.

Nota: Limite per i descrittori dei file in Solaris

È possibile che lo script di inizializzazione di Caching Proxy non imposti il numero massimo desiderato per i descrittori dei file a causa di un limite di tutto il sistema Solaris relativo ai descrittori di file. Se il valore di sistema massimo è inferiore all'impostazione nello script di inizializzazione di Caching Proxy, viene utilizzato il limite per il sistema. È possibile modificare il limite di descrittori di file per evitare problemi di prestazioni del proxy dovute a un valore troppo basso (inferiore a 1024). Immettere il comando **ulimit** per visualizzare il numero di descrittori attualmente disponibili. Se il valore è inferiore a 1024, aumentare il limite dei descrittori di file. Per aumentare tale limite a 1024, aggiungere la riga seguente al file /etc/system:

```
set rlim_fd_cur=0x400
```

Disattivazione dell'avvio e arresto automatico

Per disattivare l'avvio e l'arresto automatico:

- Sui sistemi AIX, eliminare il comando **ibmproxy** dal file di inizializzazione.
- Sui sistemi HP-UX, eliminare i seguenti collegamenti a **ibmproxy**:
  - /sbin/rc1.d/K154ibmproxy
  - /sbin/rc2.d/S880ibmproxy
- Sui sistemi Linux, eliminare i collegamenti simbolici a **/etc/rc.d/init.d/ibmproxy** nelle sottodirectory del livello di esecuzione.

  Su SUSE Linux, eliminare i seguenti collegamenti a **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

Su Red Hat Linux, eliminare i seguenti collegamenti a **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
- Sui sistemi Solaris, eliminare il comando **ibmproxy start** e i due relativi script di interruzione come segue:
  - Eliminare S88ibmproxy dalla directory /etc/rc2.d.
  - Eliminare K54ibmproxy dalla directory /etc/rc0.d.
  - Eliminare K54ibmproxy dalla directory /etc/rc1.d.

Avvio manuale sui sistemi Linux e UNIX

A prescindere dal metodo di avvio, il comando **ibmproxy** può essere richiamato direttamente dal prompt dei comandi o dall'interno di uno script. Per una descrizione dettagliata del comando **ibmproxy**, fare riferimento a "Comando ibmproxy" a pagina 162. Vengono forniti di seguito esempi degli argomenti di uso più comune.

Su AIX:

- Per avviare il server proxy per le impostazioni internazionali predefinite, utilizzando il comando **startsrc**, immettere quanto segue:

  ```
  startsrc -s ibmproxy
  ```
- Per avviare il server proxy per qualsiasi impostazione internazionale diversa da quella predefinita, utilizzando il comando **startsrc**, immettere quanto segue:

  ```
  startsrc -s ibmproxy -e "LC_ALL=locale"
  ```
- Per avviare il server proxy con le impostazioni di runtime predefinite, senza utilizzare il comando **startsrc**, immettere quanto segue:

  ```
  ibmproxy
  ```

Su HP-UX:

- Per avviare il server proxy eseguendo lo script di inizializzazione, immettere quanto segue al prompt di root:

  ```
  /sbin/init.d/ibmproxy start
  ```
- Per avviare il server proxy come processo in background senza eseguire lo script di inizializzazione, immettere quanto segue al prompt di root:

  ```
  /usr/sbin/ibmproxy
  ```
- Per avviare il server proxy come processo in primo piano senza eseguire lo script di inizializzazione, immettere quanto segue al prompt di root:

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

In Linux:

- Per avviare il server proxy eseguendo lo script di inizializzazione, immettere quanto segue al prompt di root:

  ```
  /etc/rc.d/init.d/ibmproxy start
  ```
- Per avviare il server proxy come processo in background senza eseguire lo script di inizializzazione, immettere quanto segue al prompt di root:

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

- Per avviare il server proxy come processo in primo piano senza eseguire lo script di inizializzazione, immettere quanto segue al prompt di root:

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

- Per avviare il server proxy utilizzando un file di configurazione SQUID preesistente, squidConfig.file, immettere quanto segue al prompt di root:

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

  dove il file *errors_icons.conf* identifica le icone da utilizzare per i tipi di file indicati durante la visualizzazione dei contenuti delle directory.

In Solaris:

- Per avviare il server proxy eseguendo lo script di inizializzazione, immettere quanto segue al prompt di root:

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

- Per avviare il server proxy come processo in background senza eseguire lo script di inizializzazione, immettere quanto segue al prompt di root:

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

- Per avviare il server proxy come processo in primo piano senza eseguire lo script di inizializzazione, immettere quanto segue al prompt di root:

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

Avvio come servizio di Windows

Se Caching Proxy viene installato come servizio di Windows, viene avviato come qualsiasi altro servizio di Windows:

1. Fare clic su **Start –> Impostazioni (per Windows 2000) –> Pannello di controllo**.
2. Nella finestra del **Pannello di controllo**, fare doppio clic su **Strumenti di amministrazione –> Servizi**.
3. Nella finestra **Servizi**, evidenziare **Caching Proxy**.
4. Fare clic su **Avvia** per avviare il servizio Caching Proxy.

Se Caching Proxy viene installato come un servizio, può essere configurato per l'avvio automatico all'avvio di Windows. In tal caso, non è necessario accedere al sistema per consentire al proxy di soddisfare le richieste. Per avviare automaticamente il proxy:

1. Fare clic su **Start –> Impostazioni (per Windows 2000) –> Pannello di controllo**.
2. Nella finestra del **Pannello di controllo**, fare doppio clic su **Strumenti di amministrazione –> Servizi**.
3. Nella finestra **Servizi**, evidenziare **Caching Proxy**.
4. Fare clic sul pulsante di scelta **Automatico**, quindi su **Avvia** per avviare il servizio Caching Proxy automaticamente all'avvio di Windows.

Aggiornamento della variabile d'ambiente PATH

Se Caching Proxy è contrassegnato come `Avviato` nella finestra **Servizi**, ma il proxy non funziona, è possibile che la macchina non sia stata riavviata dopo l'installazione del proxy. Se il servizio Caching Proxy è impostato per interagire con il desktop, il mancato riavvio può inoltre provocare la visualizzazione del

seguente messaggio di errore in una casella a comparsa: `Errore catalogo messaggi: impossibile caricare il catalogo messaggi o catalogo messaggi non valido`

Riavviare la macchina per consentire l'aggiornamento del valore della variabile d'ambiente PATH nel registro di configurazione di Windows. Se il registro di configurazione non viene aggiornato, la variabile PATH potrebbe indicare i percorsi corretti per Caching Proxy e GSK7, ma funzionare in modo errato.

Nota: Esiste un potenziale conflitto per i sistemi Windows quando sia Caching Proxy, sia un'altra applicazione, quale un file system di rete, vengono eseguiti come servizi. A volte Caching Proxy non è in grado di interpretare un percorso contenente un'unità remota gestita da un'applicazione file system anch'essa in esecuzione come servizio.

Il problema può verificarsi se il percorso del servizio file system appare prima del percorso del servizio Caching Proxy nella variabile d'ambiente di Windows PATH. Il problema può essere risolto modificando la variabile PATH per collocare i servizi file system verso la fine delle impostazioni.

Questo problema non influisce sulle unità remote controllate da applicazioni non eseguite come servizi di Windows. Ad esempio, Caching Proxy può accedere alle unità condivise su altre macchine Windows visibili attraverso una rete locale (LAN).

Avvio come applicazione di Windows

Utilizzando il menu Start

Quando Caching Proxy viene installato come applicazione di Windows, la procedura di installazione crea una voce **Caching Proxy** come sottomenu del menu **Start**. Per avviare Caching Proxy come un'applicazione, fare clic su **Start –> Programmi –> IBM WebSphere –> Edge Components –> Caching Proxy**.

Questa procedura di avvio esegue il server proxy con le impostazioni di configurazione correnti. Per specificare altre impostazioni all'avvio, utilizzare la procedura di avvio con comando (vedere la sezione successiva).

Utilizzando il prompt dei comandi

Per avviare il server da qualsiasi prompt dei comandi Windows o DOS, utilizzare il comando **ibmproxy**. Se Windows non è stato arrestato e riavviato dopo l'installazione del server, immettere il percorso completo per questo comando, come segue (per impostazione predefinita):

```
c:\Programmi\IBM\edge\cp\bin\ibmproxy.exe
```

Il comando **ibmproxy** avvia il server con le impostazioni di configurazione correnti. Se la configurazione del server non è stata modificata dopo l'installazione, la configurazione corrente si basa sulle informazioni immesse durante l'installazione e sulle opzioni predefinite.

Il comando **ibmproxy** avvia il server come un'applicazione, anche se Caching Proxy è stato installato per l'esecuzione come servizio. Per forzare l'esecuzione del server come un'applicazione, è inoltre possibile specificare l'opzione di comando **-noservice**. Altre opzioni di comando modificano le impostazioni di configurazione durante il runtime.

Avvio di istanze multiple di server proxy

È possibile eseguire istanze multiple del server proxy simultaneamente, ma ciascuna dovrà rimanere in ascolto su una porta diversa. Sui sistemi AIX, è possibile avviare una sola istanza con SRC. È necessario specificare file di configurazione univoci per tutte le istanze del server, dal momento che il file di configurazione identifica il numero di porta e tale numero deve essere diverso per ciascun server su una determinata macchina. Per avviare un'istanza aggiuntiva del server, quando ne è presente almeno una già in esecuzione, immettere il seguente comando:

- Su Linux e UNIX:

  `ibmproxy -r altro_file_di_configurazione`
- Su Windows:

  `ibmproxy -noservice -r altro_file_di_configurazione`

dove *altro_file_di_configurazione* è un file di configurazione univoco.

Quando si avviano istanze multiple del server, registrare l'ID del processo visualizzato per ciascuna istanza. Tali ID sono necessari per arrestare istanze specifiche del server.

Nota: Sui sistemi Linux con istanze multiple del server in esecuzione, il comando **/etc/rc.d/init.d/ibmproxy stop** arresta solo l'ultimo server avviato. Le altre istanze devono essere arrestate separatamente. Per ulteriori informazioni, fare riferimento a "Arresto manuale sui sistemi Linux e UNIX".

Arresto manuale sui sistemi Linux e UNIX

Per arrestare il server:

- È necessario accedere con l'utente che ha avviato il processo o con il superutente root.
- È necessario utilizzare lo stesso metodo con cui è stato avviato il server. Nella tabella seguente sono elencati i metodi di avvio e i metodi di arresto corrispondenti.

Tabella 2. Metodi di avvio e arresto per i sistemi Linux e UNIX

Metodo di avvio	Metodo di arresto
Da /etc/inittab (su AIX)	Immettere `stopsrc -s ibmproxy`
Da /sbin/init.d (su HP-UX)	Immettere `/sbin/init.d/ibmproxy stop`
Da /etc/rc.d/init.d (su Linux)	Immettere `/etc/rc.d/init.d/ibmproxy stop`
`ibmproxy`	1. Individuare l'ID del processo **ibmproxy** : su AIX, immettere `ps -aef | grep "ibmproxy"`. Su Linux, immettere `ps -aux | grep ibmproxy | grep ID_server`. Su Solaris e HP-UX, immettere `ps -ef | grep "ibmproxy"` 2. Arrestare il processo **ibmproxy**: immettere `kill id_processo` Per arrestare tutti i server su questa macchina: immettere `killall ibmproxy`
`ibmproxy -nobg`	Immettere `ctrl-c`

Tabella 2. Metodi di avvio e arresto per i sistemi Linux e UNIX (Continua)

`ibmproxy -r -`*`altro_file_di_configurazione`*(su AIX)	Immettere `stopsrc -s ibmproxy -p` *`id_processo`*
`ibmproxy -r -`*`altro_file_di_configurazione`*(su Linux)	1. Individuare l'ID del processo **ibmproxy**: immettere `ps aux | grep ibmproxy | grep` *`id_processo`* 2. Arrestare il processo **ibmproxy**: immettere `kill` *`id_processo`*

Per arrestare il server al prompt di root, immettere:

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

Limitazioni ai comandi di arresto

Durante l'uso dei comandi di arresto, si possono sperimentare le seguenti limitazioni:

- **AIX, HP-UX e Linux**

  Sui sistemi AIX, HP-UX e Linux, i comandi per arrestare il sistema Caching Proxy a volte arrestano solo il processo Caching Proxy. Il comando AIX che provoca questo comportamento è **stopsrc -s ibmproxy**. Il comando HP-UX e Linux che provoca questo comportamento è **ibmproxy -stop**.

  Il processo PACD, utilizzato dal server LDAP, potrebbe rimanere in esecuzione dopo l'arresto del server proxy. Il processo PACD può essere arrestato in sicurezza utilizzando il comando **kill** nel modo seguente:

  `kill -15` *`ID_processo_PACD`*

- **Solaris**

  L'immissione del comando **ibmproxy -stop** su un sistema Solaris non ha lo stesso effetto che sugli altri sistemi operativi. A causa di una limitazione nel codice di Solaris, la fase Server Termination del plugin non viene eseguita quando si utilizza **ibmproxy -stop** sulle piattaforme Solaris.

  Questa limitazione ha implicazioni per il software del server proxy e per i plugin implementati dal cliente.

  Il processo PACD, utilizzato dal server LDAP, potrebbe rimanere in esecuzione dopo l'arresto del server proxy. Il processo PACD può essere arrestato in sicurezza utilizzando il comando **kill** nel modo seguente:

  `kill -15` *`ID_processo_PACD`*

Arresto manuale su un sistema Windows

È possibile arrestare il server Caching Proxy analogamente a quanto avviene per gli altri programmi Windows.

Se il proxy è installato come servizio:

1. Fare clic su **Start –> Impostazioni (per Windows 2000) –> Pannello di controllo**.
2. Nella finestra del **Pannello di controllo**, fare doppio clic su **Strumenti di amministrazione –> Servizi**.
3. Nella finestra **Servizi**, evidenziare **Caching Proxy**.

4. Fare clic su **Arresta** per arrestare il servizio Caching Proxy.

Se il proxy non è installato come servizio, eseguire una delle operazioni qui riportate per arrestare Caching Proxy:

- Fare clic sull'icona **x** nell'angolo superiore destro.
- Dal menu **File**, fare clic su **Esci**.
- Premere **Alt + F4**.

Riavvio dopo modifiche alla configurazione

Dopo aver modificato la configurazione del server, mediante i moduli di Gestione e configurazione o la modifica del file ibmproxy.conf, è necessario riavviare il server per rendere effettive le modifiche. Nella maggior parte dei casi, è possibile riavviare il server senza doverlo prima arrestare. Tuttavia, alcune impostazioni non vengono aggiornate da un semplice riavvio. Per ulteriori informazioni, vedere Tabella 6 a pagina 165.

Per riavviare il server senza prima arrestarlo, fare clic sul pulsante **Riavvia** su qualsiasi modulo di Configurazione e amministrazione, oppure immettere quanto segue: `ibmproxy -restart`

Parte 2. Configurazione e ottimizzazione del processo Caching Proxy

Questa sezione illustra l'interazione tra il componente Caching Proxy e il sistema operativo, l'hardware del computer e la rete. Fornisce inoltre procedure per la configurazione di tale interazione. Questi elementi della configurazione di server proxy vengono normalmente gestiti dall'amministratore del sistema e devono essere attentamente coordinati con le risorse di rete, quali indirizzi IP e nomi host, nonché con le risorse di sistema, quale la memoria disponibile e i cicli della CPU.

Di seguito vengono forniti i titoli di ciascun capitolo di questa sezione:

Capitolo 6. Definizione del server

Caching Proxy viene tipicamente eseguito come processo in background su un computer host configurato per agire come server di rete. Questo processo è associato con (*collegato a*) uno o tutti gli indirizzi IP (Internet Protocol) attivi sul computer host. Ascolta diversi protocolli Internet, quali FTP e HTTP, su porte specificate ed esegue azioni per queste richieste in base alla configurazione stabilita per il suo funzionamento. (Per ulteriori informazioni, fare riferimento a Parte 3, "Configurazione del funzionamento di Caching Proxy", a pagina 37.)

Per impostazione predefinita, Caching Proxy assume lo stesso nome del computer host. Questo comportamento predefinito può essere modificato specificando espressamente un nome host per il server proxy. Per associare Caching Proxy a un indirizzo IP specifico, è necessario modificare il nome host del server proxy in modo che corrisponda a quell'indirizzo IP.

Nota: Nel caso in cui il server proxy tenti un'associazione a un indirizzo IP senza che il nome host sia impostato su un indirizzo IP disponibile, l'associazione fallisce e il server proxy rimane in ascolto su tutti gli indirizzi IP disponibili.

Il nome host del server proxy non influisce sulla risoluzione del traffico client. Il server proxy non confronta il proprio nome host con il valore dell'argomento nome host nell'intestazione della richiesta HTTP. Il nome host del server proxy viene a volte incorporato nelle pagine locali con contenuto generato in modo dinamico, quali i messaggi di errore. Viene inoltre trasmesso in risposta al client richiedente come valore dell'argomento ″Via″ nell'intestazione HTTP.

Il server proxy può essere configurato per sostituire il nome host del client che effettua la richiesta con il nome host del server proxy prima di trasmettere la richiesta al server di destinazione. In questo modo, il server di destinazione viene forzato a mantenere il canale di comunicazione attraverso il server proxy, anziché stabilire una connessione diretta con il client.

Definire il processo del server proxy specificando l'ubicazione fisica dei file del server proxy sul computer host, il nome con cui il server proxy fa riferimento a se stesso e le porte su cui è in ascolto come valori per le direttive ServerRoot, Hostname e Port. Se l'host è dotato di indirizzi IP multipli, il server proxy può essere associato a un indirizzo specifico impostando il valore della direttiva BindSpecific su On e il valore della direttiva Hostname sullo specifico indirizzo IP.

Una porta di gestione fornisce un metodo per accedere ai moduli di Gestione e configurazione ed eseguire la manutenzione del server. Per consentire l'accesso al server proxy attraverso una porta di gestione, specificare un valore per la direttiva AdminPort. Le richieste ricevute sulla porta di gestione non vengono accodate a quelle ricevute sulla porta standard. È possibile scrivere regole di mappatura per consentire l'accesso ai moduli di Gestione e configurazione attraverso questa porta.

Quando la direttiva BindSpecific è attivata, Caching Proxy è associato alla porta specificata dalla direttiva Port insieme all'indirizzo IP derivato dal valore della direttiva Hostname. La porta specificata dalla direttiva AdminPort è associata a tutti gli indirizzi IP disponibili sul sistema.

Per ignorare il nome predefinito del server in esecuzione, quale IBM-PROXY o IBM_HTTP_SERVER, specificare un valore per la direttiva HeaderServerName. Questo valore popola il campo Risposte HTTP del server.

Per migliorare le prestazioni del proxy, è possibile impostare il valore della direttiva PureProxy su On. Questo disabilita completamente tutte le funzionalità di cache.

Direttive associate

Le direttive che seguono definiscono il processo del server proxy:

- "Hostname — Indica di specificare il nome dominio completo o l'indirizzo IP del server" a pagina 212
- "ServerRoot — Indica di specificare la directory dove è installato il programma server" a pagina 261
- "HeaderServerName — Indica di specificare il nome del server proxy restituito nell'intestazione HTTP" a pagina 212
- "BindSpecific — Indica di specificare se il server è associato a uno o a tutti gli indirizzi IP" a pagina 179
- "Port — Indica di specificare la porta su cui il server è in ascolto per ricevere richieste" a pagina 238
- "AdminPort — Indica di specificare la porta per richiedere moduli o pagine di amministrazione" a pagina 175
- "PureProxy — Indica di disattivare un proxy dedicato" a pagina 252

Per ulteriori informazioni, fare riferimento a Capitolo 4, "Modifica manuale del file ibmproxy.conf", a pagina 13.

Moduli di Gestione e configurazione

I moduli di Gestione e configurazione che seguono modificano i valori delle direttive associate:

- **Configurazione server –> Impostazioni di base –> Nome host**
- **Configurazione server –> Impostazioni di base –> Root server**
- **Configurazione server –> Impostazioni di base –> Numero porta/e predefinita/e**
- **Configurazione server –> Impostazioni di base –> Numero porta di gestione**
- **Configurazione server –> Impostazioni di base –> Opzioni di associazione**
- **Configurazione proxy –> Prestazioni proxy –> Esegui come un proxy puro**

Nota: Non è possibile utilizzare i moduli di Gestione e configurazione per modificare la direttiva HeaderServerName.

Per ulteriori informazioni, fare riferimento a Capitolo 2, "Utilizzo dei moduli di Gestione e configurazione", a pagina 7.

Capitolo 7. Determinazione della proprietà del processo

Quando un utente diverso dal superutente root avvia Caching Proxy, tale utente mantiene la proprietà di tutti i processi associati al server proxy. Tuttavia, se Caching Proxy viene avviato dal superutente root, una funzione di impostazione dell'ID utente nel server proxy legge le direttive UserId e GroupId nel file ibmproxy.conf e imposta la proprietà del processo all'utente e al gruppo specificati. Questo ha lo scopo di limitare l'accesso ai file e proteggere il computer. Se si modificano le direttive UserId o GroupId, è necessario aggiornare la proprietà e le autorizzazioni per le directory di log e gli altri file, quale una ACL (Access Control List), utilizzati dal server proxy.

Stabilire la proprietà del processo del server proxy specificando l'ID utente, l'ID gruppo e l'ubicazione del file in cui l'ID del processo viene registrato sotto forma di valori per le direttive UserID, GroupID e PidFile.

Per forzare l'esecuzione del processo del server proxy in primo piano, impostare il valore della direttiva NoBG su On.

Su sistemi Linux:

Sui sistemi Linux, verrà modificata la proprietà dei soli processi e thread responsabili dell'ascolto di connessioni. I processi e i thread responsabili di altre attività nel flusso di lavoro saranno ancora di proprietà dell'utente root. Tutti i processi e i thread ricevono numeri ID di processo (PID). Il comando **ps** elenca tutti gli ID di processo, a prescindere dalla loro associazione con un processo o un thread.

Nota: Su alcuni kernel Linux, Caching Proxy potrebbe generare il seguente messaggio di errore nel log degli errori:

```
Impossibile inizializzare i gruppi per l'utente nobody, errore n.: 1
```

È possibile ignorare il messaggio di errore poiché non influisce sul normale funzionamento di Caching Proxy. È possibile risolvere il problema del messaggio di errore esportando le seguenti variabili di ambiente prima di avviare Caching Proxy:

```
esportare RPM_FORCE_NPTL=1
esportare LD_ASSUME_KERNEL=2.4.19:
```

Direttive associate

Le direttive che seguono definiscono la proprietà del processo del server proxy:

- "UserId — Indica di specificare l'ID utente predefinito" a pagina 271
- "GroupId — Indica di specificare l'ID gruppo" a pagina 212
- "NoBG — Indica di eseguire il processo Caching Proxy in primo piano" a pagina 231
- "PidFile (solo Linux e UNIX) — Indica di specificare il file in cui memorizzare l'ID processo di Caching Proxy" a pagina 237

Per ulteriori informazioni, fare riferimento a Capitolo 4, "Modifica manuale del file ibmproxy.conf", a pagina 13.

Moduli di Gestione e configurazione

I moduli di Gestione e configurazione che seguono modificano i valori delle direttive associate:

- **Configurazione server –> Impostazioni di base –> ID utente**
- **Configurazione server –> Impostazioni di base –> ID gruppo**
- **Configurazione server –> Impostazioni di base –> Ubicazione file ID processo**

Nota: Non è possibile utilizzare i moduli di Gestione e configurazione per modificare la direttiva NoBG.

Per ulteriori informazioni, fare riferimento a Capitolo 2, “Utilizzo dei moduli di Gestione e configurazione”, a pagina 7.

Capitolo 8. Gestione delle connessioni

Caching Proxy genera un nuovo thread per gestire ciascuna richiesta client. Se non ci sono thread disponibili, il server proxy tiene in attesa le richieste fino a che non ottiene un maggior numero di thread disponibili. Man mano che il numero di thread attivi aumenta, il server proxy consuma più memoria. Specificare il numero massimo di thread attivi come valore della direttiva MaxActiveThreads.

Il backlog di ascolto è il numero di richieste in sospeso per le connessioni client, registrato dal server prima di rifiutare connessioni ai nuovi client. Basare questa impostazione sul numero di richieste che il server è in grado di elaborare in pochi secondi. Un server deve rispondere a una connessione client prima della sua scadenza. Specificare il numero massimo di connessioni che possono essere mantenute nel backlog come valore della direttiva ListenBacklog.

Il server proxy può mantenere connessioni client/server permanenti. Con una connessione permanente, il server accetta richieste multiple dal client e invia risposte attraverso la stessa connessione TCP/IP. L'uso delle connessioni permanenti riduce la latenza per i client e il carico per la CPU sul server proxy, con il costo minimo di un leggero aumento della memoria del server. La velocità di elaborazione generale aumenta quando il server non stabilisce una connessione TCP/IP distinta per ciascuna richiesta e risposta, e la connessione TCP/IP può essere utilizzata con la massima efficienza quando è permanente.

Il lotto connessioni lato server applica i vantaggi delle connessioni permanenti lato server consentendo di riutilizzare le connessioni esistenti tra il server proxy e i server di origine. Ciascuna connessione riutilizzata risparmia tre pacchetti TCP (due pacchetti di sincronizzazione tridirezionali per impostare la connessione e uno per chiuderla). I vantaggi del lotto connessioni lato server comprendono:

- Minore congestione della rete (grazie alla riduzione al minimo dell'apertura e chiusura di connessioni)
- Minore tempo della CPU utilizzano nei router, client e server
- Minore memoria utilizzata su client e server
- In caso di mancati riscontri della cache, risposta più rapida del proxy (evitando di aprire e chiudere connessioni)

Nota: Il lotto connessioni è consigliato solo in un ambiente controllato. Può ridurre le prestazioni laddove i server di origine non siano compatibili HTTP 1.1. Notare inoltre che è essenziale che i server di origine siano configurati in modo adeguato. Di seguito viene fornito un semplice esempio dal file di configurazione di Apache 1.3.19:

- `#KeepAlive: se consentire o meno connessioni permanenti (più di una richiesta per #connessione). Impostare su Off per disattivarla#`
- `KeepAlive On`
- `#MaxKeepAliveRequests: il numero massimo di richieste da consentire durante una connessione permanente. Impostare a 0 per consentire un numero illimitato. Lasciare questo numero alto per le massime prestazioni#`
- `Max KeepAliveRequests 0`
- `#KeepAliveTimeout: numero di secondi da attendere per la richiesta successiva dallo stesso client sulla stessa connessione#`

- `KeepAliveTimeout 240`

  Queste impostazioni mantengono aperte le connessioni ai server Web per tutto il tempo in cui sono in uso e consentono al proxy, anziché al server di origine, di gestire le connessioni. Di conseguenza, le connessioni vengono organizzate in lotti solo nella misura necessaria.

Quando il lotto connessioni lato server è abilitato, le connessioni HTTP ai server di origine vengono organizzate in lotti. Anche le connessioni SSL vengono organizzate in lotti nelle configurazioni in cui la direttiva SSLEnable per il proxy è impostata su On.

Configurare la modalità di gestione del lotto connessioni specificando il numero massimo di socket inattivi da mantenere per server in qualsiasi momento, il tempo di attesa del server prima di terminare una connessione permanente inattiva e l'intervallo con cui il thread di raccolta dati inutili verifica la presenza di connessioni scadute (il valore predefinito è di due minuti).

Definire il tempo in cui le varie connessioni rimangono aperte specificando i valori delle direttive InputTimeout, OutputTimeout, PersistTimeout, ReadTimeout e ScriptTimeout.

Direttive associate

Le direttive che seguono gestiscono le connessioni con il processo del server proxy:

- "MaxActiveThreads — Indica di specificare il numero massimo di thread attivi" a pagina 226
- "ConnThreads — Indica di specificare il numero di thread di connessione da utilizzare per la gestione delle connessioni" a pagina 193
- "ListenBacklog — Indica di specificare il numero di connessioni client backlog di ascolto che il server può supportare" a pagina 221
- "ProxyPersistence — Indica di autorizzare connessioni permanenti" a pagina 250
- "MaxPersistRequest — Indica di specificare il numero massimo di richieste da ricevere su una connessione permanente" a pagina 227
- "ServerConnPool — Indica di specificare il lotto connessioni ai server di origine" a pagina 260
- "MaxSocketPerServer — Indica di specificare il numero massimo di socket aperti per server" a pagina 228
- "ServerConnTimeout — Indica di specificare il tempo di inattività massimo" a pagina 260
- "ServerConnGCRun — Indica di specificare l'intervallo in cui eseguire il thread di raccolta di dati inutili" a pagina 260
- "PersistTimeout — Indica di specificare il tempo di attesa del client prima di inviare un'altra richiesta" a pagina 236
- "InputTimeout — Indica di specificare il timeout di input" a pagina 217
- "ReadTimeout — Indica di specificare il limite di tempo di una connessione" a pagina 254
- "OutputTimeout — Indica di specificare il timeout dell'output" a pagina 233
- "ScriptTimeout – Indica di specificare l'impostazione di timeout per gli script" a pagina 258

Per ulteriori informazioni, fare riferimento a Capitolo 4, "Modifica manuale del file ibmproxy.conf", a pagina 13.

Moduli di Gestione e configurazione

I moduli di Gestione e configurazione che seguono modificano i valori delle direttive associate:

- **Configurazione server –> Gestione del sistema –> Prestazioni –> Numero massimo di thread attivi**
- **Configurazione server –> Gestione del sistema –> Prestazioni –> Dimensioni del backlog di ascolto**
- **Configurazione proxy –> Prestazioni proxy –> Consenti connessioni permanenti**
- **Configurazione server –> Gestione del sistema –> Prestazioni –> Numero massimo di richieste**
- **Configurazione server –> Gestione del sistema –> Prestazioni –> Timeout persistenza**
- **Configurazione server –> Gestione del sistema –> Timeout –> Timeout in entrata**
- **Configurazione server –> Gestione del sistema –> Timeout –> Timeout lettura**
- **Configurazione server –> Gestione del sistema –> Timeout –> Timeout in uscita**
- **Configurazione server –> Gestione del sistema –> Timeout –> Timeout script**
- **Configurazione server –> Gestione del sistema –> Timeout –> Timeout persistenza**

Note:

1. Non è possibile utilizzare i moduli di Gestione e configurazione per modificare le direttive ServerConnPool, MaxsocketPerServer, ServerConnTimeout o ServerConnGCRun.
2. È possibile modificare PersistTimeout dal modulo **Configurazione server –> Gestione del sistema –> Prestazioni** o dal modulo **Configurazione server –> Gestione del sistema –> Timeout**.

Per ulteriori informazioni, fare riferimento a Capitolo 2, “Utilizzo dei moduli di Gestione e configurazione”, a pagina 7.

Capitolo 9. Ottimizzazione del processo server proxy

È possibile migliorare notevolmente le prestazioni di Caching Proxy impostando correttamente e ottimizzando il sistema. Di seguito vengono forniti alcuni suggerimenti per migliorare l'impostazione e l'ottimizzazione.

Impostazione delle direttive legate alle prestazioni

Le direttive che seguono influiscono in misura significativa sulle prestazioni del processo del server proxy:

- "PureProxy — Indica di disattivare un proxy dedicato" a pagina 252. Questa funzione migliora le prestazioni del sistema disattivando completamente la memorizzazione nella cache.
- "ProxyPersistence — Indica di autorizzare connessioni permanenti" a pagina 250. Questa funzione consente a client e server di mantenere connessioni aperte. Le connessioni permanenti riducono il tempo di ritardo per le richieste di documenti dal server proxy, ma richiedono una maggiore larghezza di banda di rete, oltre a un thread dedicato sul server per ciascuna connessione. Non consentire connessioni permanenti se si impostano limiti per il numero di thread disponibili.

I campi dei moduli di Gestione e configurazione che seguono modificano i valori delle direttive associate:

- **Configurazione proxy –> Prestazioni proxy: Esegui come un proxy puro**
- **Configurazione proxy –> Prestazioni proxy: Consenti connessioni permanenti**

Esame delle altre applicazioni

Esaminare i servizi o daemon in esecuzione sul sistema e rimuovere quelli superflui per aumentare la memoria e i cicli della CPU a disposizione. Ad esempio, se sul sistema viene eseguito un server Web che fornisce solo poche pagine Web, considerare se è il caso di utilizzare solo Caching Proxy come unico server Web. Disattivare altri server Web nel modo seguente:

- Su AIX: esaminare /etc/inittab
- Su Linux: esaminare /etc/rc.d/rc*x*.d per il livello di esecuzione predefinito del sistema (normalmente, 2)
- Su HP-UX e Solaris: esaminare /etc/rc*x*.d per il livello di esecuzione predefinito del sistema (normalmente, 2).
- Su sistemi Windows:
  1. Fare clic su **Start –> Impostazioni (per Windows 2000) –> Pannello di controllo –> Strumenti di amministrazione –> Servizi**.
  2. Consultare i servizi superflui impostati su `Automatico`.
  3. Modificare il tipo di avvio per tali servizi, da `Automatico` a `Manuale`.

Verifica dello spazio di paginazione

Accertarsi che il sistema disponga di spazio di paginazione sufficiente a garantirne il corretto funzionamento. Il sistema richiede uno spazio di paginazione pari al doppio della memoria fisica. Se possibile, distribuire lo spazio di paginazione tra più unità fisiche. Ad esempio, un server Netfinity 5000 con 512 MB di memoria e cinque unità SCSI richiede 1 GB di spazio di paginazione totale, con circa 200 MB su ciascuna unità.

Ottimizzazione del file system

Caching Proxy crea e distrugge numerosi file durante il funzionamento. Se il server proxy registra gli accessi (mediante il log degli accessi, il log degli accessi del proxy o il log degli accessi alla cache), indirizzare i log a un file system dedicato in modo che, in caso di aumento improvviso, non utilizzino lo spazio destinato ad un'altra funzione, quale la cache.

Ottimizzazione della configurazione TCP/IP

Caching Proxy è sensibile alle modifiche alle configurazioni TCP/IP. La riduzione dei valori TCP/IP su un sistema operativo potrebbe causare un funzionamento imprevisto del server proxy. Nello specifico, se i valori TCP/IP impostati sono troppo bassi, le connessioni potrebbero venire riavviate dai client che si connettono al server proxy o dai server di origine a cui si connette il proxy. Ciò accade soprattutto per i client che si connettono al server proxy attraverso una connessione a banda ridotta (56700 bps o meno). Se è necessario ridurre i parametri TCP/IP, agire con cautela.

Ottimizzazione dei tempi di attesa TCP per i sistemi a carichi elevati (HP-UX, Linux, Solaris, Windows)

L'intervallo di attesa TCP specifica il tempo durante il quale un socket resta in attesa di un pacchetto FIN dal mittente prima della chiusura forzata. Negli ambienti a carico elevato, il server proxy potrebbe sembrare bloccato se un gran numero di socket rimane in sospeso, nello stato TIME_WAIT, dopo la chiusura delle connessioni. La riduzione dell'intervallo di attesa TCP riduce il numero di socket in sospeso e, negli ambienti a carico elevato, può prevenire il blocco del server proxy. Si consiglia di impostare questo intervallo a 5 secondi.

Per impostare l'intervallo di attesa TCP a 5 secondi:

- Su HP-UX:

  Digitare il seguente comando:

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

  Servirsi dell'utilità "sam" per impostare il parametro del kernel max_thread_proc a un valore di almeno 2048.

  Nota: Inoltre, considerare se è il caso di regolare i seguenti parametri del 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_recv_hiwater_def.

- Su Linux:

  Immettere i seguenti comandi:

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

- Su Solaris:

  Digitare il seguente comando:

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

  Modificare il file /etc/system perché appaia come segue:

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

- Su Windows:

  Per impostare un tempo di attesa TCP, è necessario creare una voce del registro di configurazione. Per ulteriori informazioni, fare riferimento alla documentazione di Windows.

Ottimizzazione del kernel Linux

Diverse limitazioni nel kernel Linux sono basse e possono essere modificate. Alcune possono essere modificate attraverso il file system /proc, altre richiedono la ricompilazione del kernel.

Nota: il file system /proc è virtuale; ciò significa che non esiste fisicamente sul disco. Serve piuttosto da interfaccia per il kernel Linux. Poiché non esiste, i valori immessi vengono persi al riavvio. Di conseguenza, le modifiche che si desidera apportare al file system /proc devono essere inserite nel file /etc/rc.d/rc.local su RedHat o nel file /etc/rc.config su SUSE. In questo modo, le modifiche vengono sempre attivate al riavvio.

Di seguito vengono forniti alcuni consigli:

- Il valore massimo per i descrittori di file è 4096 per impostazione predefinita. È possibile modificarlo aggiungendo quanto segue al file rc.local:

  ```
  echo 32768 > /proc/sys/fs/file-max
  ```

- Il valore massimo per gli inode è 16384 per impostazione predefinita. È possibile modificarlo aggiungendo quanto segue al file rc.local:

  ```
  echo 65536 > /proc/sys/fs/inode-max
  ```

- L'intervallo di porte TCP e UDP è, per impostazione predefinita, 1024 – 4999. È possibile modificarlo in 32768 – 61000 aggiungendo quanto segue al file rc.local:

  ```
  echo 32768 61000 > /proc/sys/net/ipv4/ip_local_port_range
  ```

- Per impostazione predefinita, il numero di attività consentite è 512. Se vengono eseguite troppe attività, questo influirà sul numero massimo di thread per un processo. È possibile aumentare questo limite a 2048 modificando il valore di NR_TASKS nel file *SorgentiProprioKernel*/include/linux/tasks.h.
- Inoltre, modificare il valore di MIN_TASKS_LEFT_FOR_ROOT a 24. Per rendere effettiva questa modifica, è necessario ricompilare il kernel.

Se si decide di ricompilare il kernel, abilitare solo le opzioni assolutamente necessarie. Se uno specifico daemon non è necessario, non eseguirlo.

Impostazione delle variabili di ottimizzazione thread su AIX

Sui sistemi AIX, è possibile migliorare le prestazioni di Caching Proxy utilizzando thread con ambito esteso all'intero sistema e consentendo l'uso di più heap da parte dei thread. Le prestazioni sono legate alla funzionalità multiprocessore del sistema operativo e alla pianificazione dei thread del sistema operativo sottostante. È possibile aumentare le prestazioni impostando le seguenti variabili di ottimizzazione dei thread su AIX nel modo qui riportato:

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

È possibile impostare queste variabili d'ambiente prima di avviare `/usr/sbin/ibmproxy`, oppure aggiungerle a `/etc/rc.ibmproxy` se si utilizza **startsrc -s ibmproxy** per avviare il server proxy. Dopo aver regolato queste variabili di ottimizzazione dei thread, l'aumento delle prestazioni sarà più evidente sui sistemi SMP. Tuttavia, in alcuni casi, un aumento potrà essere evidente anche sui sistemi a processore singolo.

Nota: Per ulteriori informazioni, consultare la documentazione del sistema operativo AIX per i dettagli sulle variabili di ottimizzazione dei thread.

Parte 3. Configurazione del funzionamento di Caching Proxy

Questa sezione illustra le modalità di risposta del componente Caching Proxy alle richieste client e fornisce procedure per la configurazione di tale funzionamento. Questi elementi della configurazione di server proxy vengono normalmente gestiti da un amministratore Web e non influiscono sugli altri processi sul computer host o sui computer nella rete.

Di seguito vengono forniti i titoli di ciascun capitolo di questa sezione:

Capitolo 10. Gestione dell'elaborazione delle richieste

Quando Caching Proxy riceve una richiesta client, esegue l'azione specificata nel campo metodo sull'oggetto specificato nel campo URL, se il metodo richiesto è stato abilitato. Il server proxy risolve l'URL in base a un insieme di regole di mappatura definite dall'amministratore. Tali regole di mappatura potrebbero fornire istruzioni a Caching Proxy perché agisca come server Web, recuperando l'oggetto dal file system locale, o come server proxy, recuperando l'oggetto da un server di origine.

Questo capitolo descrive l'attivazione dei metodi, la definizione di regole di mappatura e la configurazione di un server proxy surrogato.

Attivazione dei metodi HTTP/FTP

Le richieste client al server comprendono un campo metodo che indica l'azione che il server deve eseguire sull'oggetto specificato.

Di seguito viene fornito un elenco di metodi supportati dal server proxy e una descrizione delle modalità di risposta a una richiesta client contenente il metodo, se quest'ultimo è attivato.

Nota: Alcuni metodi sono identici per le richieste HTTP e FTP. L'attivazione di tali metodi per HTTP ne comporta l'attivazione automatica anche per FTP.

DELETE
Il server proxy elimina l'oggetto identificato dall'URL. DELETE consente ai client di cancellare file da Caching Proxy. Utilizzare le impostazioni di protezione del server per definire quali utenti possono eseguire il metodo DELETE e su quali file. Per maggiori dettagli, consultare Capitolo 25, "Impostazioni della protezione server", a pagina 111.

GET Il server proxy restituisce i dati identificati nell'URL. Se l'URL fa riferimento a un programma eseguibile, il proxy restituisce l'output del programma. Questo metodo può essere gestito su connessioni permanenti.

HEAD
Il server proxy restituisce solo l'intestazione del documento HTTP identificato dall'URL, senza il corpo del documento.

OPTIONS
Il server proxy restituisce informazioni relative alle opzioni di comunicazione sulla catena di richiesta-risposta identificata dall'URL. Questo metodo consente a un client di determinare le opzioni e i requisiti associati a un oggetto o le funzionalità di un server senza dover agire sull'oggetto o recuperarlo.

POST La richiesta contiene dati e un URL. Il server proxy accetta i dati racchiusi nella richiesta come nuova subordinata della risorsa identificata nell'URL, che elabora i dati. La risorsa può essere un programma che accetta dati, un gateway verso un altro protocollo o un programma che accetta annotazioni.

Il metodo POST è destinato alla gestione delle annotazioni di risorse esistenti. Gli esempi comprendono l'invio di un messaggio a una bacheca elettronica, a un gruppo di discussione, a una mailing list o analogo

gruppo di risorse; l'immissione di un blocco di dati, ad esempio da un modulo a un programma di gestione dati; oppure l'estensione di un database mediante un'operazione di **accodamento**. In Caching Proxy, il metodo POST viene utilizzato per elaborare i moduli di Gestione e configurazione.

Questo metodo può essere gestito su connessioni permanenti.

PUT La richiesta contiene dati e un URL. Il server proxy memorizza i dati nella risorsa identificata nell'URL. Se la risorsa esiste già, PUT la sostituisce con i dati contenuti nella richiesta. Se la risorsa non esiste, PUT la crea e la popola con i dati contenuti nella richiesta. Questo metodo può essere gestito su connessioni permanenti.

L'attivazione del metodo PUT consente la scrittura di file su Caching Proxy utilizzando HTTP e FTP. Poiché PUT consente ai clienti di scrivere su Caching Proxy, è necessario utilizzare impostazioni di protezione del server per definire gli utenti autorizzati all'uso del metodo PUT e i file su cui tale metodo può essere applicato. (Consultare Capitolo 25, "Impostazioni della protezione server", a pagina 111.)

TRACE

Il server proxy utilizza l'istruzione echo per il messaggio di richiesta inviato dal client. Questo metodo consente al client di vedere cosa viene ricevuto all'altra estremità della catena di richiesta e utilizzare tali dati per verifica o diagnosi. Il tipo di contenuto della risposta del proxy è message/http.

Direttive associate

Le direttive che seguono abilitano i metodi HTTP/FTP:

- "Enable — Indica di abilitare i metodi HTTP" a pagina 201
- "Disable — Indica di disabilitare i metodi HTTP" a pagina 200

Per ulteriori informazioni, fare riferimento a Capitolo 4, "Modifica manuale del file ibmproxy.conf", a pagina 13.

Moduli di Configurazione e amministrazione

I moduli di Gestione e configurazione che seguono modificano i valori delle direttive associate:

- **Configurazione server –> Elaborazione delle richieste –> Metodi HTTP –> GET**
- **Configurazione server –> Elaborazione delle richieste –> Metodi HTTP –> HEAD**
- **Configurazione server –> Elaborazione delle richieste –> Metodi HTTP –> POST**
- **Configurazione server –> Elaborazione delle richieste –> Metodi HTTP –> PUT**
- **Configurazione server –> Elaborazione delle richieste –> Metodi HTTP –> DELETE**
- **Configurazione server –> Elaborazione delle richieste –> Metodi HTTP –> OPTIONS**
- **Configurazione server –> Elaborazione delle richieste –> Metodi HTTP –> TRACE**

Nota: Se si disabilita il metodo POST, non sarà possibile utilizzare i moduli di Gestione e configurazione per configurare Caching Proxy.

Per ulteriori informazioni, fare riferimento a Capitolo 2, "Utilizzo dei moduli di Gestione e configurazione", a pagina 7.

Definizione delle regole di mappatura

Le regole di mappatura sono direttive di configurazione che fanno sì che le richieste client a Caching Proxy vengano elaborate in un certo modo, ad esempio inoltrate a un server di origine (meccanismo proxy), reindirizzate o respinte. L'impostazione corretta delle regole di mappatura è importante per il corretto funzionamento di Caching Proxy. Le regole di mappatura influiscono su quanto segue:

- Funzionamento base del proxy
- Accesso ai moduli di Gestione e configurazione basati su browser
- Possibilità di memorizzare nella cache i risultati di servlet e altro contenuto generato in modo dinamico

Le direttive per le regole di mappatura utilizzano la forma che segue:

regola maschera destinazione [*indirizzo_IP* | *nome_host*]:[*porta*]

Solo le richieste che corrispondono alla combinazione di maschera e IP/porta sono soggette alla regola. Una maschera può contenere caratteri jolly, ad esempio https://**/*.asp.

L'ordine con cui le direttive compaiono nel file di configurazione è significativo. Ad eccezione delle direttive Map, non appena viene rilevata una corrispondenza tra la richiesta e una maschera, la richiesta viene elaborata senza valutare le regole successive. La direttiva Map sostituisce l'URL nella richiesta. Questa nuova richiesta viene ancora confrontata con le restanti regole di mappatura.

Regole di mappatura

Le seguenti regole di mappatura si applicano alle richieste client che corrispondono alla maschera specificata:

- **Map** — riscrive la richiesta. La regola Map sostituisce l'URL di una richiesta (maschera) con un altra stringa URL (destinazione). Dopo questa sostituzione, la richiesta contenente la nuova stringa viene ancora confrontata con le rimanenti regole di mappatura.
- **Pass, Exec** — soddisfano la richiesta localmente. Le regole Pass ed Exec elaborano la richiesta sul server proxy. La regola Pass mappa l'URL di una richiesta (maschera) su un file fornito dal server proxy (destinazione); la regola Exec mappa l'URL di una richiesta su un programma CGI eseguito sul server proxy.
- **Fail** — respinge la richiesta. La regola Fail respinge una richiesta (maschera) sul server proxy. Qualsiasi richiesta che corrisponde alla maschera di una regola Fail non subisce ulteriore elaborazione. Le regole Fail non hanno argomenti di destinazione.
- **Redirect** — inoltra la richiesta. La regola Redirect inoltra una richiesta (maschera) a un altro server Web (destinazione). Poiché un URL completo, comprensivo del protocollo di destinazione, costituisce la destinazione di questa regola, è possibile cambiare protocollo durante il reindirizzamento, ad esempio per aggiungere la codifica SSL a una richiesta HTTP. Il reindirizzamento non verifica la cache prima di soddisfare la richiesta.
- **Proxy, ProxyWAS** — agisce come proxy per la richiesta. Le regole Proxy e ProxyWAS passano le richieste (maschere) a un altro server (destinazione). A differenza di una semplice regola Redirect, le regole Proxy consentono al server proxy di verificare la cache per soddisfare una richiesta, memorizzare nella cache il contenuto dai server di origine e scrivere intestazioni HTTP che abilitano funzioni avanzate. Utilizzare la regola ProxyWAS anziché Proxy quando il server di origine è un WebSphere Application Server.

La regola di mappatura seguente si applica alla risposta del server di origine:

- **ReversePass** — intercetta automaticamente le richieste reindirizzate. Una regola ReversePass individua una corrispondenza tra la risposta dal server di origine e la maschera quando la risposta passa attraverso il server proxy nel percorso verso il client. La direttiva ReversePass è progettata per rilevare un codice di stato di reindirizzamento che farebbe sì che un client contatti direttamente il server di origine. Al client viene fornita istruzione di contattare il server definito nell'argomento destinazione.

Le regole di mappatura che seguono sono valide per le applicazioni API:

- **nameTrans** — accetta la richiesta ed esegue un'applicazione API, definita dal percorso file sostituito durante la fase di traduzione dei nomi dell'elaborazione della richiesta.
- **service** — accetta la richiesta ed esegue un'applicazione API, definita dal percorso file sostituito durante la fase di servizio dell'elaborazione della richiesta.

Configurazione di un server surrogato

Per configurare un surrogato standard:

- Impostare la porta del server proxy su 80.

  ```
  Porta 80
  ```

- Aggiungere una regola Proxy, prima di tutte le altre, per agire da proxy per tutte le richieste ricevute sulla porta 80 al server di origine.

  ```
  Proxy /* http://server.di.contenuti.com/* :80
  ```

- Abilitare una porta di amministrazione diversa dalla 80.

  ```
  AdminPort 8080
  ```

Ciò consente l'invio tramite proxy di tutto il traffico HTTP sulla porta 80 al server di origine. Il traffico in entrata sulla porta di amministrazione non corrisponde alla regola proxy con caratteri jolly iniziale, per cui non viene inoltrato. Le restanti regole di mappatura vengono utilizzate per elaborare la richiesta.

Direttive associate

Le direttive che seguono definiscono le regole di mappatura:

- "Map — Indica di modificare le richieste corrispondenti con una nuova stringa richiesta" a pagina 225
- "Pass — Indica di specificare la maschera per accettare le richieste" a pagina 234
- "Exec — Indica di eseguire un programma CGI per eseguire la corrispondenza delle richieste" a pagina 205
- "Redirect — Indica di specificare una maschera per le richieste inviate a un altro server" a pagina 254
- "Proxy — Indica di specificare i protocolli proxy o il proxy inverso" a pagina 247
- "ProxyWAS — Indica di specificare di inviare le richieste a WebSphere Application Server" a pagina 252
- "ReversePass — Indica di intercettare automaticamente le richieste reindirizzate" a pagina 256

Per ulteriori informazioni, fare riferimento a Capitolo 4, "Modifica manuale del file ibmproxy.conf", a pagina 13.

Moduli di Configurazione e amministrazione

Il modulo di Gestione e configurazione che segue modifica i valori delle direttive associate:

- **Configurazione server –> Elaborazione delle richieste –> Inoltro delle richieste**

Nota: I moduli di Gestione e configurazione non supportano l'argomento numero di porta.

Per ulteriori informazioni, fare riferimento a Capitolo 2, "Utilizzo dei moduli di Gestione e configurazione", a pagina 7.

Abilitazione della riscrittura delle giunzioni (facoltativa)

La direttiva JunctionRewrite consente alla routine di riscrittura delle giunzioni in Caching Proxy di riscrivere le risposte dai server di origine per garantire che gli URL relativi al server vengano mappati sul server di origine adeguato quando si utilizzano le giunzioni. È necessario abilitare anche il plug-in di riscrittura delle giunzioni. Le giunzioni vengono definite dalle regole di mappatura del proxy.

Quando si utilizzano le regole di mappatura del proxy per definire la giunzione, la direttiva Proxy può essere utilizzata con o senza l'opzione JunctionPrefix.

Definizione della giunzione senza l'opzione JunctionPrefix

Di seguito vengono forniti esempi di giunzioni valide su cui è possibile agire mediante la routine di riscrittura delle giunzioni:

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

Di seguito viene fornito un esempio di una giunzione valida su cui *non* agisce la routine di riscrittura delle giunzioni:

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

Di seguito vengono forniti alcuni esempi di giunzioni non valide:

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

Queste regole di mappatura hanno creato giunzioni per shopserver, authserver e b2bserver. Considerare che shopserver restituisce un documento HTML con i seguenti URL contenuti nei tag HTML adeguati:

- /index.html (riferimento relativo al server)
- /images/shop.gif (riferimento relativo al server)
- buy/buy.jsp (riferimento relativo alla directory)
- http://ebay.com (riferimento assoluto)

La routine di riscrittura delle giunzioni sovrascrive i riferimenti relativi al server utilizzando le regole di mappatura del proxy nel modo seguente:

- /shop/index.html (modificato)
- /shop/images/shop.gif (modificato)
- buy/buy.jsp (invariato)
- http://ebay.com (invariato)

Definizione della giunzione con l'opzione JunctionPrefix (metodo consigliato)

Quando si utilizza l'opzione JunctionPrefix con la direttiva Proxy, anziché dedurre JunctionPrefix dal primo schema di URL nella regola Proxy, è possibile dichiarare il prefisso di giunzione nella regola Proxy utilizzando il formato seguente:

`Proxy` *`schema_url1 schema_url2`* `JunctionPrefix:`*`prefisso_url`*

Quando si utilizza JunctionPrefix, non vi è alcun limite al formato del primo schema URL. Per supportare la riscrittura delle giunzioni quando *non* si utilizza l'opzione JunctionPrefix, l'URL proxy deve avere il formato seguente: `Proxy`

`/market/* http://b2bserver/*`. Tuttavia, quando si utilizza JunctionPrefix, la regola Proxy seguente è valida per la riscrittura delle giunzioni:

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

La routine di riscrittura delle giunzioni influisce sui seguenti tag:

Tabella 3. Tag influenzati dalla routine di riscrittura delle giunzioni

Tag	**Attributi**
!—	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 routine di riscrittura delle giunzioni non influisce sui tag generati da JavaScript o da plug-in all'interno del browser.

Direttive associate

Le direttive che seguono vengono utilizzate per abilitare la routine e il plug-in di riscrittura delle giunzioni.

- "ServerInit — Indica di personalizzare la fase Inizializzazione del server" a pagina 261
- "Transmogrifier — Indica di personalizzare la fase Manipolazione dei dati" a pagina 270
- "JunctionRewrite — Indica di attivare la riscrittura dell'URL" a pagina 218

- "JunctionRewriteSetCookiePath — Indica di riscrivere l'opzione di percorso nell'intestazione Set-Cookie, quando si utilizza il plugin JunctionRewrite" a pagina 218
- "JunctionReplaceUrlPrefix — Indica di sostituire l'URL anziché inserire il prefisso, se si utilizza il plugin JunctionRewrite" a pagina 217
- "JunctionSkipUrlPrefix — Indica di ignorare la riscrittura degli URL che già contengono il prefisso, quando si utilizza il plugin JunctionRewrite" a pagina 219

Per ulteriori informazioni, fare riferimento a Capitolo 4, "Modifica manuale del file ibmproxy.conf", a pagina 13.

Moduli di Configurazione e amministrazione

Il modulo di Gestione e configurazione che segue può essere utilizzato per abilitare il plug-in di riscrittura delle giunzioni:

- **Configurazione server –> Elaborazione delle richieste –> Elaborazione delle richieste API**

Nota: I moduli di Gestione e configurazione non supportano la direttiva JunctionRewrite.

Per ulteriori informazioni, fare riferimento a Capitolo 2, "Utilizzo dei moduli di Gestione e configurazione", a pagina 7.

UseCookie come alternativa a JunctionRewrite

È possibile utilizzare i cookie per memorizzare le informazioni del server di back-end nel modo seguente: viene inviato un cookie al browser del client. Quando il browser invia richieste per risorse nella pagina HTML, allega un cookie per cui Caching Proxy inoltra le richieste al server di back-end corretto.

Per utilizzare i cookie come alternativa a JunctionRewrite, apportare le seguenti modifiche al file ibmproxy.conf:

1. Sostituire **JunctionRewrite on** con **JunctionRewrite on UseCookie**.
2. Commentare il plug-in JunctionRewrite.

Di seguito viene fornito un confronto del plug-in JunctionRewrite e dell'implementazione con cookie.

- Plug-in JunctionRewrite
  - La pagina HTML viene riscritta.
  - Non supporta la riscrittura di linguaggi di script e applet, a meno che non venga utilizzato il plug-in Transmogrifier. Vedere "Plugin Transmogrifier di esempio per estendere la funzionalità JunctionRewrite" a pagina 47.
  - Prestazioni ridotte.
  - Nessuna limitazione alle configurazioni del server di back-end. Il client può avere accesso incrociato ai server di back-end in una sessione.
- Implementazione con cookie
  - La pagina HTML *non* viene riscritta. Viene inviato un cookie al client.
  - Il browser del client deve avere il supporto dei cookie abilitato.
  - Migliori prestazioni.
  - Alcune limitazioni alle configurazioni del server di back-end. Utilizzabile solo quando un client accede al server di back-end in una sessione.

Nota: È presente una limitazione nota, legata all'uso di JunctionRewrite con l'opzione UseCookie. Gli URL per tutte le richieste verranno tradotti, in modo errato, anche se il cookie si applica solo a una sottodirectory dell'host. Di seguito vengono forniti due modi per gestire correttamente gli URL in ROOT, che non richiedono la giunzione:

- Collocare le regole del proxy prima della direttiva JunctionRewrite nel file ibmproxy.conf. (Tutte le regole del proxy collocate prima della direttiva JunctionRewrite non saranno riscritte.)
- Mappare esplicitamente ogni URL, anziché utilizzare un carattere jolly (*). Ad esempio:

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

Plugin Transmogrifier di esempio per estendere la funzionalità JunctionRewrite

Viene fornito del codice di esempio personalizzabile che riscrive e analizza i blocchi di tag JavaScript (SCRIPT) e applet (APPLET) nei file HTML. Da solo, il plugin JunctionRewrite non può elaborare i collegamenti a risorse in JavaScript o nei valori dei parametri di Java™.

Dopo aver installato Caching Proxy, è possibile compilare lo stesso codice e configurarlo per l'esecuzione con JunctionRewrite.

I seguenti file di esempio si trovano nella sottodirectory ...samples/cp/, all'interno della directory in cui è stato scaricato il fix pack.

- Makefile (Makefile per questo plug-in di esempio)
- junctionRewrite2.h (interfaccia per il gestore del programma di analisi personalizzato)
- junctionRewrite2.c (implementazione per l'interfaccia precedente)
- scriptHandler.c (gestore riscrittura JavaScript di esempio)
- appletHandler.c (gestore blocchi Applet di esempio)
- junctionRewrite2.def (file def del plug-in per Windows)
- junctionRewrite2.exp (file di esportazione del plug-in per Linux e UNIX)

Capitolo 11. Gestione della consegna di contenuti locali

Le regole di mappatura Pass e Exec vengono utilizzate per fornire contenuti locali a un client che ne fa richiesta. Per impostazione predefinita, una regola Pass con una maschera jolly viene collocata come ultima regola di mappatura. Questa regola indirizza tutte le richieste che non soddisfano le maschere precedenti perché recuperino i file da una directory di destinazione, detta generalmente directory root dei documenti.

Quando viene ricevuto un URL che non contiene un nome file, Caching Proxy soddisfa la richiesta ricercando nella directory specificata, se presente, o nella directory root dei documenti, se non viene specificata una directory, un file corrispondente all'elenco di pagine di benvenuto specificato nel file di configurazione. Se viene definita più di una pagina iniziale, il server proxy ricerca le pagine nell'ordine con cui sono definite. La prima pagina di benvenuto individuata viene fornita al client.

La pagina iniziale del server è la pagina Web che il server fornisce per impostazione predefinita quando riceve una richiesta contenente solo l'URL del server, senza una directory o un nome file. Come spiegato in precedenza, la regola di mappatura jolly predefinita richiede la memorizzazione della pagina iniziale del server nella directory root dei documenti e la corrispondenza del nome file della pagina iniziale con una pagina di benvenuto definita.

Nota: In alcuni browser Web, il termine *pagina iniziale* viene utilizzato per indicare la prima pagina caricata dal browser al suo avvio. In questo documento, il termine viene utilizzato solo per la pagina iniziale del server.

Questo capitolo descrive come definire la directory root dei documenti e le pagine di benvenuto.

Definizione della directory root dei documenti

Le directory root dei documenti predefinite sono:

- Su Linux e UNIX: /opt/ibm/edge/cp/server_root/pub/*lang*/
- Su Windows: *unità*:\Programmi\IBM\edge\cp\root_server\pub*lang*\, oppure la directory specificata come directory HTML durante l'installazione

Direttive associate

Le direttive che seguono definiscono la directory root dei documenti:

- "Pass — Indica di specificare la maschera per accettare le richieste" a pagina 234

Per ulteriori informazioni, fare riferimento a Capitolo 4, "Modifica manuale del file ibmproxy.conf", a pagina 13.

Moduli di Gestione e configurazione

Per modificare la directory root dei documenti nei moduli di Gestione e configurazione, utilizzare la procedura seguente:

1. Selezionare **Configurazione server –> Elaborazione richieste –> Inoltro richieste**.

2. Nella tabella di inoltro delle richieste, individuare la riga contenente la stringa /* (slash asterisco) nella colonna **Maschera di Richiesta**. Questa rappresenta la directory root dei documenti. Nella casella **Indice** sotto la tabella, fare clic sul numero corrispondente al numero nella colonna **Indice** per tale riga.
3. Fare clic su **Sostituisci**.
4. Nell'elenco a discesa **Azione**, fare clic su **Pass**.
5. Immettere /* nel campo Maschera di richiesta URL.
6. Immettere la nuova directory root dei documenti nel campo **Percorso file di sostituzione**.
7. Fare clic su **Inoltra**.
8. Dopo che le modifiche sono state accettate, fare clic sull'icona **Riavvia server** (!) nel frame superiore.

Dopo il riavvio, il server comincia a utilizzare la nuova directory root dei documenti.

Per ulteriori informazioni, fare riferimento a Capitolo 2, "Utilizzo dei moduli di Gestione e configurazione", a pagina 7.

Definizione delle pagine di benvenuto predefinite

Il server ricerca la pagina iniziale nella directory root dei documenti, ma il file specifico restituito viene definito dall'elenco delle pagine di benvenuto.

Informazioni sulle pagine di benvenuto

Quando il server riceve una richiesta URL che non specifica un nome file, tenta di soddisfarla in base a un elenco di pagine di benvenuto impostato nel file di configurazione del server. Tale elenco definisce i file da utilizzare come pagine iniziali predefinite. Il server determina la pagina iniziale mediante una corrispondenza tra l'elenco di pagine di benvenuto e i file nella directory root dei documenti. La prima corrispondenza individuata è il file restituito come pagina iniziale. Se non viene individuata alcuna corrispondenza, il server visualizza un elenco dei contenuti della directory root dei documenti.

Per utilizzare un determinato file come pagina iniziale del server e restituirlo quando una richiesta non specifica né una directory, né un nome file, è necessario collocarlo nella directory root dei documenti e accertarsi che il suo nome corrisponda a uno dei nomi file presenti nell'elenco delle pagine di benvenuto.

Il file di configurazione predefinito definisce questi nomi file, in quest'ordine, per l'uso come pagine di benvenuto:

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

Il server restituisce il primo file che individua come corrispondente a un nome file nell'elenco. Fino a che non viene creato un file welcome.html o index.html, collocandolo nella directory root dei documenti, il server utilizza Frntpage.html come pagina iniziale.

Ad esempio, se si utilizza la configurazione predefinita e la directory root dei documenti non contiene un file denominato welcome.html, ma contiene file denominati index.html e FrntPage.html, il file index.html viene utilizzato come pagina iniziale.

Se non viene individuata una pagina iniziale, viene visualizzata la struttura della directory root dei documenti.

Direttive associate

Le direttive che seguono definiscono le pagine di benvenuto:

- "Welcome — Indica di specificare i nomi dei file di benvenuto" a pagina 274

Per ulteriori informazioni, fare riferimento a Capitolo 4, "Modifica manuale del file ibmproxy.conf", a pagina 13.

Moduli di Gestione e configurazione

Il modulo di Gestione e configurazione che segue definisce le pagine di benvenuto:

- **Configurazione server –> Directory e pagina di benvenuto –> Pagina di benvenuto**

Per ulteriori informazioni, fare riferimento a Capitolo 2, "Utilizzo dei moduli di Gestione e configurazione", a pagina 7.

Capitolo 12. Gestione delle connessioni FTP

Caching Proxy funge da proxy per le richieste di URL FTP e le inoltra al server FTP adeguato, ma non può essere utilizzato per inoltrare via proxy le richieste da un client FTP. Può supportare solo le richieste FTP ricevute da un client HTTP (utilizzando lo schema di protocollo ftp://).

Solo i metodi GET, PUT e DELETE sono supportati per le richieste di file FTP. Solo il metodo GET è supportato per le richieste di elenchi di directory FTP. Per impostazione predefinita, PUT e DELETE sono disabilitati in Caching Proxy. Per ulteriori informazioni, fare riferimento a "Attivazione dei metodi HTTP/FTP" a pagina 39.

Questo capitolo descrive la protezione dei file FTP e la gestione di accessi al server FTP, percorsi directory e concatenazione.

Protezione dei file FTP

Se è stato abilitato il metodo PUT per il caricamento dei file FTP o il metodo DELETE per la loro eliminazione, è necessario definire la protezione proxy FTP almeno per le richieste PUT e DELETE, per impedire l'aggiornamento non autorizzato dei file sul server FTP.

Per proteggere l'inoltro tramite proxy delle richieste FTP, nei moduli di Gestione e configurazione, selezionare **Configurazione server –> Protezione documenti**. Per creare un'impostazione di protezione per le richieste di file FTP, includere `ftp://` all'inizio della maschera di richiesta. Ad esempio, per proteggere i file in una directory denominata esami, utilizzare la maschera `ftp://esami/*`.

Per ulteriori informazioni sulla creazione di impostazioni di protezione, vedere Capitolo 25, "Impostazioni della protezione server", a pagina 111.

Gestione del login su server FTP

Se non vengono specificati un ID utente e una password nell'URL della richiesta, Caching Proxy tenta di accedere al server FTP richiesto in modo anonimo, utilizzando l'ID utente ANONYMOUS. Molti server FTP richiedono un indirizzo e-mail come password per FTP anonimo. Se il server FTP richiede una password per il login anonimo, Caching Proxy invia l'indirizzo e-mail specificato dalla direttiva WebmasterEmail nel file di configurazione.

Per impostare l'indirizzo e-mail del Webmaster nei moduli di Gestione e configurazione, selezionare **Configurazione server –> Gestione sistema –> SNMP MIB**. L'indirizzo e-mail può essere impostato anche utilizzando la direttiva WebmasterEmail; per i dettagli, vedere la sezione di riferimento: "WebMasterEMail — Indica di impostare un indirizzo e-mail per ricevere report di server selezionati" a pagina 273.

Se il server FTP nell'URL della richiesta prevede una combinazione specifica di ID utente e password per consentire l'accesso, gli utenti possono immettere l'ID e la password nell'URL della richiesta, ad esempio:

`ftp://`*`ID_utente`*`:`*`password`*`@`*`ftpserverhost`*`/`

Se non si desidera specificare la password per l'ID utente FTP nell'URL della richiesta, gli utenti possono immettere solo l'ID utente nell'URL: `ftp://ID_utente@ftpserverhost`. Caching Proxy tenta dapprima di accedere al server FTP con l'ID utente specificato, senza password. Se il login ha esito negativo senza una password, il browser richiede la password associata all'ID utente specificato.

Per i login non anonimi, è necessario specificare almeno l'ID utente nell'URL. Se l'ID utente non viene specificato, viene tentato il login anonimo e al client non viene richiesto l'ID utente.

Gestione dei percorsi directory FTP

È necessario specificare in Caching Proxy se si desidera interpretare i nomi percorso negli URL FTP come relativi alla directory di lavoro dell'utente o alla directory root. Ad esempio, se un utente che accede a un server FTP ha una directory di lavoro predefinita denominata /export/home/user1 e desidera recuperare un file denominato test1.exe da una sottodirectory denominata test, il proxy utilizza gli URL seguenti per recuperare il file dal server FTP, a seconda di come vengono interpretati gli URL FTP:

- Se vengono impostati nomi percorso *assoluti*:
  `ftp://user1:user1pw@FTPhost/export/home/user1/test/test1.exe`
- Se vengono impostati nomi percorso *relativi*:
  `ftp://user1:user1pw@FTPhost/test/test1.exe`

Se vengono impostati percorsi URL FTP relativi, gli utenti possono ancora specificare un nome percorso assoluto utilizzando la convenzione di accodare al carattere slash iniziale (/) la notazione `%2F`, che indica la directory root. Ad esempio, se user1, la cui directory di lavoro è /export/home/user1, desidera accedere a un file nella directory di lavoro di user2, /export/home/user2, la richiesta `ftp://user1:user1pw@FTPhost/%2Fexport/home/user2/file` viene interpretata correttamente come un URL relativo alla directory root /, ossia, un nome percorso assoluto, anche se sono stati scelti i nomi percorso URL FTP relativi.

Per specificare in che modo debbano essere interpretati gli URL FTP, nei moduli di Gestione e configurazione, selezionare **Configurazione proxy –> Prestazioni proxy**. Nella parte inferiore del modulo, in **I percorsi URL FTP URL devono essere:**, selezionare **percorsi assoluti** per specificare la directory root del server, oppure **percorsi relativi** per specificare la directory di lavoro dell'utente come inizio del percorso.

Questa impostazione può essere modificata anche nel file di configurazione del proxy; per ulteriori informazioni, vedere "FTPUrlPath — Indica di specificare la modalità di interpretazione di URL FTP" a pagina 210.

Gestione dei concatenamenti FTP

Se si concatenano più server Web proxy tra loro, è possibile specificare che le richieste contenenti URL FTP vengano inviate a un server Web proxy concatenato, anziché direttamente al server FTP. Per specificare un server proxy concatenato per le richieste FTP, nei moduli di Gestione e configurazione, selezionare **Configurazione proxy –> Concatenamento proxy e domini non proxy**. Lo schema di protocollo http:// viene utilizzato per specificare l'URL del proxy concatenato, anche quando la concatenazione richiede uno schema di protocollo ftp://.

Per configurare la concatenazione FTP utilizzando il file di configurazione del proxy, vedere la sezione di riferimento dedicata a “ftp_proxy — Indica di specificare un altro server proxy per le richieste FTP” a pagina 209.

Capitolo 13. Personalizzazione dell'elaborazione server

Questo capitolo descrive l'utilizzo dell'inclusione di informazioni lato server per inserire informazioni nei programmi CGI e nei documenti HTML forniti a un client. Vengono inoltre illustrate la personalizzazione dei messaggi di errore del server e la mappatura delle risorse.

Inclusione di informazioni lato server

L'inclusione di informazioni lato server consente di aggiungere informazioni ai programmi CGI e ai documenti HTML inviati dal server al client quando agisce come server di origine, ossia non per oggetti inviati tramite proxy o memorizzati nella cache. La data corrente, le dimensioni di un file, la data di ultima modifica sono esempi del tipo di informazioni che possono essere trasmesse al client. Questa sezione descrive il formato dei comandi per l'inclusione di informazioni lato server e illustra il funzionamento dei comandi di inclusione di informazioni lato server nei programmi CGI e nei documenti HTML. È inoltre possibile utilizzare l'inclusione di informazioni lato server per personalizzare le pagine di errore.

Considerazioni per l'inclusione di informazioni lato server

Prima di utilizzare l'inclusione di informazioni lato server sul server, prendere in considerazione le problematiche legate alle prestazioni, alla sicurezza e ai rischi:

- Le prestazioni possono subire un impatto significativamente negativo quando il server elabora i file mentre li invia.
- La sicurezza può essere compromessa se si permette a utenti ordinari di eseguire comandi sul server. Prestare attenzione durante la decisione in merito alle directory in cui inserire l'inclusione di informazioni lato server e quelle in cui inserire il comando **exec**. È possibile ridurre al minimo il rischio per la sicurezza se non si abilita il comando **exec**.
- L'uso dell'inclusione di informazioni lato server può causare alcuni problemi. Ad esempio, non è possibile fare riferimento ai file in modo ricorsivo: se si esegue il file sleepy.html e il programma individua `<-- !#include file="sleepy.html" -->` , il server non rileva l'errore e può bloccarsi. (Il riferimento non ricorsivo a file all'interno di altri file non costituisce un problema.)

Configurazione per l'inclusione di informazioni lato server

Per abilitare l'inclusione di informazioni lato server, nei moduli di Gestione e configurazione, selezionare **Configurazione server –> Impostazioni di base**. Utilizzare questo modulo per specificare quali tra i seguenti tipi di inclusione di informazioni lato server sono accettabili:

- Script CGI
- File
- Tutti tranne gli script CGI che utilizzano il comando **exec**
- Nessuna

Utilizzare questo modulo anche per specificare se eseguire l'elaborazione dell'inclusione lato server per i documenti di testo o HTML oltre agli altri tipi di file.

Inoltre, accertarsi che l'estensione file utilizzata per l'inclusione sia riconosciuta. Nei moduli di Gestione e configurazione, selezionare **Configurazione server –> Tipi MIME e codifica**, e utilizzare il modulo **Tipi MIME**. Notare che le estensioni shtml e htmls sono riconosciute per impostazione predefinita.

Per configurare il server per l'inclusione di informazioni lato server mediante la modifica delle direttive nel file di configurazione del proxy, vedere le sezioni di riferimento dedicate alle seguenti direttive:

- "AddType — Indica di specificare il tipo dati di file con particolari suffissi" a pagina 173
- "imbeds — Indica di specificare se viene utilizzata l'elaborazione di inclusione lato server" a pagina 215

Formato per l'inclusione di informazioni lato server

I comandi di inclusione devono essere inseriti nel documento HTML o nel programma CGI come commenti. I comandi hanno il formato seguente:

```
t<!--#tag direttiva=valore ... -->
o
<!--#tag direttiva="valore" ... -->
```

Le virgolette intorno ai valori sono facoltative, ma necessarie per incorporare spazi.

Direttive per l'inclusione di informazioni lato server

Questa sezione illustra le direttive accettate dal server per l'inclusione di informazioni lato server. (Da non confondersi con le direttive per il file di configurazione del proxy, documentate in Appendice B, "Direttive del file di configurazione", a pagina 165.)

config—controlla l'elaborazione dei file

Utilizzare questa direttiva per controllare determinati aspetti dell'elaborazione dei file. I tag validi sono `cmntmsg`, `errmsg`, `sizefmt` e `timefmt`.

cmntmsg

Utilizzare questo tag per specificare un messaggio che precede l'inizio dei commenti aggiunti da altre direttive. Per qualsiasi direttiva contenente testo tra la specifica di una direttiva e `"-->"`, tale testo viene trattato come un commento e aggiunto al file inviato dal server al client.

Esempio:

```
<!--#config cmntmsg="[Questo è un commento]" -->
<!-- #echo var="  " testo extra -->
```

Risultato: `<!--[Questo è un commento] testo extra -->`

Predefinito: `[quanto  segue era estraneo alla direttiva]`

errmsg

Utilizzare questo tag per specificare il messaggio che viene inviato al client se si verifica un errore durante l'elaborazione di un file. Il messaggio viene registrato nel log degli errori del server.

Esempio:

```
<!-- #config errmsg="[Si è verificato un errore]" -->
```

Predefinito: `"[Si è verificato un errore durante l'elaborazione di questa direttiva]"`

sizefmt

Utilizzare questo tag per specificare il formato di visualizzazione delle dimensioni dei file. Negli esempi seguenti, `bytes` è il valore utilizzato per visualizzare il numero di byte, mentre `abbrev` è il valore utilizzato per visualizzare il numero di kilobyte o megabyte.

Esempio 1:

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

Risultato: `1024`

Esempio 2:

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

Risultato: `1K`

Predefinito: `"abbrev"`

timefmt

Utilizzare questo tag per specificare il formato utilizzato per fornire la data.

Esempio:

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

Risultato: `"10/18/95 12:05:33"`

Predefinito: `"%a, %d %b %Y %T %Z"`

I seguenti formati `strftime()` sono validi con il tag `timefmt`:

Identificatore	Significato
%%	Sostituisci con %
%a	Sostituisci con il giorno della settimana abbreviato
%A	Sostituisci con il giorno della settimana in forma estesa
%b	Sostituisci con il nome del mese abbreviato
%B	Sostituisci con il nome del mese in forma estesa
%c	Sostituisci con la data e l'ora
%C	Sostituisci con il numero di secolo (anno diviso 100 e troncato)
%d	Sostituisci con il giorno del mese (01-31)
%D	Inserisci la data come *%m/%g/%a*
%e	Inserisci il mese dell'anno come numero decimale (01-12) (Solo in C POSIX, si tratta di un campo a due caratteri, con allineamento a destra e riempimento vuoto)
%E[cCxyY]	Se il formato di data/ora alternativo non è disponibile, i descrittori %E vengono mappati sulle loro controparti abbreviate (ad esempio, %EC viene mappato su %C)
%Ec	Sostituisci con la rappresentazione alternativa di data e ora

Identificatore	Significato
%EC	Sostituisci con il nome dell'anno base (periodo) nella rappresentazione alternativa
%Ex	Sostituisci con la rappresentazione alternativa della data
%EX	Sostituisci con la rappresentazione alternativa dell'ora
%Ey	Sostituisci con l'offset da %EC (solo anno) nella rappresentazione alternativa
%EY	Sostituisci con la rappresentazione alternativa dell'anno completa
%h	Sostituisci con il nome del mese abbreviato (lo stesso che %b)
%H	Sostituisci con l'ora (formato 0-24) come numero decimale (00-23)
%I	Sostituisci con l'ora (formato 0-12) come numero decimale (00-12)
%j	Sostituisci con il giorno dell'anno (001-366)
%m	Sostituisci con il mese (01-12)
%M	Sostituisci con il minuto (00-59)
%n	Sostituisci con una nuova riga
%O[deHlmMSUwWy]	Se il formato di data/ora alternativo non è disponibile, i descrittori %E vengono mappati sulle loro controparti abbreviate (ad esempio, %Od viene mappato su %d)
%Od	Sostituisci con il giorno del mese, utilizzando i simboli numerici alternativi, con il numero di zeri di riempimento iniziali adeguato se è previsto un simbolo alternativo allo zero, altrimenti con spazi
%Oe	Sostituisci con il giorno del mese, utilizzando i simboli numerici alternativi, con spazi di riempimento iniziali
%OH	Sostituisci con l'ora (formato 0-24), utilizzando i simboli numerici alternativi
%OI	Sostituisci con l'ora (formato 0-12), utilizzando i simboli numerici alternativi
%Om	Sostituisci con il mese, utilizzando i simboli numerici alternativi
%OM	Sostituisci con i minuti, utilizzando i simboli numerici alternativi
%OS	Sostituisci con i secondi, utilizzando i simboli numerici alternativi
%OU	Sostituisci con il numero di settimana dell'anno (Domenica come primo giorno della settimana, regole corrispondenti a %U), utilizzando i simboli numerici alternativi
%Ow	Sostituisci con il giorno della settimana (Domenica=0), utilizzando i simboli numerici alternativi
%OW	Sostituisci con il numero di settimana dell'anno (Lunedì come primo giorno della settimana), utilizzando i simboli numerici alternativi
%Oy	Sostituisci con l'anno (offset da %C) nella rappresentazione alternativa e utilizzando i simboli numerici alternativi
%p	Sostituisci con l'equivalente locale di AM o PM

Identificatore	Significato
%r	Sostituisci con la stringa equivalente a %I:%M:%S %p
%R	Sostituisci con la notazione oraria 0-24 (%H:%M)
%S	Sostituisci con i secondi (00-61)
%t	Sostituisci con un carattere di tabulazione
%T	Sostituisci con una stringa equivalente a %H:%M:%S
%u	Sostituisci con il giorno della settimana come numero decimale (1-7), con 1 che rappresenta Lunedì
%U	Sostituisci con il numero di settimana dell'anno (00-53), dove Domenica è il primo giorno della settimana
%V	Sostituisci con il numero di settimana dell'anno (01-53), dove Lunedì è il primo giorno della settimana
%w	Sostituisci con il giorno della settimana (0-6), dove Domenica è 0
%W	Sostituisci con il numero di settimana dell'anno (00-53), dove Lunedì è il primo giorno della settimana
%x	Sostituisci con la rappresentazione adeguata della data
%X	Sostituisci con la rappresentazione adeguata dell'ora
%y	Sostituisci con il numero di due cifre dell'anno all'interno del secolo
%Y	Sostituisci con il numero dell'anno completo di 4 cifre
%Z	Sostituisci con il nome del fuso orario o con nessun carattere se il fuso orario non è noto

La configurazione del sistema operativo determina i nomi completi e abbreviati dei mesi e gli anni.

echo—visualizza i valori delle variabili

Utilizzare questa direttiva per visualizzare il valore delle variabili d'ambiente specificate con il tag `var`. Se non viene rilevata una variabile, viene visualizzato (`Nessuna`). Inoltre, **echo** può visualizzare un valore impostato dalle direttive **set** o **global**. Le seguenti variabili di ambiente possono essere visualizzate:

DATE_GMT
La data e l'ora corrente secondo il fuso orario di Greenwich (GMT, Greenwich Mean Time). La formattazione di questa variabile viene definita utilizzando la direttiva **config timefmt**.

DATE_LOCAL
La data e l'ora corrente secondo il fuso orario locale. La formattazione di questa variabile viene definita utilizzando la direttiva **config timefmt**.

DOCUMENT_NAME
Il nome del primo dei documenti. Se l'HTML è stato generato da un programma CGI, questa variabile contiene il nome del programma CGI.

DOCUMENT_URI
L'URL completo richiesto dal client, senza la stringa di interrogazione.

LAST_MODIFIED
La data e l'ora dell'ultima modifica apportata al documento corrente. La formattazione di questa variabile viene definita utilizzando la direttiva **config timefmt**.

QUERY_STRING_UNESCAPED
L'interrogazione di ricerca inviata dal client. Non è definita a meno che l'HTML non sia stato generato da un programma CGI.

SSI_DIR
Il percorso del file corrente, relativo a SSI_ROOT. Se il file corrente si trova in SSI_ROOT, questo valore è "/".

SSI_FILE
Il nome del file corrente.

SSI_INCLUDE
Il valore utilizzato nel comando di inclusione che ha recuperato il file corrente. Non definito per il primo file.

SSI_PARENT
Il percorso e il nome del file contenente il comando di inclusione che ha recuperato il file corrente, relativo a SSI_ROOT.

SSI_ROOT
Il percorso del primo file. Tutte le richieste di inclusione devono trovarsi in questa directory o in una delle sue sottodirectory.

Esempio:

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

exec—specifica programmi CGI

Utilizzare questa direttiva per includere l'output di un programma CGI. La direttiva exec scarta eventuali intestazioni HTTP prodotte dal programma CGI *tranne* le seguenti:

Content-type
Determina se analizzare il corpo dell'output per altre inclusioni

Content-encoding
Determina se è necessaria la traduzione da EBCDIC ad ASCII

Last-modified
Sostituisce il valore corrente dell'intestazione last-modified a meno che questo non sia successivo al valore specificato

cgi—specifica l'URL del programma CGI

Utilizzare questa direttiva per specificare l'URL di un programma CGI.

In questo esempio, **program** è il programma CGI da eseguire, **path_info** e **query_string** rappresentano uno o più parametri passati al programma come variabili d'ambiente:

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

Questo esempio illustra l'uso delle variabili:

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

flastmod—visualizza la data e l'ora di ultima modifica del documento

Utilizzare questa direttiva per visualizzare la data e l'ora dell'ultima modifica apportata al documento. La formattazione di questa variabile viene definita dalla

direttiva **config timefmt**. I tag **file** e **virtual** sono validi con questa direttiva e i relativi significati sono definiti nel modo seguente.

Formati direttive:

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

file Utilizzare questo tag per specificare il nome di un file. Per **flastmod**, **fsize** e **include**, **file** è assunto come relativo a **SSI_ROOT** se preceduto da **'/'**. Altrimenti, è relativo a **SSI_DIR**. Il file specificato deve esistere in **SSI_ROOT** o in una delle sue sottodirectory. Ad esempio:

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

virtual

Utilizzare questo tag per specificare l'URL di un percorso virtuale a un documento. Per **flastmod**, **fsize** e **include**, **virtual** viene sempre passato attraverso le direttive di mappatura del server. Ad esempio:

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

Esempio:

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

Risultato: `12Maggio96`

fsize—visualizza le dimensioni del file

Utilizzare questa direttiva per visualizzare le dimensioni del file specificato. La formattazione di questa variabile viene definita dalla direttiva **config sizefmt**. I tag **file** e **virtual** sono validi per questa direttiva, e i relativi significati sono identici a quelli definiti in precedenza per la direttiva **flastmod**.

Esempio:

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

Risultato: `1K`

global—definisce variabili globali

Utilizzare questa direttiva per definire variabili globali che possono essere successivamente sottoposte all'operazione echo da parte di questo file o di eventuali file inclusi.

Esempio:

```
U<!--#global var=NomeVariabile value="UnValore" -->
```

Ad esempio, per fare riferimento a un documento parent oltre il limite virtuale, è necessario impostare una variabile globale DOCUMENT_URI. Inoltre, è necessario fare riferimento alla variabile globale nel documento child. Questo esempio illustra il codice HTML da inserire nel documento parent:

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

Questo esempio illustra il codice HTML da inserire nel documento child:

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

include—include un documento nell'output

Utilizzare questa direttiva per includere il testo di un documento nell'output. I tag **file** e **virtual** sono validi con questa direttiva e i relativi significati sono identici a quelli definiti in precedenza per la direttiva **flastmod**.

set—imposta le variabili da sottoporre a echo

Utilizzare questa direttiva per impostare una variabile che può essere sottoposta a echo in un secondo momento, ma solo da parte di questo file.

Esempio:

```
<!--#set var="Variabile 2" value="AltroValore" -->
```

Durante la definizione di una direttiva, è possibile sottoporre a echo una stringa nel mezzo di `value`. Ad esempio:

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

Variabili: una direttiva di impostazione lato server è generalmente seguita da una direttiva echo, in modo che ricerchi la variabile impostata, indichi dove si trova e proceda con la funzione. Può contenere riferimenti multipli a variabili. Le impostazioni lato server consentono inoltre di sottoporre a echo una variabile già impostata. Se non viene rilevata una variabile impostata, non viene visualizzato nulla.

Quando una impostazione lato server incontra un riferimento variabile all'interno di una direttiva di inclusione di informazioni lato server, tenta di risolverlo sul lato *server*. Nella seconda riga dell'esempio seguente, la variabile lato server `&index;` viene utilizzata con la stringa `var` per costruire il nome di variabile `var1`. Alla variabile `&var1;` viene quindi assegnato un valore inserendo un carattere escape prima di & in `&ecirc;` in modo che non venga riconosciuto come una variabile. Viene invece utilizzato come una stringa per creare il valore `fr&ecirc;d`, o *fred* con accento circonflesso sulla e. La variabile `&ecirc;` è una variabile lato client.

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

I caratteri che possono essere preceduti da escape (detti variabili escape) sono preceduti da un carattere backslash (\) e comprendono quanto segue:

Carattere	Significato
\a	Avviso (campanello)
\b	Backspace
\f	Alimentazione modulo (nuova pagina)
\n	Nuova riga
\r	Ritorno a capo
\t	Tabulazione orizzontale
\v	Tabulazione verticale
\'	Virgoletta singola
\"	Virgoletta doppia
\?	Punto interrogativo
\\	Backslash
\-	Trattino

Carattere	Significato
\.	Punto
\&	Asterisco

Personalizzazione dei messaggi di errore

È possibile personalizzare i messaggi di errore restituiti da Caching Proxy e definire messaggi specifici per particolari condizioni di errore. Nei moduli di Gestione e configurazione, selezionare **Configurazione server –> Personalizzazione dei messaggi di errore**. Utilizzare questo modulo per selezionare una condizione di errore e specificare un particolare file HTML da utilizzare per tale condizione.

Per personalizzare i messaggi di errore modificando le direttive nel file di configurazione del proxy, vedere la sezione di riferimento dedicata alla direttiva "ErrorPage — Indica di specificare un messaggio personalizzato per una determinata condizione di errore" a pagina 203.

Reindirizzamento del protocollo RTSP (Real Time Streaming Protocol)

WebSphere Application Server, Versione 6.0.2 introduce il supporto streaming media sotto forma di Redirector RTSP. RTSP consente a Caching Proxy di agire come il primo punto di contatto con i media player e di reindirizzare le loro richieste a un adeguato server proxy o a un server di contenuti che fornisce il contenuto multimediale richiesto.

RTSP, il protocollo Real Time Streaming, è definito nella RFC 2326. Si tratta di un protocollo Internet standard per il controllo dei flussi di dati. Sebbene non includa tecnologie per la *consegna* dei flussi, è abbastanza flessibile da poter essere utilizzato per controllare i flussi di dati che non hanno a che fare con la riproduzione video o audio.

Informazioni sul reindirizzamento RTSP

La funzione di reindirizzamento RTSP consente a Caching Proxy di reindirizzare le richieste per qualsiasi sessione di streaming multimediale controllata da RTSP. Sono inclusi i seguenti tipi di elementi multimediali:

- Audio registrato RealNetworks
- Video registrato RealNetworks
- Stream live RealNetworks (audio e video)
- File di Microsoft Media Player
- File di Apple Quicktime

Qualsiasi lettore configurabile per contattare un server proxy sulla sua porta RTSP, normalmente la 554, può utilizzare questo framework in Caching Proxy per far gestire le proprie richieste dal reindirizzamento RTSP.

Il reindirizzamento RTSP non memorizza nella cache, né agisce come proxy diretto per le presentazioni multimediali. Deve essere utilizzato insieme a un server per audio e/o video in streaming per fornire una o entrambe queste funzioni. Caching Proxy con il reindirizzamento RTSP deve avere accesso in rete a uno o più server proxy RTSP.

Limitazione a RTSP

Questa funzione è soggetta alla seguente limitazione:

Attualmente, sono supportate solo le tecnologie RealNetworks. Queste comprendono il server proxy RealProxy, il server di origine RealServer e il lettore multimediale RealPlayer.

Migliorie a RTSP

In precedenza, il reindirizzamento RTSP era soggetto a una limitazione per cui tutte le richieste per lo stesso server di origine, per qualsiasi URL, venivano reindirizzate allo stesso modo. Il reindirizzamento basato su nome file o altre parti dell'URL richiesto non era possibile. Questa limitazione è stata superata. Il reindirizzamento RTSP utilizza ora l'URL completo delle richieste ricevute, insieme al valore di soglia (rtsp_proxy_threshold) impostato nel file di configurazione di Caching Proxy per stabilire se reindirizzare la richiesta client al server di origine o a un server proxy. Le richieste allo stesso server di origine vengono ora gestite singolarmente.

Configurazione del reindirizzamento RTSP

Le direttive del file di configurazione che seguono vengono utilizzate per controllare il reindirizzamento RTSP. Le impostazioni per queste direttive non vengono aggiornate con il semplice riavvio del server. Il server dev'essere totalmente arrestato e quindi avviato per rendere effettive le modifiche a queste direttive.

- "RTSPEnable — Indica di abilitare il reindirizzamento RTSP" a pagina 257
- "rtsp_proxy_server - Indica di specificare i server per il reindirizzamento" a pagina 257
- "rtsp_proxy_threshold — Indica di specificare il numero di richieste prima di reindirizzarle alla cache" a pagina 258
- "rtsp_url_list_size — Indica di specificare il numero di URL nella memoria proxy" a pagina 258

Capitolo 14. Configurazione delle opzioni per le intestazioni

Quando richiedono documenti, i client Web inviano intestazioni che forniscono ulteriori informazioni sul browser o la richiesta. Le intestazioni vengono generate automaticamente all'invio di una richiesta.

Caching Proxy mette a disposizione diverse opzioni per la personalizzazione delle informazioni nelle intestazioni per mantenerle nascoste al server di destinazione. Anche se la sostituzione dell'intestazione effettiva con una più generica presenta il vantaggio di aumentare l'anonimato del client, ha anche lo svantaggio di impedire la personalizzazione della pagina in base all'intestazione, prevista per alcune pagine Web.

Le intestazione utilizzano normalmente la forma che segue:

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

Questa intestazione comprende i seguenti campi:

- **User-Agent:** fornisce informazioni sul browser e il sistema operativo.
- **Client-IP:** fornisce l'indirizzo IP del client che richiede l'URL.
- **Referer:** fornisce al server di destinazione l'URL del riferimento a questa pagina.

Per la maggior parte, è possibile bloccare le intestazioni mediante adeguate impostazioni della configurazione del proxy. Tuttavia, alcuni campi dell'intestazione sono necessari per il server di origine, per cui bloccandoli le pagine Web potrebbero venire visualizzate in modo errato; ad esempio, in alcuni casi il blocco del campo ″host″ dell'intestazione fa sì che gli utenti visualizzino la pagina Web sbagliata. Per ulteriori informazioni sui campi dell'intestazione, fare riferimento alla specifica HTTP Versione 1.1.

Direttive associate

Per modificare le opzioni di intestazione mediante la modifica del file di configurazione proxy, vedere le sezioni di riferimento dedicate alle seguenti direttive:

- "NoProxyHeader — Indica di specificare le intestazioni client da bloccare" a pagina 232
- "ProxyFrom — Indica di specificare un client con un'intestazione From:" a pagina 249
- "ProxyIgnoreNoCache — Indica di ignorare una richiesta di caricamento" a pagina 250
- "ProxySendClientAddress — Indica di generare un'intestazione IP Address: del client" a pagina 250
- "ProxyUserAgent — Indica di modificare la stringa agente utente" a pagina 251
- "ProxyVia — Indica di specificare il formato dell'intestazione HTTP" a pagina 251

Per ulteriori informazioni, fare riferimento a Capitolo 4, "Modifica manuale del file ibmproxy.conf", a pagina 13.

Moduli di Gestione e configurazione

È possibile utilizzare due moduli di Gestione e configurazione per specificare le opzioni di intestazione:

- Selezionare **Configurazione proxy –> Opzioni di riservatezza**. Nel modulo **Impostazioni di riservatezza**, impostare quanto segue:
  - **Inoltra l'indirizzo IP del client al server di destinazione**

    Selezionare questa casella per consentire l'inoltro dell'indirizzo IP del client richiedente al server di destinazione (dei contenuti). Se non si seleziona questa casella, il server di destinazione riceve l'indirizzo IP del server proxy. Lasciando questa casella deselezionata si aumenta l'anonimato del client durante la navigazione sul Web.
  - **Stringa User-agent**

    Digitare la stringa da inviare nell'intestazione al server di destinazione in sostituzione del tipo di browser e del sistema operativo in uso su un client. Ad esempio: specificando `Caching Proxy 4.0` si sostituisce `Mozilla 2.02/OS2` nell'intestazione seguente:

    ```
    Content-Type:MIME
    User-Agent: Mozilla 2.02/OS2
    Referer: http://www.ics.raleigh.ibm.com/WebTrafficExpress/main.html
    Pragma:no-cache
    ```
  - **From:**

    Immettere l'indirizzo di e-mail letto dal server di destinazione durante l'analisi dell'intestazione "From:". Si potrebbe voler specificare l'indirizzo di e-mail dell'amministratore del proxy, dal momento che l'amministratore è la persona che deve ricevere le segnalazioni di eventuali problemi.
  - Fare clic su **Inoltra** per apportare le modifiche al file di configurazione.
- Selezionare **Configurazione proxy –> Filtro intestazioni proxy**. Utilizzare questo modulo per elencare le intestazioni HTTP da bloccare:
  1. Fare clic su **Aggiungi** o **Rimuovi** e indicare una posizione di indice per l'intestazione bloccata.
  2. Digitare l'intestazione HTTP del client da bloccare. (Fare riferimento alla specifica HTTP 1.1 per un elenco completo e una spiegazione delle intestazioni.)
  3. Fare clic su **Inoltra** per apportare le modifiche al file di configurazione.

Per ulteriori informazioni, fare riferimento a Capitolo 2, "Utilizzo dei moduli di Gestione e configurazione", a pagina 7.

Capitolo 15. Informazioni sull'API (application programming interface)

L'API (application programming interface) viene illustrata completamente nella *Programming Guide for Edge Components*. Le direttive API contenute nel file di configurazione abilitano le routine plug-in richiamate durante le fasi specifiche nel flusso di elaborazione delle richieste. Queste routine plug-in possono sostituire le routine incorporate o essere eseguite in aggiunta.

Direttive associate

Di seguito sono riportate le direttive API:

- "Authentication — Indica di personalizzare la fase Autenticazione" a pagina 177
- "Authorization — Indica di personalizzare la fase Autorizzazione" a pagina 178
- "Error — Indica di personalizzare la fase Errore" a pagina 202
- "Log — Indica di personalizzare la fase Log" a pagina 222
- "Midnight — Indica di specificare il plugin dell'API utilizzato per archiviare i log" a pagina 229
- "NameTrans — Indica di personalizzare la fase Conversione nome" a pagina 230
- "ObjectType — Indica di personalizzare la fase Tipo di oggetto" a pagina 233
- "PostAuth — Indica di personalizzare la fase PostAuth" a pagina 238
- "PostExit — Consente di personalizzare la fase PostExit" a pagina 239
- "PreExit — Indica di personalizzare la fase PreExit" a pagina 239
- "ServerInit — Indica di personalizzare la fase Inizializzazione del server" a pagina 261
- "ServerTerm — Indica di personalizzare la fase Chiusura del server" a pagina 262
- "Service — Indica di personalizzare la fase Servizio" a pagina 262
- "Transmogrifier — Indica di personalizzare la fase Manipolazione dei dati" a pagina 270
- "TransmogrifiedWarning — Indica di inviare un messaggio di avvertenza al client" a pagina 270

Per ulteriori informazioni, fare riferimento a Capitolo 4, "Modifica manuale del file ibmproxy.conf", a pagina 13.

Moduli di Gestione e configurazione

Il modulo di Gestione e configurazione che segue modifica i valori delle direttive associate:

- **Configurazione server –> Elaborazione delle richieste –> Elaborazione delle richieste API**

Per ulteriori informazioni, fare riferimento a Capitolo 2, "Utilizzo dei moduli di Gestione e configurazione", a pagina 7.

Parte 4. Configurazione della cache di server proxy

Questa sezione illustra la cache del proxy e le relative modalità di configurazione. La cache può essere impostata per l'archiviazione dei file in memoria (cache in memoria) o su uno o più dispositivi di memorizzazione (cache su disco). È possibile configurare un agente di aggiornamento della cache per eseguire il caricamento preventivo nella cache dei file richiesti di frequente e applicare diversi filtri URL al processo di memorizzazione nella cache. Inoltre, questa sezione illustra la condivisione della cache mediante l'uso dell'accesso remoto alla cache o del plugin ICP (Internet caching protocol), la rimozione dei file obsoleti con la raccolta dati inutili della cache, e la memorizzazione nella cache dei file generati in modo dinamico.

Di seguito vengono forniti i titoli di ciascun capitolo di questa sezione:

Capitolo 16. Panoramica della memorizzazione nella cache del server proxy

La memorizzazione nella cache è una funzione in base alla quale il server proxy salva le copie locali dei file che i client richiedono; in questo modo, il server può fornirle velocemente prendendole dalla cache quando vengono richieste da quei client o da altri.

Il Caching Proxy è compatibile con HTTP 1.1 e segue generalmente il protocollo HTTP 1.1 per memorizzare e determinare lo stato di aggiornamento dei documenti.

In questo capitolo vengono illustrate alcune funzioni della cache del server proxy. Per quelle funzioni che possono essere configurate, nei seguenti capitoli vengono forniti ulteriori dettagli su come impostare i valori appropriati.

Memoria cache

Il server proxy può memorizzare la cache su un'unità di memoria fisica o nella memoria del sistema. La scelta della memoria cache migliore per il sistema dipende dalle capacità dell'hardware di cui si dispone e se sia importante una risposta cache veloce o un numero maggiore di elementi memorizzati nella cache. Normalmente, il tempo di risposta di una memoria cache è superiore rispetto a una cache su disco, ma la dimensione di una memoria cache è limitata dalla quantità di RAM della macchina del server proxy. La dimensione di una cache su disco è limitata dalla dimensione dell'unità di memoria che, normalmente, è molto più grande della quantità di RAM.

Per le cache su disco, il Caching Proxy utilizza una cache su disco non formattato, ciò vuol dire che il server proxy scrive direttamente sull'unità cache senza utilizzare i protocolli di lettura e scrittura del sistema operativo. È necessario preparare l'unità di memoria di una cache su disco utilizzando il comando **htcformat**. Le informazioni sul comando **htcformat** sono incluse nella sezione Capitolo 17, "Configurazione della memorizzazione cache di base", a pagina 77.

L'indice di cache

In una cache di memoria o su disco, il Caching Proxy utilizza lo spazio di memoria del sistema per contenere un indice della cache che riduce il tempo di elaborazione necessario per trovare i file memorizzati nella cache.

La struttura della directory di cache del Caching Proxy e i metodi di ricerca sono diversi da quelli degli altri server proxy. Il Caching Proxy gestisce un indice nella memoria con le informazioni sui file contenuti nella cache. L'uso della RAM per la ricerca, anziché di un disco o di un altro supporto, determina una ricerca e un recupero dei file più veloce.

L'indice include gli URL, le ubicazioni cache e le informazioni sulla scadenza degli oggetti memorizzati nella cache. Per questo motivo, la quantità di memoria necessaria per contenere l'indice è proporzionale al numero di oggetti nella cache.

Quando si riceve una richiesta da un client, il proxy controlla l'indice della cache nella memoria di quell'URL.

- Se il file non è nell'indice, la richiesta viene fatta al server di destinazione.
  - L'URL viene quindi controllato per stabilire se il file richiamato può essere memorizzato nella cache. Se possibile, il server proxy memorizza nella cache il file richiamato.
  - L'indice di cache viene quindi aggiornato con le informazioni sull'URL, l'ubicazione e la scadenza dell'oggetto appena memorizzato.
- Se il file è nell'indice:
  - Le informazioni sulla scadenza vengono memorizzate nella cache per stabilire se il file memorizzato è aggiornato.
    - Se l'oggetto è scaduto, viene contattato il server di destinazione e l'oggetto scaduto è sostituito da un documento appena richiamato. Le informazioni sulla scadenza vengono aggiornate nell'indice di cache.
    - Se l'oggetto non è scaduto, il documento viene supportato dalla cache proxy.

Memorizzazione nella cache di FTP

Se il proxy viene configurato sulle richieste di cache, è in grado di memorizzare nella cache le richieste di file FTP e le richieste di file HTTP. Tuttavia, poiché i file FTP non contengono lo stesso tipo di informazioni di intestazione dei file HTTP, le date di scadenza dei file FTP memorizzati nella cache vengono calcolate in modo diverso dagli altri file memorizzati nella cache.

Se si effettua una richiesta al server FTP per richiamare un file, il proxy prima invia una richiesta LIST per il file al server FTP per ottenere le informazioni di directory FTP sul file. Se il server FTP risponde alla richiesta LIST con una risposta positiva di completamento e con le informazioni di directory del file, il proxy crea un'intestazione HTTP Last-Modified con la data analizzata delle informazioni sulla directory FTP. La funzione di memorizzazione nella cache del proxy utilizza questa intestazione Last-Modified, insieme al valore impostato nella direttiva CacheLastModifiedFactor nel file di configurazione, per stabilire l'intervallo di tempo in cui il file FTP rimane nella cache prima di scadere.

Per maggiori informazioni su come l'intestazione Last-Modified e la direttiva CacheLastModifiedFactor vengono utilizzate per stabilire l'intervallo di tempo in cui un file rimane nella cache, consultare Capitolo 19, "Manutenzione del contenuto della cache", a pagina 85.

I file FTP richiamati per un ID utente specifico, anziché da un collegamento anonimo, vengono considerati file privati e non memorizzati nella cache.

Memorizzazione nella cache di DNS

Oltre alla memorizzazione su cache dei contenuti Web, il server proxy esegue la memorizzazione nella cache (DNS) del server nome dominio. Ad esempio, se un client richiede un URL da www.myWebsite.com, il proxy chiede al server DNS di risolvere il nome host www.myWebsite.com su un indirizzo IP. L'indirizzo IP viene quindi memorizzato nella cache per migliorare il tempo di risposta delle successive richieste a quel nome host. La memorizzazione nella cache DNS è automatica e non può essere configurata.

Esclusioni cache

Alcuni file e documenti non vengono mai memorizzati nella cache. Tra questi sono inclusi:

- I file restituiti dalle richieste che utilizzano metodi HTTP diversi da GET, come ad esempio POST e PUT.
- Qualsiasi documento che richiede autenticazione, a meno che la memorizzazione nella cache di tali documenti non sia esplicitamente consentita dal server di origine.
- L'output dinamico di qualsiasi script CGI (perché è univoco ogni volta che viene richiesto). I risultati generati dinamicamente dai servlet e dalle JSP (JavaServer Pages) eseguiti da IBM WebSphere Application Server possono essere memorizzati se è abilitata la memorizzazione dinamica nella cache. Per maggiori informazioni, fare riferimento a Capitolo 22, "Memorizzazione nella cache di contenuto generato dinamicamente", a pagina 101.
- Qualsiasi file restituito da un URL contenente un punto interrogativo (?), a meno che non sia consentita la memorizzazione nella cache delle query. (Fare riferimento a Capitolo 18, "Controllo degli elementi memorizzati nella cache", a pagina 81 per informazioni sulla configurazione della memorizzazione nella cache dei risultati di query).

È possibile limitare ulteriormente gli elementi memorizzati nella cache impostando dei filtri di cache. Ad esempio, si può desiderare che server proxy non memorizzi nella cache i file supportati localmente dal proxy. Per informazioni, fare riferimento a Capitolo 18, "Controllo degli elementi memorizzati nella cache", a pagina 81.

Gestione cache

La gestione della cache include diversi fattori. Come amministratore server, è possibile specificare quanto segue:

- Quali documenti sono memorizzati nella cache (fare riferimento a Capitolo 18, "Controllo degli elementi memorizzati nella cache", a pagina 81 per maggiori dettagli).
- Il numero di documenti che può essere memorizzato nella cache (fare riferimento a Capitolo 17, "Configurazione della memorizzazione cache di base", a pagina 77 per informazioni).
- Per quanto tempo i documenti vengono considerati correnti (fare riferimento a Capitolo 19, "Manutenzione del contenuto della cache", a pagina 85 per informazioni).
- La frequenza con cui la cache viene ripulita (raccolta di dati inutili) e il tipo di file che si tende a conservare (fare riferimento a Capitolo 19, "Manutenzione del contenuto della cache", a pagina 85 per informazioni).
- Come vengono indicizzati i documenti memorizzati nella cache (fare riferimento a Capitolo 17, "Configurazione della memorizzazione cache di base", a pagina 77 per informazioni).
- Quando viene aggiornata la cache (Fare riferimento a Capitolo 20, "Configurazione dell'agente cache per il precaricamento e l'aggiornamento automatici", a pagina 91 per informazioni).
- Accesso remoto alla cache (fare riferimento a Capitolo 21, "Utilizzo di una cache condivisa", a pagina 97 per informazioni).
- Come vengono conservati e archiviati i log (fare riferimento a Capitolo 17, "Configurazione della memorizzazione cache di base", a pagina 77 per informazioni).

Inoltre, è possibile regolare la configurazione cache per migliorare le prestazioni del Caching Proxy. Per maggiori informazioni sull'ottimizzazione delle prestazioni, fare riferimento a Capitolo 23, "Ottimizzazione della cache del server proxy", a pagina 105.

Capitolo 17. Configurazione della memorizzazione cache di base

Se sono state utilizzate le impostazioni predefinite nel Programma di installazione del prodotto Edge Components per installare il Caching Proxy, la memorizzazione nella cache è abilitata e la cache è memorizzata nella memoria. È possibile regolare le seguenti impostazioni di cache di base per personalizzare la cache in base alle esigenze del sistema in uso.

Se non è stato utilizzato il programma di installazione, configurare queste impostazioni per abilitare la memorizzazione nella cache.

Le operazioni di base necessarie per configurare la cache sono le seguenti:

1. Abilitazione della memorizzazione nella cache.
2. Configurazione della memoria di cache.

Dopo aver configurato le impostazioni cache di base, è possibile aggiungere o modificare le impostazioni per le seguenti funzioni.

- Personalizzare la memoria cache.
- Salvare o caricare la memoria cache sul disco.
- Limitare il numero di elementi da memorizzare nella cache utilizzando i filtri URL.
- Espandere ciò che verrà memorizzato nella cache abilitando la memorizzazione nella cache dei risultati di query o dei file generati dinamicamente.
- Configurare la scadenza dei file memorizzati nella cache e la raccolta dati inutili.
- Configurare il precaricamento e l'aggiornamento automatico della cache.
- Configurare la condivisione cache con RCA (remote cache access) o ICP (Internet caching protocol).
- Configurare la registrazione.

In questo capitolo vengono fornite o indicate le istruzioni sulla modifica di queste informazioni.

1. Abilitazione della memorizzazione nella cache

Per abilitare la memorizzazione nella cache, abilitare la direttiva Memorizzazione nella cache oppure selezionare la casella di controllo **Abilita memorizzazione nella cache del proxy** sul modulo di configurazione **Configurazione cache –> Impostazioni cache**. Se non si specifica un'unità cache, la cache verrà memorizzata nella memoria. Per creare una cache su disco, seguire le operazioni in "2. Configurazione della memoria cache".

2. Configurazione della memoria cache

Le attività per la configurazione della memoria cache dipendono dall'uso di una cache di memoria o di una cache su disco.

Per utilizzare una cache di memoria, personalizzare l'impostazione Memoria cache in modo da includere una quantità di memoria sufficiente per contenere i contenuti di una cache. Consultare "Impostazione memoria di cache" a pagina 78 per le dimensioni di memoria cache consigliate.

Per utilizzare una cache su disco, effettuare quanto segue:

1. Preparare un'unità di memoria per contenere la cache.

   La cache richiede un'unità formattata. Si consiglia di dedicare un'intera unità o partizione disco alla cache. La dimensione massima per la cache è 16392 KB.

   Per formattare l'unità cache:

   a. Scegliere un'unità che contenga la cache. Verificare che nessun altro programma stia utilizzando quello spazio memoria e che sia possibile accedere all'unità come a un'unità non formattata (formattato in modalità carattere).

   b. Formattare l'unità mediante il comando **htcformat**. La sintassi è la seguente:

      ```
      htcformat raw_device_path [-blocksize block_size]
           [-blocks number_of_blocks]
      ```

      Gli argomenti -blocksize e -blocks sono facoltativi. La dimensione blocco predefinita è di 8192 byte. Se non viene specificato il numero di blocchi, la partizione disco verrà riempita con tutti i blocchi che è in grado di contenere.

      Se si specifica il percorso unità, specificare il percorso dell'unità non formattata.

      - Sulle piattaforme AIX, il percorso dell'unità non formattata per un volume logico definito come /dev/lv02 è /dev/rlv02
      - Sulle piattaforme Linux, è necessario eseguire prima il comando **raw** per poi eseguire **htcformat** e associare il percorso unità non formattata all'unità sdb1 SCSI reale.

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

      - Sulle piattaforme HP-UX e Solaris, il percorso unità non formattata di una partizione definita come /dev/dsk/c0t0d0s0 è /dev/rdsk/c0t0d0s0
      - Sulle piattaforme, il percorso dell'unità non formattata per un'unità e: è \\.\e:

      Consultare il materiale di riferimento sul file system per maggiori informazioni riguardo l'accesso a unità non formattate.

2. Specificare l'unità cache mediante la direttiva CacheDev o il modulo di configurazione delle **Impostazioni cache**. È possibile specificare più di un'unità.

Avvertenza:
Sui sistemi Windows, il comando htcformat non contrassegna automaticamente l'unità cache come non scrivibile.

Se il sistema operativo tenta di scrivere sull'unità cache, i dati memorizzati nella cache potrebbero andare persi. Per evitare ciò, è possibile utilizzare il programma di utilità Windows Disk Manager per preparare il disco prima di usare il comando htcformat. Per preparare il disco, utilizzare il programma di utilità del disco per eliminare l'unità o la partizione che si desidera utilizzare, quindi ricrearla senza formattarla. In questo modo, il sistema considera l'unità non disponibile per la memoria del sistema.

Personalizzazioni facoltative

Impostazione memoria di cache

Impostare il valore nella direttiva CacheMemory (o nel campo **Memoria cache** del modulo di configurazione **Impostazioni cache**), in base ai seguenti principi. La quantità di memoria impostata su questo valore viene utilizzata per supportare

l'infrastruttura cache, incluso l'indice cache e, se la memorizzazione nella cache è configurata, per memorizzare i contenuti della cache.

Valori minimi

Per una prestazione ottimale delle cache su disco, è consigliabile un valore di memoria cache minimo di 64 MB per il supporto dell'infrastruttura cache, incluso l'indice di cache. Con l'aumento della dimensione di cache, aumenta anche l'indice di cache e, di conseguenza, è necessaria più memoria per memorizzare l'indice. Un valore di memoria cache di 64 MB è sufficiente per supportare l'infrastruttura cache e memorizzare un indice di cache per una cache su disco con una dimensione fino a 6,4 GB. Per delle cache su disco più grandi, la memoria cache deve essere l'1% della dimensione cache.

Per le cache di memoria, il valore della memoria cache equivale alla quantità di memoria riservata per il supporto dell'infrastruttura cache e per la cache stessa. È consigliabile un valore di memoria cache minimo di 64 MB.

Valore massimo

Se per una memoria cache è assegnata troppa memoria fisica, si possono verificare operazioni indesiderate come errori di "memoria insufficiente" o guasti sul server proxy. Le limitazioni di valore per la memoria cache sono dovuti alle limitazioni di un'applicazione da 32 bit. Poiché il Caching Proxy è un'applicazione a 32 bit, può utilizzare un massimo di 2 GB di memoria.

Il Caching Proxy assegna la memoria definita dalla direttiva CacheMemory e la utilizza come cache per memorizzare gli oggetti. Se si tratta di una cache di memoria o di una cache su disco non formattato, è necessario assegnare altra memoria per le strutture dati per la cache, per I/E di rete e buffer di connessione, buffer di sessione e memoria per il processo principale e per tutti i thread. Inoltre, è possibile che le richieste di alcuni client debbano assegnare un blocco lotto di memoria più ampio rispetto a quello predefinito. Quindi, se la direttiva CacheMemory è impostata approssimativamente su 2 GB, è possibile che il Caching Proxy non abbia spazio sufficiente per funzionare, soprattutto sotto carichi di richieste eccessivi.

È consigliabile, quindi, che il valore della direttiva CacheMemory sia inferiore o uguale a 1600 MB. Un valore superiore a 1600 MB crea interferenza con la memoria di cui il Caching Proxy ha bisogno per il normale funzionamento e causa degli effetti collaterali sfavorevoli. Questi effetti collaterali includono un maggiore uso della CPU (possibilmente fino al 100%), errori di memoria insufficiente e prestazioni più lente. Se si richiede una dimensione cache complessiva maggiore, utilizzare le unità cache o implementare una configurazione cache condivisa con RCA o ICP.

Salvataggio o caricamento della memoria cache su disco

È possibile importare ed esportare i contenuti cache su e da un file di dump. Ciò risulta utile se la memoria cache va persa durante il riavvio o se si distribuisce la stessa cache su più proxy.

Impostazione dei filtri di memorizzazione nella cache

I filtri possono limitare ciò che è memorizzato nella cache confrontando il modulo della richiesta URL. Consultare Capitolo 18, "Controllo degli elementi memorizzati nella cache", a pagina 81 per maggiori dettagli sulle impostazioni dei filtri.

Configurazione della memorizzazione nella cache per i risultati di query e per i file generati dinamicamente

Facoltativamente, è possibile configurare il server proxy per memorizzare i risultati delle richieste di query. Per impostazione predefinita, gli URL che contengono un punto interrogativo (?) non sono memorizzati nella cache. Fare riferimento a "Memorizzazione nella cache delle risposte di query" a pagina 82 per maggiori dettagli.

Un'altra possibilità è quella di memorizzare i risultati del servlet o dell'esecuzione JSP da un IBM WebSphere Application Server. Fare riferimento a Capitolo 22, "Memorizzazione nella cache di contenuto generato dinamicamente", a pagina 101 per maggiori dettagli.

Configurazione della scadenza dei file e della raccolta dati inutili

Fare riferimento a Capitolo 19, "Manutenzione del contenuto della cache", a pagina 85 per informazioni sulla configurazione quando i file nella cache scadono e su come rimuovere i file obsoleti.

Configurazione del precaricamento automatico

La cache può essere configurata per aggiornare automaticamente i file più comuni su una base giornaliera prima che vengano richiesti. Per informazioni, fare riferimento a Capitolo 20, "Configurazione dell'agente cache per il precaricamento e l'aggiornamento automatici", a pagina 91.

Configurazione della condivisione cache

In determinate circostanze, utilizzando una cache condivisa si aumenta la probabilità di trovare un file richiesto nella cache. Per informazioni, fare riferimento a Capitolo 21, "Utilizzo di una cache condivisa", a pagina 97.

Configurazione della registrazione

La manutenzione di log accurati e ridotti è importante per la gestione del Caching Proxy. Parte 6, "Monitoraggio di Caching Proxy", a pagina 139 contiene informazioni sulla configurazione e sull'utilizzo dei log di server proxy.

Capitolo 18. Controllo degli elementi memorizzati nella cache

Il caching proxy offre diversi metodi di filtraggio che permettono di controllare quali file, documenti e altri oggetti vengono memorizzati nella cache. Tali metodi includono le seguenti funzioni:

- Filtri di memorizzazione nella cache basati sull'URL
- Memorizzazione nella cache delle risposte di query
- Memorizzazione nella cache di file supportati localmente
- Memorizzazione nella cache parziale basata sull'URL
- Memorizzazione nella cache di file basati su parte dell'URL di richiesta
- Memorizzazione nella cache di file generati dinamicamente — fare riferimento a Capitolo 22, "Memorizzazione nella cache di contenuto generato dinamicamente", a pagina 101

Nota: Il modulo **Configurazione della cache** –> **Funzionamento della cache** di Gestione e configurazione contiene un'opzione intitolata **Cache basata su URL in entrata**. (La direttiva del file di configurazione corrispondente è denominata CacheByIncomingURL.) Questa direttiva fa riferimento al nome file del file memorizzato nella cache. Selezionare la casella alla base del nome file del file memorizzato nella cache sull'URL in entrata; se questa casella di controllo non è selezionata, il nome file si basa sull'URL in uscita.

Configurazione di filtri di memorizzazione nella cache basati sull'URL

Il server proxy può essere configurato per confrontare le richieste a una maschera URL per stabilire se un file è memorizzato nella cache. Questa funzione viene configurata impostando le maschere per le richieste i cui file sono *sempre* memorizzati nella cache e separando le maschere per le richieste i cui file non devono *mai* essere memorizzati nella cache. È possibile utilizzare più maschere.

Un sistema simile viene utilizzato per consentire la memorizzazione nella cache delle risposte di query. Per informazioni, fare riferimento a "Memorizzazione nella cache delle risposte di query" a pagina 82.

Per impostare i filtri di memorizzazione nella cache dell'URL modificando il file ibmproxy.conf, fare riferimento a "CacheOnly — Indica di memorizzare solo i file con gli URL corrispondenti a una maschera" a pagina 187 e "NoCaching — Indica di specificare di non memorizzare nella cache i file con URL corrispondenti a una maschera" a pagina 231.

Per impostare i filtri di memorizzazione nella cache dell'URL nei moduli Gestione e configurazione, utilizzare il campo **Configurazione della cache** –> **Funzionamento della cache**: **Filtraggio cache secondo l'URL**. Utilizzare questa sezione per specificare gli URL i cui file sono sempre memorizzati nella cache oppure specificare gli URL i cui file non sono mai memorizzati nella cache. Per specificare i due elenchi, uno relativo ai file da memorizzare sempre nella cache, un altro dei file che non devono mai essere memorizzati nella cache, creare un elenco e fare clic su **Inoltra** prima di creare l'altro elenco.

Memorizzazione nella cache delle risposte di query

Le risposte restituite dalle query (richieste di URL che contengono un punto interrogativo), possono essere memorizzate utilizzando i filtri della memorizzazione nella cache. Questa funzione può essere utile in scenari di proxy inversi (sostituto) nel caso in cui molti client facciano al stessa richiesta di query.

La memorizzazione nella cache delle query può essere configurata modificando la direttiva CacheQueries nel file di configurazione ibmproxy.conf. La direttiva CacheQueries ha le seguenti opzioni:

- Sempre — tutte le risposte di query dagli host, corrispondenti alla maschera, verranno memorizzate nella cache, se sono memorizzabili, secondo gli standard HTTP 1.1.
- Pubbliche — le risposte di query dagli host, corrispondenti alla maschera, verranno memorizzate nella cache se contengono l'intestazione ″Cache-control: public″ o un'intestazione di riconvalida forzata e se sono memorizzabili secondo gli standard HTTP 1.1.

Altre informazioni su queste opzioni sono disponibili in "CacheQueries — Indica di specificare le risposte cache agli URL contenenti un carattere punto interrogativo (?)" a pagina 187.

Per configurare la memorizzazione nella cache delle risposte di query nei moduli Gestione e configurazione, utilizzare il campo **Configurazione della cache** –> **Funzionamento della cache**: **Filtraggio della risposta query cache secondo l'URL**. Per specificare i due elenchi, creare un elenco e fare clic su **Inoltra** prima di creare l'altro elenco.

Requisiti aggiuntivi per la memorizzazione nella cache delle risposte di query

Oltre alla configurazione dell'impostazione della memorizzazione nella cache delle query, verificare che le seguenti impostazioni siano configurate correttamente per abilitare le risposte di query da memorizzare. Fare riferimento a "Configurazione aggiornamento cache" a pagina 88 per informazioni su come impostare queste opzioni mediante i moduli Gestione e configurazione.

- CacheTimeMargin — Questa direttiva specifica una scadenza minima; i file la cui scadenza è inferiore a questo livello minimo, non verranno memorizzati nella cache. Poiché le risposte di query a volte hanno delle scadenze molto brevi, diminuendo il valore dell'impostazione di tale direttiva sarà possibile memorizzare nella cache un numero maggiore di query. Fare riferimento a "CacheTimeMargin — Indica di specificare la durata minima per la memorizzazione di un file nella cache" a pagina 188 oppure utilizzare il modulo **Impostazioni di scadenza cache**, descritto in "Configurazione aggiornamento cache" a pagina 88.
- CacheDefaultExpiry — questa direttiva indica la scadenza dei file che non hanno una data di scadenza esplicita o una data dell'ultima modifica da cui calcolare la scadenza. Aumentando, a partire da un valore predefinito di 0, questa impostazione per le richieste HTTP sarà possibile memorizzare nella cache un numero maggiore di risposte di query. Tuttavia, memorizzando l'impostazione in questo modo si aumenta anche il rischio che contenuti obsoleti vengano forniti dalla cache. Fare riferimento a "CacheDefaultExpiry — Indica di specificare la scadenza predefinita dei file" a pagina 181 oppure utilizzare il modulo **Impostazioni di scadenza cache**, descritto in "Configurazione aggiornamento cache" a pagina 88.

- CacheLastModifiedFactor — questa direttiva viene utilizzata per calcolare una data di scadenza per i file che hanno una data dell'ultima modifica ma nessuna data di scadenza esplicita. Impostando il fattore dei file HTTP su un valore più alto, si aumenta l'intervallo di tempo in cui un file HTTP risiede nella cache senza essere riconvalidato. Memorizzando l'impostazione in questo modo si aumenta anche il rischio che contenuti obsoleti vengano forniti dalla cache. Fare riferimento a "CacheLastModifiedFactor — Indica di specificare il valore per determinare le date di scadenza" a pagina 183 oppure utilizzare il modulo **Fattore ultima modifica**, descritto in "Configurazione aggiornamento cache" a pagina 88.
- Facoltativamente, impostare le direttive SignificantUrlTerminator e AggressiveCaching. Fare riferimento a "SignificantURLTerminator — Indica di specificare un codice di interruzione per le richieste URL" a pagina 263 e "AggressiveCaching — Indica di specificare la memorizzazione nella cache di file non memorizzabili nella cache" a pagina 176.

Memorizzazione nella cache di file supportati localmente

Poiché non è conveniente memorizzare nella cache i file forniti da server proxy, i file che hanno origine nel dominio locale del server per impostazione predefinita non vengono memorizzati nella cache. Per memorizzare nella cache gli oggetti che hanno origine nel dominio locale del server, controllare la casella di controllo **Memorizzazione nella cache dei file dominio locale** sul modulo Gestione e configurazione **Configurazione della cache** –> **Funzionamento della cache**. In alternativa, impostare la direttiva CacheLocalDomain nel file di configurazione proxy su `on`.

Memorizzazione nella cache dei file secondo URL parziale

Gli elementi possono essere memorizzati nella cache sulla base di una sola parte specificata (importante) dell'URL in entrata, anziché dell'URL completo. Ciò è utile per il supporto Web modello transazione o per la memorizzazione dinamica nella cacha, poiché la stessa risposta viene spesso restituita per diverse richieste in entrata se parti significative degli URL delle richieste in entrata sono identiche.

Non è possibile utilizzare i moduli Gestione e configurazione per una memorizzazione cache particolare basata sugli URL parziali. Al contrario, utilizzare la direttiva SignificantUrlTerminator nel file di configurazione proxy per specificare un codice di interruzione per le richieste URL. Questa specifica fa in modo che il Caching Proxy valuti solo i caratteri prima del codice di interruzione quando elabora la richiesta e determina se il file di richiesta è memorizzato nella cache. Se viene definito un codice di interruzione, il Caching Proxy confronta gli URL in entrata con i codici di interruzione nell'ordine in cui vengono definiti nel file ibmproxy.conf. Per ulteriori informazioni, consultare "SignificantURLTerminator — Indica di specificare un codice di interruzione per le richieste URL" a pagina 263.

Direttive di file di configurazione correlati

Per impostare i filtri di cache direttamente modificando il file di configurazione del proxy, vedere le sezioni di riferimento delle seguenti direttive:

- "NoCaching — Indica di specificare di non memorizzare nella cache i file con URL corrispondenti a una maschera" a pagina 231
- "CacheOnly — Indica di memorizzare solo i file con gli URL corrispondenti a una maschera" a pagina 187

- "CacheQueries — Indica di specificare le risposte cache agli URL contenenti un carattere punto interrogativo (?)" a pagina 187
- "CacheLocalDomain — Indica di specificare se memorizzare nella cache il dominio locale" a pagina 184
- "SignificantURLTerminator — Indica di specificare un codice di interruzione per le richieste URL" a pagina 263

Consultare Capitolo 16, "Panoramica della memorizzazione nella cache del server proxy", a pagina 73 per informazioni sui documenti che non possono essere memorizzati nella cache.

Capitolo 19. Manutenzione del contenuto della cache

Poiché la memorizzazione nella cache include la creazione e il salvataggio di una copia del file fornito, è necessaria una manutenzione costante affinché la cache funzioni correttamente. I file memorizzati nella cache devono essere controllati per verificare l'*aggiornamento* e convalidati se non sono più coerenti con i file del server di origine. Il processo di scadenza di questo file viene illustrato in "Scadenza file". Inoltre, i file inutilizzati o non validi devono essere rimossi dalla cache per fare spazio ai nuovi file. Questo processo di eliminazione dalla cache viene descritto in "Raccolta dati inutili" a pagina 89.

Scadenza file

L'aggiornamento della cache consiste nel mantenere nella memoria cache quegli oggetti coerenti con l'oggetto originale presente sul server dei contenuti. Per ogni documento o altro oggetto memorizzato nella cache, il Caching Proxy calcola un tempo in cui l'oggetto scade.

Per le pagine HTTP, l'intestazione del documento, generato dal server dei contenuti, contiene le informazioni sulla scadenza.

Poiché il protocollo FTP non include le informazioni di scadenza equivalenti, il Caching Proxy genera la propria intestazione `Last-Modified:` per i file FTP, basata sulle informazioni della directory FTP di ciascun file e utilizza tali informazioni per calcolare i tempi di scadenza. Se il server proxy non è in grado di ottenere le informazioni di directory per il file del server FTP, viene utilizzato il valore predefinito corrispondente all'URL FTP. Inoltre, poiché non esiste un formato data standard per i server FTP, il Caching Proxy potrebbe non riconoscere la data e l'ora inviate da alcuni server FTP. In tal caso, viene utilizzato il valore predefinito dell'ora di scadenza del server proxy. Questa procedura consente al proxy di gestire la memorizzazione nella cache delle pagine HTTP e dei file FTP in un modo simile.

La scadenza può essere specificata da un server dei contenuti in uno dei seguenti modi (in ordine di preferenza):

1. Il server dei contenuti specifica un'intestazione che indica `Cache-control: s-maxage=`*n*. Questa informa il proxy che l'oggetto è aggiornato per *n* secondi dopo essere stato ricevuto.
2. Il server dei contenuti specifica un'intestazione che indica `Cache-control: max-age=` *n*. Questa informa il proxy che l'oggetto è aggiornato per *n* secondi dopo essere stato ricevuto.
3. Il server dei contenuti specifica l'intestazione: `Expires:` *n*. Questa informa il proxy che l'oggetto è aggiornato fino all'ora specificata da *n*.
4. Il server dei contenuti indica quando il documento è stato modificato per l'ultima volta tramite l'intestazione `Last-Modified:` *n*. Il server proxy calcola il periodo di tempo trascorso dal momento in cui è avvenuta l'ultima modifica del documento, lo moltiplica per il fattore Ultima modifica cache impostato nel file di configurazione proxy e presume che il documento sia valido per quel periodo di tempo. Ad esempio, se il server dei contenuti indica che il documento è stato modificato una settimana (sette giorni) fa e il fattore Ultima modifica cache è 0,14, il server proxy presume che il documento sia valido per

circa un giorno. Consultare “Configurazione aggiornamento cache” a pagina 88 per le istruzioni sull’impostazione del fattore Ultima modifica cache.

5. Se il server dei contenuti non specifica nessuna delle informazioni sopra indicate, il Caching Proxy ricerca l’impostazione Scadenza predefinita cache che corrisponde all’URL corrente e la utilizza come scadenza. Consultare “Configurazione aggiornamento cache” a pagina 88 per le istruzioni sull’impostazione dei valori di Scadenza predefinita cache.

Una volta calcolata l’ora di scadenza, nel modo appena descritto, il Caching Proxy controlla l’eventuale presenza di un valore di Mantenimento minimo da applicare a questo URL. Se il valore è presente e l’ora specificata è superiore a quella calcolata, l’ora indicata dal valore Mantenimento minimo viene utilizzata come ora di scadenza dell’oggetto. Questa condizione è valida anche se il Caching Proxy calcola un’ora di scadenza di 0 minuti per un documento. Quindi, per evitare dei contenuti obsoleti, utilizzare l’impostazione Mantenimento minimo con molta attenzione. (Per impostare il valore di Mantenimento minimo, utilizzare la direttiva CacheMinHold oppure l’impostazione **Configurazione cache –> Impostazioni di scadenza cache**: **Scadenza URL**. Fare riferimento a “Configurazione aggiornamento cache” a pagina 88 per maggiori informazioni).

Il valore dell’ora di scadenza finale viene confrontato con l’ora specificata nell’impostazione Margine ora. Se l’ora di scadenza è superiore al valore di Margine ora, il documento viene memorizzato nella cache; in caso contrario, non viene aggiunto nella cache. (Per impostare il valore Margine ora, utilizzare la direttiva CacheTimeMargin oppure vedere le istruzioni in “Configurazione aggiornamento cache” a pagina 88).

Se il documento si trova nella cache ma è scaduto, il Caching Proxy invia una richiesta speciale, nota come richiesta *if-modified-since*, al server dei contenuti. A causa di questa richiesta, il server dei contenuti invia il documento solo se è stato modificato dal momento in cui è stato ricevuto dal proxy. Se il documento non è stato modificato, il server dei contenuti invia un messaggio informativo e non rinvia la pagina. In tal caso, il proxy fornisce il documento memorizzato nella cache. Per i file FTP, il server proxy simula il processo if-modified-since. Se stabilisce che il file non è stato modificato sul server FTP, fornisce il file dalla cache. In caso contrario, ottiene la versione più aggiornata dal server FTP.

Informazioni aggiuntive sull’aggiornamento della cache

- La maggior parte dei documenti Web statici (in opposizione ai documenti generati dinamicamente) include l’intestazione Last-Modified. Questo è il modo più comune per i proxy per calcolare le ore di scadenza dei documenti e il primo metodo che il Caching Proxy tenta per i file FTP. Se il tentativo non riesce, il proxy fa riferimento ai valori della Scadenza predefinita.
- Pochi documenti utilizzano le intestazioni Cache-control: s-maxage, Cache-control: max-age o Expires:.
- Le pagine generate dinamicamente, che normalmente non sono memorizzabili nella cache, possono includere un’intestazione `Expires: 0` o `Cache-control: no-cache`, e indica che il documento scade immediatamente. Per maggiori informazioni sulla memorizzazione nella cache di file di IBM WebSphere Application Server generati in modo dinamico, consultare Capitolo 22, “Memorizzazione nella cache di contenuto generato dinamicamente”, a pagina 101.
- Fare attenzione a impostare la Scadenza predefinita su un valore diverso da 0 minuti per gli URL che utilizzano la sintassi HTTP:. Molte delle pagine generate

dinamicamente non includono nessuna intestazione di scadenza e sono quindi soggette al valore di Scadenza predefinito. L'impostazione della Scadenza predefinita su un valore superiore a 0 minuti consente al proxy di memorizzare tali oggetti, ma questo potrebbe determinare dei contenuti non aggiornati (o dei risultati imprevisti dei programmi CGI o servlet).

- Nelle seguenti circostanze, il server proxy convalida di nuovo i documenti con il server per ogni richiesta, a prescindere dal fatto che il documento memorizzato nella cache sia scaduto o meno:
  - Il documento include una delle seguenti intestazioni:
    - Cache-control: s-maxage
    - Cache-control: must-revalidate
    - Cache-control: proxy-revalidate
  - Il documento richiede le credenziali dell'utente ma può essere memorizzato nella cache dal server.
  - Il documento contiene un'intestazione Cache-Control: no-cache ma viene comunque memorizzato nella cache (a causa della memorizzazione aggressiva nella cache).

Informazioni sulle date in FTP

Poiché il protocollo FTP non definisce le date e le ore in modo così rigido come il protocollo HTTP, diversi fattori possono determinare delle leggere differenze tra l'intestazione Last-Modified, generata dal proxy per i file FTP, e la data effettiva del file. Tali fattori includono quanto segue:

- A differenza del protocollo HTTP, il protocollo FTP non specifica che le date restituite devono avere l'ora GMT (Greenwich Mean Time). La data restituita dal server FTP sembra essere impostata sull'ora locale del server FTP. Poiché il proxy non ha modo di determinare secondo quale fuso orario è in esecuzione il server FTP, interpreta l'ora in base al proprio fuso orario. Un'eccezione è data dal server FTP di Windows che restituisce le date in base all'ora GMT. Se il proxy rileva che il server FTP è in esecuzione su sistemi Windows, presume che la data della directory sia in base all'ora GMT.
- Alcuni server FTP specificano la data nelle informazioni sulla directory restituita solo nel formato *Mese Giorno Anno* e non includono le informazioni sulle ore e i minuti effettivi della data specificata. Se il server FTP non restituisce le informazioni sulle ore e i minuti del file, il proxy presuppone che il file sia stato modificato per l'ultima volta nelle ultime ore e minuti possibili della data restituita dal server FTP. Ad esempio, se il server FTP restituisce le informazioni, sulla directory di un file, che indicano che questo file è stato modificato per l'ultima volta il 13 ottobre 1998 ma non include le informazioni sulle ore e i minuti, il proxy presuppone che l'ultima modifica del file è avvenuta alle ore 23:59:59 del 13 ottobre 1998. Quindi, se non si tratta di un server FTP di Windows, il proxy converte questa data dal fuso orario locale all'ora GMT corrispondente.

Quando un file FTP di cache scade, il proxy simula il processo di riconvalida if-modified-since per tale file. Questo processo è possibile emettendo il comando FTP LIST del file richiesto, analizzando la data del file dalla risposta restituita dal server FTP e confrontando tale data con quella generata dal server proxy per l'intestazione Last-Modified quando il file è stato richiamato. Se la data del file non è stata modificata, il server proxy contrassegna come riconvalidato il file FTP memorizzato nella cache, imposta una nuova ora di scadenza per il file e fornisce quest'ultimo dalla cache anziché richiamarlo di nuovo dal server FTP. Se le due

date non corrispondono, il proxy richiama di nuovo il file del server FTP e memorizza nella cache la nuova copia con la nuova data del file.

Non è possibile ottenere sempre le informazioni di directory per il file del server FTP. Se il proxy non è in grado di determinare la data del file FTP, non genera l'intestazione Last-Modified per il file. Al contrario, utilizza il valore specificato per la direttiva CacheDefaultExpiry che corrisponde all'URL, in modo da determinare il periodo di tempo in cui conservare il file nella cache. Quando questo intervallo scade, il proxy richiama di nuovo il file dal server FTP. Se alcuni file FTP della cache sembrano utilizzare spesso la direttiva CacheDefaultExpiry e vengono richiamati frequentemente (generando un volume elevato di traffico di rete), specificare un valore CacheDefaultExpiry più granulare per quei file. In questo modo, tali file vengono conservati più a lungo nella cache.

Per specificare le impostazioni di scadenza della cache nei moduli Gestione e configurazione, utilizzare il modulo **Configurazione della cache** –> **Impostazioni di scadenza cache** –> **Limite di tempo dei file memorizzati nella cache**. Per maggiori dettagli sulle date di scadenza dei file memorizzati nella cache, consultare "Scadenza file" a pagina 85.

Configurazione aggiornamento cache

Per specificare l'ora di scadenza dei file memorizzati nella cache, nei moduli Gestione e configurazione selezionare **Configurazione della cache–> Impostazioni di scadenza cache**. Sono utili i seguenti moduli.

Scadenza basata su URL

Utilizzare questo modulo per impostare l'intervallo di tempo minimo in cui i file vengono conservati nella cache in base agli URL. È possibile specificare diversi funzionamenti della memorizzazione nella cache per diverse maschere di richiesta URL.

Per impostare la scadenza dei file basati sull'URL modificando il file di configurazione del proxy, consultare le sezioni di riferimento in Appendice B, "Direttive del file di configurazione", a pagina 165 per le seguenti direttive:

- "CacheMinHold — Indica di specificare l'intervallo di tempo entro il quale i file saranno disponibili" a pagina 186

Impostazioni di scadenza predefinita

Utilizzare il modulo **Impostazioni di scadenza cache** per specificare le impostazioni di scadenza predefinita dei file utilizzati e non. È possibile impostare diversi valori per i file HTTP, FTP e Gopher e diversi valori per i file utilizzati e non.

Questo modulo contiene anche ulteriori opzioni di scadenza dei file:

- **Abilitazione controllo di scadenza file memorizzati nella cache**. Questa casella di controllo è selezionata per impostazione predefinita. Generalmente, è consigliabile selezionare questa opzione in modo che il server non invii contenuti obsoleti.
- **Disattivazione del richiamo dei file da server remoti**. Selezionare questa opzione se non si desidera che il server richiami i file dai server remoti.
- **Non memorizzare nella cache file che scadranno entro**. Per evitare che i file memorizzati nella cache scadano in un periodo di tempo breve, specificare l'intervallo con questa opzione. Per impostazione predefinita, i file che scadono entro 10 minuti non vengono memorizzati nella cache.

Per configurare le impostazioni di scadenza predefinita modificando il file di configurazione del proxy, consultare le pagine di riferimento delle seguenti direttive:

- "CacheDefaultExpiry — Indica di specificare la scadenza predefinita dei file" a pagina 181
- "CacheExpiryCheck — Indica di specificare se il server restituisce file scaduti" a pagina 182
- "CacheTimeMargin — Indica di specificare la durata minima per la memorizzazione di un file nella cache" a pagina 188
- "CacheUnused — Indica di specificare per quanto tempo conservare nella cache i file non utilizzati" a pagina 189
- "CacheNoConnect — Indica di specificare la modalità cache autonoma" a pagina 186

Impostazioni del fattore Ultima modifica

Utilizzare il modulo **fattore Ultima modifica** per impostare il valore che il proxy utilizza per calcolare una data di scadenza per i file memorizzati nella cache senza data di scadenza nelle relative intestazioni. È possibile impostare diversi valori per i file che corrispondono alle diverse maschere di richiesta. La prima maschera corrispondente viene utilizzata per calcolare la data di scadenza.

Per impostare il fattore Ultima modifica cambiando direttamente il file di configurazione del proxy, vedere "CacheLastModifiedFactor — Indica di specificare il valore per determinare le date di scadenza" a pagina 183.

Limite di tempo cache

Utilizzare il modulo di configurazione **Limite di tempo dei file memorizzati nella cache** per impostare il tempo massimo in cui un file rimane nella cache. I limiti di tempo vengono impostati in base alle maschere di richiesta ed è possibile specificare che i file vengono scartati o riconvalidati quando scade il limite di tempo. Queste impostazioni possono essere utilizzate per conservare i file le cui date di scadenza non sono valide o i file con scadenze estremamente lunghe.

Per impostare il limite massimo di scadenza per i file memorizzati nella cache modificando il file di configurazione proxy, vedere quanto segue:

- "CacheMaxExpiry — Indica di specificare la durata massima per i file memorizzati nella cache" a pagina 185
- "CacheClean — Indica di specificare per quanto tempo conservare i file memorizzati nella cache" a pagina 181

Raccolta dati inutili

Per diffondere gli URL memorizzati nella cache e ridurre l'uso delle risorse di sistema, il Caching Proxy esegue il processo di pulitura noto come *raccolta dati inutili*, in cui vengono rimossi dalla cache i file vecchi o inutilizzati per fare spazio ai file più aggiornati.

Il processo di raccolta dati inutili esamina i file nella directory di cache e cerca di eliminare quelli scaduti per ridurre la dimensione della cache e fare spazio ai nuovi file. La raccolta dati inutili viene eseguita automaticamente, ma alcune impostazioni possono essere configurate in modo da adattare il processo alle esigenze dell'utente.

Configurazione della raccolta dati inutili

Per configurare la raccolta dati inutili, nei moduli Gestione e configurazione selezionare **Configurazione della cache –> Impostazioni dati inutili**. Utilizzare questo modulo per impostare un valore *limite massimo di occupazione* e un valore *limite minimo di occupazione*, che stabilisce quando la raccolta dati inutili viene avviata e arrestata. Quando la quantità di spazio nella cache raggiunge o supera la percentuale impostata per il valore di limite massimo di occupazione, viene avviata la raccolta dati inutili. La raccolta dati inutili continua fino a quando la percentuale dello spazio utilizzato nella cache è uguale o inferiore al valore di limite minimo di occupazione.

È possibile scegliere tra due algoritmi di raccolta dati inutili. L'algoritmo **tempo di risposta** ottimizza il tempo necessario per rispondere agli utenti rimuovendo dalla cache i file grandi. L'algoritmo **larghezza di banda** ottimizza l'uso della larghezza di banda della rete rimuovendo dalla cache i file più piccoli. Scegliere uno o entrambi.

Per configurare la raccolta dati inutili modificando il file di configurazione del proxy, vedere le sezioni di riferimento delle seguenti direttive:

- "Gc — Indica di specificare la raccolta di dati inutili" a pagina 210
- "GcHighWater — Indica di specificare l'inizio della raccolta di dati inutili" a pagina 211
- "GcLowWater — Indica di specificare la fine della raccolta di dati inutili" a pagina 211
- "CacheAlgorithm — Indica di specificare l'algoritmo cache" a pagina 180

Capitolo 20. Configurazione dell'agente cache per il precaricamento e l'aggiornamento automatici

La maggior parte dei server caching proxy memorizza un file solo in seguito alla richiesta dell'utente. Il Caching Proxy dispone di un agente cache che fornisce un precaricamento automatico della cache. L'agente cache richiama automaticamente gli URL specificati, gli URL più noti o entrambi e li posiziona nella cache prima che vengano richiesti.

In alcuni casi, è necessario impostare il nome host del server proxy e identificare il log di accesso del server prima che la cache venga precaricata. Per configurare l'agente cache nei moduli Gestione e configurazione, selezionare **Configurazione della cache** e utilizzare i moduli **Precaricamento cache** e **Aggiornamento cache**. I file che rappresentano i risultati di query (ovvero, i file i cui URL includono il punto interrogativo (?)) vengono memorizzati solo se è abilitata la memorizzazione nella cache di query.

L'aggiornamento e il precaricamento automatici della cache offrono i seguenti vantaggi:

- La memorizzazione nella cache viene applicata agli URL specificati prima che un utente richieda le pagine.
- La cache viene popolata prima che il server sia occupato con le attività dell'utente.
- È possibile ottenere più velocemente i file correnti dalla cache anziché recuperarli sulla prima richiesta.

Gli svantaggi comprendono:

- Il server proxy è occupato nella memorizzazione di pagine nella cache anche durante le ore di minore attività dell'utente.
- È necessario esercitare un po' di controllo su ciò che viene caricato automaticamente. Il caricamento di file collegati a pagine di alto livello, come gli indici Web e i siti di ricerca, possono generare richieste di un gran numero di pagine.

Per una maggiore efficienza, impostare l'agente cache in modo che sia in esecuzione quando le attività dell'utente sono ad un livello minimo e prima che il server sia occupato con le richieste dei client. A questo punto, i file nella cache sono pronti per fornire un servizio rapido non appena l'utente li richiede. Per impostazione predefinita, l'agente cache viene avviato ogni notte alle 3.00 ora locale.

Nota: Se l'agente cache è in esecuzione per aggiornare la cache, è necessario rimuovere i commenti della riga ″Proxy http:*″ nel file ibmproxy.conf. In caso contrario, nel log degli errori viene generato l'″Errore 403 vietato per effetto della regola″ e l'aggiornamento della cache non viene completato.

Impostazione del nome host del server

Sulle piattaforme Linux e UNIX, specificare il nome host del server proxy la cui cache è stata precaricata e aggiornata. Sulle piattaforme Windows, specificare il nome host solo se il server proxy aggiornato non si trova sulla macchina locale (notare che l'aggiornamento della cache di un server remoto in base ai file più utilizzati non è possibile perché l'agente cache locale non può accedere al log di accesso della cache del server remoto).

Per impostare un nome host del server proxy, nei moduli Gestione e configurazione, selezionare **Configurazione della cache –> Aggiornamento cache: identificazione del server di destinazione cache**.

Precaricamento della cache con file specifici

Per precaricare la cache con il contenuto memorizzato sugli URL specifici, nei moduli Gestione e configurazione utilizzare **Configurazione della cache –> Precaricamento cache**. In questo modulo, è possibile specificare gli URL dell'agente cache da caricare. Il proxy richiama quelle pagine quando l'agente cache viene avviato, senza considerare se erano già presenti nella cache (questi URL vengono specificati nel file di configurazione proxy dalla direttiva LoadURL). È possibile utilizzare questo modulo anche per definire gli URL il cui contenuto non è stato mai memorizzato nella cache. Per questo tipo di precaricamento della cache non è necessario accedere a un log di accesso della cache.

Utilizzare il modulo **Precaricamento cache** per configurare le seguenti opzioni:

- **Aggiornamento giornaliero della cache**—Selezionare questa casella di controllo se si desidera che l'agente cache aggiorni la cache ogni notte. Se non si desidera attivare l'agente cache, verificare che la casella non sia selezionata.
- **Ora di aggiornamento cache**—Se si desidera attivare l'agente cache ad un'ora diversa dalle 3.00 ora locale, specificare un'ora.
- **Contenuti cache**—Nel campo **Indirizzo IP o URL**, specificare gli URL da caricare. Per evitare che gli URL vengano caricati, specificarli e fare clic su **Ignora** nella casella **Stato cache**.

Precaricamento della cache con file memorizzati frequentemente nella cache

Per precaricare automaticamente le pagine più visitate, utilizzare il modulo **Configurazione cache –> Aggiorna cache**. Questa funzione richiede un Log di accesso cache per il server proxy. (La posizione e il nome del log di accesso possono essere modificati; fare riferimento a Parte 6, "Monitoraggio di Caching Proxy", a pagina 139 per informazioni). Gli URL più noti vengono determinati automaticamente dal log di accesso cache. L'amministratore può specificare anche il numero delle pagine note da precaricare nella cache. (Questo numero viene specificato nel file di configurazione del proxy dalla direttiva LoadTopCached).

Utilizzare il modulo **Aggiornamento cache** per configurare le seguenti opzioni:

- **Aggiornamento giornaliero della cache**—Selezionare questa casella di controllo se si desidera che l'agente cache aggiorni la cache ogni notte. Se non si desidera attivare l'agente cache, verificare che la casella non sia selezionata.
- **Ora di aggiornamento cache**—Se si desidera attivare l'agente cache ad un'ora diversa dalle 3.00, specificare ora e minuti diversi.

- **Identifica server di destinazione cache**—Utilizzare questa opzione se si desidera aggiornare un server diverso dalla macchina locale. (Non è possibile aggiornare un server remoto in base alla frequenza di accesso ai file specifici).
- **Memorizza nella cache gli URL più noti**—Specificare il numero di URL da memorizzare nella cache dal log di accesso della cache della notte precedente.
- **Carica pagine collegate**—Utilizzare questa impostazione per configurare la modalità di esplorazione (consultare la seguente sezione per informazioni sul tale modalità). Impostare il numero dei livelli da esplorare e se esplorare tutte le pagine (**always**), nessuna pagina (**never**), solo le pagine specificate dall'amministratore (**admin**), o solo le pagine più note (**topn**). Specificare anche se esplorare gli host, se aumentare l'intervallo tra le richieste e se memorizzare nella cache le immagini in linea.
- **Numero di thread**—Impostare il numero massimo di thread da utilizzare per aggiornare la cache.
- **Profondità massima della coda lavoro**—Impostare la coda massima per gli URL da richiedere.
- **Numero massimo di URL da richiedere**—Impostare il numero massimo di pagine da caricare. Questo numero viene controllato prima che inizi il richiamo delle pagine di esplorazione.
- **Tempo massimo**—Impostare per attivare l'agente cache. Se impostato su 0 ore e 0 minuti, l'agente non viene eseguito.

Esplorazione

La modalità di *Esplorazione* è una parte facoltativa della funzione di aggiornamento automatico della cache. La maggior parte delle pagine dispone di collegamenti con altre pagine e con le informazioni relative e molto spesso gli utenti seguono il percorso che collega una pagina all'altra e un sito a un altro. L'esplorazione è un modo per memorizzare nella cache questi percorsi logici di informazione. Nella modalità di esplorazione, l'agente cache segue un livello specifico di collegamenti ipertestuali (HTML) sulle pagine che sta caricando e memorizza anche quelle pagine collegate. Le pagine collegate possono risiedere sullo stesso host della pagina di origine o su altri host. Un'illustrazione è presente in Figura 1 a pagina 94.

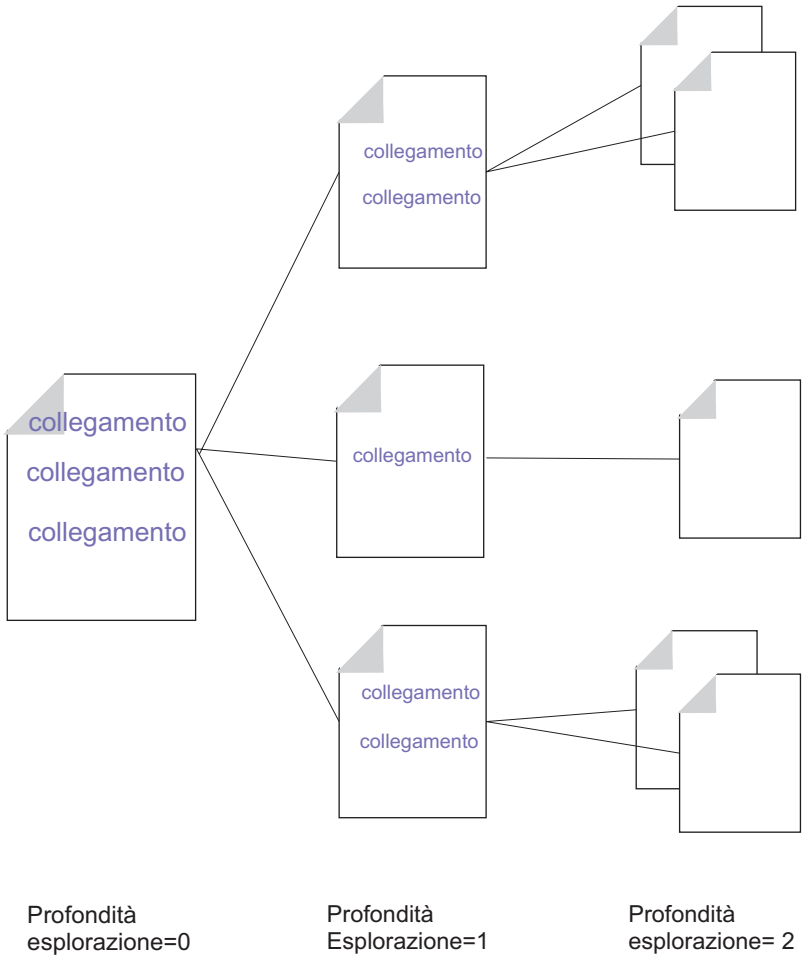

Figura 1. Esplorazione

Per controllare il processo di esplorazione, l'amministratore indica all'agente cache un numero massimo di URL che può caricare (l'impostazione predefinita è 2000), un periodo di tempo massimo in cui essere in esecuzione (l'impostazione predefinita è due ore) e un numero massimo di thread che può utilizzare (l'impostazione predefinita è quattro). L'amministratore può configurare anche altri controlli. Per impostazione predefinita, la modalità di esplorazione viene abilitata per due livelli di gerarchia e non è consentita sugli host. Inoltre, tra due richieste viene inserito un intervallo. Per modificare queste impostazioni, consultare "Direttive di file di configurazione proxy correlati" a pagina 95.

L'agente cache carica e aggiorna la cache in questo ordine:

1. Carica le pagine specifiche indicate dall'amministratore.
2. Carica le pagine note (quelle più visitate) dal log di accesso della cache.
3. Se a questo punto non viene raggiunto il numero massimo di pagine, ne vengono aggiunte altre tramite la modalità di esplorazione.

L'agente cache non controlla se è stato raggiunto il numero massimo di pagine fino a quando non comincia l'esplorazione tra i vari collegamenti. Se il valore del numero massimo di pagine (denominato MaxURLs nel file di configurazione proxy) è inferiore al numero di pagine richiamato nelle fasi 1 e 2, non viene richiamata nessuna pagina collegata.

I seguenti esempi mostrano come l'agente cache gestisce le priorità di aggiornamento della cache e l'esplorazione relative al numero massimo di URL indicato (si presume che la modalità di esplorazione sia configurata per tutti gli esempi).

Impostazione del file di configurazione	Risultato

`LoadURL http://www.getthis.com/main.html`
`LoadURL http://www.getmetoo.com/welcome.htm`
`LoadTopCached 30`
`MaxURLs 50`
	Se il log di accesso della cache ha più di 30 URL univoci, l'agente cache richiama main.html, welcome.htm e i primi 30 URL richiesti in base al log di accesso della cache. Poiché non ha raggiunto il valore MaxURLs, richiama e carica fino a 18 URL collegati dalle pagine già memorizzate.

`LoadURL http://ww.joesmith.edu/favorites.html`
`LoadURL http://www.janesmith.edu/dislikes.html`
`LoadTopCached 30`
`MaxURLs 25`
	Se il log di accesso della cache ha più di 30 URL univoci, l'agente cache richiama favorites.html, dislikes.html e i primi 30 URL richiesti dal log di accesso della cache. Nessun altro file viene richiamato in quanto è stato superato il valore in MaxURLs.

`LoadURL http://www.hello.com/hi.htm`
`LoadURL http://www.ballyhoo.com/index.html`
`LoadTopCached 20`
`MaxURLs 25`
	Se il log di accesso della cache ha più di 20 URL univoci, l'agente cache richiama hi.htm, index.html, i primi 20 URL richiesti dal log di accesso della cache e fino a 3 URL collegati dalle pagine precedenti. Nessun altro file viene richiamato in quanto è stato raggiunto il valore in MaxURLs.

Direttive di file di configurazione proxy correlati

L'agente cache può essere configurato direttamente modificando le direttive corrette nel file di configurazione proxy. Per le direttive del file di configurazione proxy relative all'agente cache, vedere le seguenti pagine di riferimento Appendice B, "Direttive del file di configurazione", a pagina 165:

- "AutoCacheRefresh — Indica di specificare se utilizzare o meno l'aggiornamento cache" a pagina 178
- "CacheAccessLog — Indica di specificare il percorso ai file di log accessi cache" a pagina 179
- "CacheRefreshTime — Indica di specificare quando avviare l'agente cache" a pagina 188
- "DelayPeriod — Indica di specificare un periodo di interruzione tra le richieste" a pagina 196
- "DelveAcrossHosts — Consente di specificare la memorizzazione nella cache tra domini" a pagina 196
- "DelveDepth — Indica di specificare fino a che punto seguire i collegamenti durante la memorizzazione nella cache" a pagina 196
- "DelveInto — Indica di specificare se l'agente cache deve seguire i collegamenti" a pagina 197
- "IgnoreURL — Indica di specificare gli URL non aggiornati" a pagina 215
- "LoadInlineImages — Indica di controllare l'aggiornamento di immagini incorporate" a pagina 221

- "LoadTopCached — Indica di specificare il numero delle pagine più utilizzate da aggiornare" a pagina 221
- "LoadURL — Indica di specificare gli URL da aggiornare" a pagina 222
- "MaxUrls — Indica di specificare il numero massimo di URL da aggiornare" a pagina 228

Avvio manuale dell'agente cache

Se è abilitato l'aggiornamento automatico della cache, l'agente cache esegue automaticamente un'operazione di aggiornamento nell'ora indicata. Tuttavia, l'agente cache può essere attivato in qualsiasi momento dalla riga comandi.

Il file eseguibile è il seguente:

- Sulle piattaforma Linux e UNIX: usr/sbin/cacheagt
- Sulle piattaforme Windows: *server_root*\bin\cacheagt.exe

  Dove *server_root* è l'unità e la directory in cui è installato il Caching Proxy (ad esempio, C:\Program Files\IBM\edge\cp).

Sulle piattaforme Linux e UNIX, è possibile eseguire automaticamente l'agente cache in vari momenti utilizzando il daemon **cron**. I lavori controllati da **cron** vengono specificati aggiungendo una riga al file di sistema crontab. Una voce di esempio del file di comando su Linux e UNIX è:

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

Questo esempio di comando avvia l'agente cache ogni giorno alle 16:45 ora locale. Si possono usare più voci per eseguire più di una volta l'agente cache, se si desidera. Per maggiori informazioni, consultare la documentazione del sistema operativo sul daemon **cron**.

Quando si utilizza un daemon **cron** per eseguire l'agente cache, disabilitare l'opzione di aggiornamento automatico usando il modulo di configurazione **Configurazione della cache –> Aggiornamento cache** o modificando il file di configurazione proxy. Altrimenti l'agente cache verrà eseguito più di una volta al giorno.

Capitolo 21. Utilizzo di una cache condivisa

È una condizione comune per un punto di presenza (POP, point of presence) del Web quella di disporre di più traffico di quanto un unico server sia in grado di gestire. Una soluzione è quella di aggiungere più server. Tuttavia, se si utilizzano più server caching proxy, il contenuto di una cache spesso si sovrappone ai contenuti delle altre cache. Oltre a una ridondanza inutile nella memoria, non è possibile ottenere il numero massimo di salvataggi della larghezza di banda perché un file memorizzato nella cache viene ricaricato dal server di origine quando una richiesta per tale file arriva a un server proxy che non ha il file nella propria memoria. Sebbene sia possibile ridurre la doppia memorizzazione nella cache tramite una catena gerarchica di server proxy, questo scenario determinerà ulteriore traffico su un particolare server e ogni collegamento in più nella catena aggiunge latenza.

La condivisione della cache risolve questi problemi permettendo a ciascuna cache di condividere i contenuti con le altre cache. I salvataggi della larghezza di banda vengono determinati dai seguenti fattori:

- Gli oggetti non vengono caricati più volte.
- Una cache logica combinata più grande fornisce un rapporto accessi maggiore.

Vengono forniti due metodi per utilizzare più cache come se fossero un'unica cache logica:

- RCA (Remote Cache Access) è una funzione del Caching Proxy che definisce una matrice di cache membro. Il file viene memorizzato in una di queste cache in base alla logica interna.
- Un plug-in di Caching Proxy viene fornito per consentire al server proxy di utilizzare ICP (Internet Caching Protocol). È possibile utilizzare il plug-in di ICP anziché di RCA se si desidera condividere i dati tra le macchine di Caching Proxy e le cache non Caching Proxy.

RCA e ICP possono essere utilizzati insieme.

RCA (Remote cache access)

Nella pianificazione di RCA, tenere presente quanto segue:

- I server proxy partecipanti devono essere vicini e connessi con collegamenti ad ampia larghezza di banda (ad esempio, FDDI, SP2 bus).
- L'appartenenza alla matrice RCA deve essere a lungo termine in modo che la configurazione sia il più possibile stabile.
- I server proxy devono avere funzionalità simili (ad esempio, CPU, dimensione di memoria e di cache).
- Le interruzioni di rete non devono essere frequenti.
- Il numero di membri di ciascuna matrice deve essere inferiore a 100.
- Tutti i membri della matrice devono utilizzare la stessa versione del software Caching Proxy.

Nota: Se i proxy nella matrice RCA utilizzano diversi sistemi operativi Linux (ad esempio, SUSE e Red Hat), verificare che l'utente ″nobody″ abbia lo

stesso UID su tutti i peer. Controllare le voci file di gruppo e password nella directory /etc/ su ogni computer e assegnare lo stesso UID a ″nobody.″

L'accesso alla cache remota non è corretto se una di queste condizioni non viene rispettata o se organizzazioni diverse gestiscono server diversi che sono membri della stessa matrice.

Configurazione di RCA (remote cache access)

Per configurare l'RCA (remote cache access), nei moduli Gestione e configurazione selezionare **Configurazione della cache –> RCA (Remote Cache Access)**. I campi di questo modulo definiscono una matrice denominata che condivide una cache logica. Inserire le informazioni richieste per ciascun membro della matrice.

Per configurare l'RCA (remote cache access) modificando il file di configurazione proxy, consultare le sezioni di riferimento in Appendice B, "Direttive del file di configurazione", a pagina 165 per le seguenti direttive:

- "ArrayName — Indica di denominare la matrice di cache remota" a pagina 177
- "Member — Indica di specificare un membro di una matrice" a pagina 228

Configurazione del plug-in ICP (Internet Caching Protocol)

Il plug-in di ICP (Internet Caching Protocol) consente al Caching Proxy di eseguire query sulle cache compatibili con ICP per cercare pagine HTML e altre risorse memorizzabili nella cache. Quando il server proxy riceve una richiesta HTTP, ricerca altre risorse per la cache. Se la risorsa non si trova nella cache locale e il plug-in di ICP è abilitato, il server proxy racchiude le richieste URL in un pacchetto di query ICP e distribuisce questo pacchetto a tutte le cache peer ICP identificate. Se una cache peer conferma di disporre della risorsa, il server proxy richiama la risorsa dalla cache del peer. Se due o più peer rispondono in modo positivo, viene elaborata la prima risposta. Se nessun peer risponde con degli accessi, il server originale continua l'elaborazione della richiesta in base al flusso di lavoro. Ad esempio, il server proxy può richiamare un altro plug-in, continuare con la routine RAC (Remote Caching Access), (se RCA è abilitato), oppure richiamare la risorsa richiesta.

Configurazione del plug-in di ICP

Il plug-in di ICP viene attivato e configurato modificando il file di configurazione proxy, ibmproxy.conf. È necessario aggiungere una direttiva ServerInit, una direttiva PreExit o entrambe alla sezione delle direttive API del file di configurazione per poter utilizzare il plug-in di ICP. Il tipo di direttiva utilizzato dipende dal ruolo che il Caching Proxy ha nel sistema ICP:

- Affinché il Caching Proxy funzioni come un server ICP, utilizzare la direttiva ServerInit per richiamare il modulo icpServer.
- Affinché il Caching Proxy funzioni come client ICP, utilizzare la direttiva PreExit per richiamare il modulo icpClient.
- Affinché il Caching Proxy funzioni come client ICP e server ICP, utilizzare entrambe le direttive.
- Utilizzare le direttive icpAddress, icpMaxThreads, icpPeer, icpPort e icpTimeout per configurare le impostazioni utilizzate dal plug-in.

Per creare queste direttive, modificare manualmente il file ibmproxy.conf, oppure, se il server proxy è già in esecuzione, collegarsi al modulo Gestione e configurazione **Configurazione server –> Elaborazione richiesta –> Elaborazione richiesta API**.

Le direttive prototipo (nel modulo dei commenti) sono state aggiunte alla sezione API del file ibmproxy.conf. Queste direttive API sono in un ordine stabilito. Se si aggiungono direttive API per abilitare nuove funzioni e moduli di plug-in, ordinare le direttive come illustrato nella sezione prototipi del file di configurazione. In alternativa, eliminare il commento o modificare se necessario le direttive API per includere il supporto per ogni funzione o plug-in desiderato.

Entrambe le direttive ServerInit e PreExit hanno due argomenti: (1) il percorso completo della libreria condivisa e (2) la chiamata di funzione. Questi argomenti sono delimitati da due punti (:). Il primo argomento è specifico del sistema e dipende dal punto in cui sono stati installati i componenti plug-in. Il secondo argomento è hard-coded nella libreria condivisa e deve essere digitato esattamente come illustrato.

Ogni direttiva deve comparire su un'unica riga nel file di configurazione proxy.

```
ServerInit
percorso_della_libreria_condivisa:icpServer
```

Esempio di Linux e UNIX:

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

Esempio di Windows:

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

```
PreExit
percorso_della_libreria_condivisa:icpClient
```

Esempio di Linux e UNIX:

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

Esempio di Windows:

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

Per configurare le impostazioni del plug-in, aggiungere o modificare le direttive ICP* fornite nel file di configurazione proxy. Per ulteriori informazioni, fare riferimento alle descrizioni delle seguenti direttive.

- "ICP_Address — Indica di specificare l'indirizzo IP per le query ICP" a pagina 213
- "ICP_MaxThreads — Indica di specificare il numero massimo di thread per le query ICP" a pagina 214
- "Occupier — Indica di specificare un membro di un cluster ICP" a pagina 214
- "ICP_Port — Indica di specificare il numero di porta per le query ICP" a pagina 215
- "ICP_Timeout — Indica di specificare il tempo massimo di attesa per le query ICP" a pagina 215
- "PreExit — Indica di personalizzare la fase PreExit" a pagina 239
- "ServerInit — Indica di personalizzare la fase Inizializzazione del server" a pagina 261

Capitolo 22. Memorizzazione nella cache di contenuto generato dinamicamente

La funzione di memorizzazione nella cache dinamica consente al Caching Proxy di memorizzare un contenuto generato dinamicamente nel modulo delle risposte delle JSP (JavaServer Pages) e dei servlet generati da un IBM WebSphere Application Server. Un modulo adattatore Caching Proxy viene utilizzato sul server delle applicazioni per modificare le risposte in modo da poterle memorizzare nella cache sul server proxy e nella cache dinamica del server delle applicazioni. Con questa funzione, è possibile memorizzare nella cache il contenuto generato dinamicamente sull'unità terminale della rete, esonerando gli host dei contenuti dal ripetere le richieste al server delle applicazioni quando più di un client richiede lo stesso contenuto.

Nota: La funzione di memorizzazione nella cache dinamica non consente al server proxy di memorizzare nella cache i risultati delle query URL. Per memorizzare i risultati delle query, configurare i filtri della memorizzazione nella cache, descritti in Capitolo 18, "Controllo degli elementi memorizzati nella cache", a pagina 81 e nella documentazione di riferimento delle direttive su "CacheQueries — Indica di specificare le risposte cache agli URL contenenti un carattere punto interrogativo (?)" a pagina 187. Possono essere memorizzati i risultati delle query provenienti dai server di origine che non sono IBM WebSphere Application Server.

A volte è necessario abilitare la memorizzazione nella cache di query affinché la funzione di memorizzazione dinamica funzioni; ad esempio, se i servlet utilizzano gli URL nel formato di query. Il server proxy considera qualsiasi URL contenente un punto interrogativo (?) come una query.

La memorizzazione nella cache di contenuti generati dinamicamente offre i seguenti vantaggi:

- Riduce il carico sugli host dei contenuti.
- Riduce il carico sui server delle applicazioni.
- Accelera la distribuzione delle risorse richieste agli utenti finali.
- Riduce l'uso della larghezza di banda tra i server.
- Aumenta la scalabilità dei siti Web che creano o forniscono contenuti generati dinamicamente.

Il server delle applicazioni esporta solo le pagine pubbliche composte per la memorizzazione nella cache del proxy. Le pagine private non vengono memorizzate dal proxy. Ad esempio, una pagina generata dinamicamente da un sito pubblico sulle previsioni del tempo, può essere esportata dal IBM WebSphere Application Server e memorizzata nella cache dal Caching Proxy. Tuttavia, una pagina generata dinamicamente, che elenca il contenuto del carrello d'acquisto di un utente, non può essere memorizzata nella cache dal server proxy. Inoltre, per poter generare in modo dinamico delle pagine, tutti i sottocomponenti di quella pagina devono poter essere memorizzati nella cache.

I file dinamici memorizzati nella cache non scadono come i file regolari; possono essere invalidati dal server delle applicazioni che li ha generati.

Le voci della cache dinamica vengono invalidate nelle seguenti circostanze:

- Il raccoglitore dati inutili della cache dinamica rimuove una voce a causa della congestione della cache.
- Il time-out, impostato nella voce servlet (servletcache.xml) o nella direttiva ExernalCacheManager del proxy, scade.
- Un agente esterno o un'applicazione richiamano le API della cache dinamica per invalidare le voci di cache.

L'invalidazione delle voci di cache dinamica viene eseguita generando un messaggio di invalidazione per l'istanza specifica del plug-in di memorizzazione nella cache dinamica del Caching Proxy. Il Caching Proxy riceve i messaggi di invalidazione per inviarli al localizzatore risorse /WES_External_Adapter. Il Caching Proxy elimina, quindi, dalla cache le voci non valide.

La memorizzazione nella cache dinamica richiede le seguenti fasi di configurazione.

- Configurazione di IBM WebSphere Application Server:
  - Configurare ogni server delle applicazioni per poter eseguire la memorizzazione nella cache dinamica locale.
  - Configurare ogni server delle applicazioni per poter utilizzare l'adattatore cache esterna.
  - Specificare quale cache esterna si può utilizzare per ogni file JSP e servlet memorizzabile nella cache.
- Configurazione di Caching Proxy:
  - Consentire al Caching Proxy di utilizzare il plug-in di memorizzazione nella cache dinamica.
  - Specificare le origini dalle quali il contenuto dinamico verrà memorizzato nella cache.

Configurazione del IBM WebSphere Application Server per la memorizzazione nella cache del proxy

Configurazione della memorizzazione nella cache dinamica sul server delle applicazioni

Seguire le istruzioni nella documentazione IBM WebSphere Application Server per configurare il server delle applicazioni all'uso della cache dinamica locale (chiamata anche cache di frammenti dinamica). La cache di frammenti dinamica interagisce con la cache esterna sul Caching Proxy di Application Server.

Configurazione dell'adattatore del server delle applicazioni

Il IBM WebSphere Application Server comunica con il Caching Proxy mediante un modulo software chiamato Adattatore cache esterna installato su Application Server.

Nota: Fare riferimento al sito Web di supporto del IBM WebSphere Application Server per la TechNote sulla configurazione della memorizzazione nella cache dinamica.

Configurazione del Caching Proxy per la memorizzazione nella cache dinamica

Per consentire al server proxy di memorizzare nella cache contenuti generati dinamicamente (risultati da servlet e JSP), è necessario effettuare due modifiche nel file di configurazione proxy, ibmproxy.conf. La prima modifica abilita il modulo plug-in per la memorizzazione dinamica; la seconda lo configura per riconoscere le origini dei contenuti dinamici memorizzabili nella cache.

Impostazione della direttiva Servizio per il plug-in di memorizzazione nella cache dinamica

Una direttiva API per l'operazione Servizio viene utilizzata per abilitare il plug-in di memorizzazione nella cache dinamica. Per creare questa direttiva, modificare manualmente il file ibmproxy.conf oppure, se il server proxy è già in esecuzione, utilizzare i moduli Gestione e configurazione per selezionare **Configurazione server –> Elaborazione richiesta –> Elaborazione richiesta API**. Il contenuto della direttiva viene illustrato negli esempi mostrati più avanti in questa sezione.

È presente una direttiva Servizio prototipo, per l'abilitazione della memorizzazione nella cache dinamica, come commento nella sezione API del file ibmproxy.conf. Ha l'intestazione `JSP Plug-in`. Le direttive API prototipo sono in un ordine stabilito. Se si aggiungono direttive API per abilitare nuove funzioni e moduli di plug-in, ordinare le direttive come illustrato nella sezione prototipi del file di configurazione. Facoltativamente, è possibile rimuovere i caratteri commento dalle direttive API prototipo e modificarli, se necessario, per includere un supporto per ciascuna funzione o plug-in desiderato.

Impostare la direttiva Servizio come illustrato nei seguenti esempi. (Ogni direttiva deve comparire su un'unica riga nel file di configurazione proxy; questi esempi a volte contengono delle interruzioni di riga per per facilitarne la lettura).

- Per AIX:

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

- Per Solaris:

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

- Per Linux:

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

- Per Windows:

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

Se il software Caching Proxy è installato in una directory diversa da quella predefinita, sostituire il percorso di installazione con il percorso di questi esempi.

Impostazione della direttiva ExternalCacheManager per la specifica delle origini dei file

Ogni Caching Proxy deve essere configurato per riconoscere l'origine dei file generati dinamicamente. Aggiungere una direttiva ExternalCacheManager al file ibmproxy.conf per ciascun server delle applicazioni che memorizza i contenuti generati dinamicamente su questo server proxy. Questa direttiva specifica un WebSphere Application Server che memorizza i risultati sul proxy e imposta un valore di scadenza massimo per i contenuti di quel server. Maggiori dettagli

vengono forniti in “ExternalCacheManager — Indica di configurare Caching Proxy per Dynamic Caching di IBM WebSphere Application Server” a pagina 207.

L’ID server, utilizzato nella direttiva ExternalCacheManager, deve corrispondere all’ID gruppo usato nella stanza gruppo di cache esterna del file dynacache.xml del server delle applicazioni.

Per il precedente esempio, aggiungere la seguente voce a ciascun file ibmproxy.conf del proxy.

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

Il Caching Proxy memorizza nella cache solo i contenuti di un IBM WebSphere Application Server il cui ID di gruppo corrisponde ad una voce ExternalCacheManager nel file ibmproxy.conf.

Capitolo 23. Ottimizzazione della cache del server proxy

Se la memorizzazione cache è abilitata, la velocità delle unità della memoria cache è molto importante per le prestazioni del Caching Proxy. In questa sezione vengono forniti dei suggerimenti sulla scelta di un tipo di memoria cache e sulla configurazione delle unità di memoria cache per migliorare le prestazioni.

Scelta del supporto per la memoria cache

Il Caching Proxy può utilizzare due diversi tipi di supporto per la memoria cache:

- Memoria
- Partizioni disco non formattate

Una cache di memoria consente un richiamo più veloce dei file, ma la dimensione di una memoria cache è limitata dalla quantità di memoria disponibile sulla macchina del server proxy. Una cache su disco, costituita da una o più partizioni disco non formattate, è più lenta di una cache di memoria ma, nella maggior parte dei casi, permette di disporre di dimensioni cache più grandi.

Ottimizzazione delle prestazioni della cache su disco

Le partizioni dell'unità utilizzata per la memorizzazione nella cache su disco, devono essere dedicate alla cache; vale a dire che non si possono utilizzare questi dischi fisici per contenere qualsiasi altro file system né per qualsiasi altro scopo diverso dalla memorizzazione nella cache del proxy. Inoltre, non è possibile utilizzare la compressione dati su un qualsiasi disco usato per la memorizzazione nella cache in quanto riduce le prestazioni.

Ogni unità di memoria cache (sia un disco che un file) è esposta a un sovraccarico di memoria sul server proxy. In generale, utilizzando un intero disco fisico su una sola unità cache, si ottengono le prestazioni migliori. L'uso di RAID o di altri meccanismi per associare più dischi fisici in un unico disco logico, può essere controproducente. Se si desidera utilizzare più dischi, specificarli come unità cache multiple mediante il modulo di configurazione **Impostazioni cache** o modificando la direttiva CacheDev nel file di configurazione proxy. Questo metodo consente al server proxy di controllare il parallelismo tra lettura e scrittura su più dischi e non si basa sulle prestazioni del sistema operativo o su un sottosistema del disco.

Raccolta dati inutili della cache

La raccolta dati inutili nella cache del server proxy elimina dalla cache i file scaduti, liberando spazio per le nuove richieste all'interno dei file di cache. La raccolta dati inutili viene attivata automaticamente quando la quantità di spazio utilizzato nella cache raggiunge il limite, specificato dall'amministratore, chiamato *limite massimo di occupazione* e continua fino a quando la quantità di spazio utilizzata non raggiunge un *limite minimo di occupazione*.

Poiché la routine di raccolta dati inutili utilizza il numero minimo di risorse CPU e non influisce sulla disponibilità del materiale scaduto all'interno della cache, non è necessario configurare l'esecuzione della raccolta dati inutili in orari stabiliti.

Per migliorare le prestazioni della raccolta dati inutili, impostare i limiti massimo e minimo di occupazione. È possibile, inoltre, configurare il tipo di algoritmo usato

per la raccolta dati inutili. Consultare “Raccolta dati inutili” a pagina 89 per maggiori informazioni sulla modifica della raccolta dati inutili.

Ottimizzazioni di piattaforme specifiche

Di seguito sono riportati dei suggerimenti per l'ottimizzazione delle prestazioni di cache su ogni piattaforma.

AIX

Creazione di un unico volume logico su un disco usando, preferibilmente, tutte le partizioni fisiche (PP) disponibili. Ad esempio, con un disco da 9 GB, creare un volume logico da 9 GB chiamato cpcache1. Formattarlo e specificarlo come unità cache del proxy utilizzando il suo volume logico non formattato, /dev/rcpcache1.

HP-UX e Solaris

Sull'unità cache, creare una partizione singola (o slice) che utilizza l'intera dimensione del disco. Ad esempio, su un disco da 9 GB, creare una partizione da 9 GB chiamata c1t3d0s0. Formattarla e specificarla come unità cache del proxy utilizzando l'unità non formattata, /dev/rdsk/c1t3d0s0.

Windows

Creare una sola partizione utilizzando l'intera dimensione del disco. Ad esempio, su un disco da 9 GB, creare una partizione da 9 GB chiamata i:. Formattarla e specificarla come unità cache del proxy utilizzando l'unità non formattata, \\.\i:.

Le informazioni sulla configurazione della cache del server proxy e sulla formattazione e specifica delle unità cache sono incluse in Parte 4, “Configurazione della cache di server proxy”, a pagina 71.

Parte 5. Configurazione della sicurezza di Caching Proxy

Questa sezione fornisce informazioni sulla sicurezza di base, l'utilizzo di SSL con Caching Proxy, l'abilitazione di hardware di crittografia e l'utilizzo del plugin di IBM Tivoli Access Manager (precedentemente detto Tivoli Policy Director) e del modulo di autorizzazione PAC-LDAP.

Di seguito vengono forniti i titoli di ciascun capitolo di questa sezione:

Capitolo 24. Informazioni sulla sicurezza del server proxy

Qualsiasi server accessibile da Internet può essere soggetto a intrusioni e il sistema su cui è in esecuzione può subire attacchi esterni. Persone non autorizzate potrebbero accedere al sistema, indovinare le password, aggiornare o eseguire i file, o anche leggere dati riservati. Parte dell'attrattiva del Web è la sua apertura. Tuttavia, si può fare un uso positivo del Web oppure abusarne.

Le seguenti sezioni descrivono come controllare gli utenti che hanno accesso ai file sul server del Caching Proxy.

Il Caching Proxy supporta le connessioni SSL (Secure Sockets Layer) in cui sono stabilite delle trasmissioni protette, incluse la codifica e la decodifica, tra il browser del client e il server di destinazione (un server dei contenuti o un server sostitutivo).

Se il Caching Proxy è configurato come sostitutivo, è in grado di stabilire delle connessioni protette con i client, con i server dei contenuti o con entrambi. Per abilitare le connessioni SSL, nei moduli Gestione e configurazione, selezionare **Configurazione proxy –> Impostazioni SSL**. Su questo modulo, selezionare la casella di controllo **Abilita SSL** e specificare un database del file di chiavi e un file password database del file di chiavi.

Si possono prendere diverse precauzioni di base per proteggere il sistema:

- Mettere a disposizione un server per l'accesso pubblico in una rete separata dalla rete interna o locale.
- Disattivare i programmi di utilità che consentono agli utenti remoti di accedere ai processi interni del server. In particolare, considerare la possibilità di disattivare i client **telnet**, **TN3270**, **rlogin** e **finger** sul sistema su cui è in esecuzione il server.
- Utilizzare il filtro o i firewall pacchetti.

  Il filtro pacchetti consente di definire la provenienza e la destinazione dei dati. È possibile configurare il sistema in modo da rifiutare alcune combinazioni origine-destinazione.

  Un firewall separa una rete interna da una rete accessibile pubblicamente, come ad esempio Internet. Il firewall è un insieme di computer o un unico computer che funziona da gateway in entrambe le direzioni, regolando e tracciando il traffico di passaggio. IBM Firewall è un esempio di software firewall.
- Script CGI di controllo. Utilizzando degli script CGI su un server Web si aumentano i rischi per la sicurezza in quanto è possibile che alcuni di questi script visualizzino delle variabili di ambiente che includono dati riservati, come gli ID utente e le password. È opportuno sapere esattamente il tipo di operazioni svolte da un programma CGI prima di eseguirlo sul server e controllare chi ha accesso agli script CGI.

Nota: Se si utilizza il Wizard di configurazione per configurare il server proxy, per abilitare SSL è necessario creare una regola di mappatura per le richieste proxy ricevute attraverso la porta 443. Per ulteriori informazioni, fare riferimento a "Definizione delle regole di mappatura" a pagina 41.

Esempi:

```
Proxy /* http://server contenuti:443
```

o

```
Proxy /* https://server contenuti:443
```

Capitolo 25. Impostazioni della protezione server

In questo capitolo viene illustrato il modo in cui proteggere i dati e i file del server utilizzando le impostazioni di protezione. Le impostazioni di protezione vengono attivate in base alla richiesta che il server riceve, in modo specifico in base alla directory, al file o al tipo di file particolare indicato dalla richiesta. In un'impostazione di protezione, le direttive secondarie controllano il modo in cui l'accesso viene garantito o negato in base alle caratteristiche delle directory o dei file protetti.

Utilizzo dei moduli Gestione e configurazione per impostare la protezione

Per definire un'impostazione di protezione e il modo in cui viene applicata, nei moduli Gestione e configurazione, selezionare **Configurazione server –> Protezione documenti**.Utilizzare questo modulo per le seguenti operazioni:

1. Impostare l'ordine di questa regola di protezione.

   Le regole di protezione vengono applicate nell'ordine in cui sono elencate nella tabella sul modulo di configurazione. Normalmente, queste vengono elencate a partire da quelle specifiche per arrivare a quelle generiche.

   Utilizzare il menu a discesa e i pulsanti per specificare la posizione di una regola di protezione.

2. Definire una maschera di richiesta.

   La protezione viene attivata in base alle maschere di richiesta che vengono confrontate con il contenuto delle richieste che i client inviano al server proxy.

   Una *richiesta* è la parte di un URL completo che segue il nome host del server. Ad esempio, se il server è denominato fine.feathers.com e un utente browser immette l'URL `http://fine.feathers.com/waterfowl/schedule.html`, il server riceve la richiesta /waterfowl/schedule.html. Le maschere di richiesta indicano i nomi di directory o di file, o entrambi, soggetti a protezione. Ad esempio, alcune richieste che attivano la protezione in base alla maschera di richiesta appena descritta (/waterfowl/schedule.html), includono /waterfowl/* e /*schedule.html.

   Immettere la maschera di richiesta nel campo **Maschera richiesta URL**.

3. Definire un'impostazione di protezione.

   Un'impostazione di protezione indica al Caching Proxy cosa fare con una richiesta che corrisponde ad una maschera di richiesta. È possibile utilizzare un'impostazione di protezione denominata o definire una nuova impostazione nel modulo **Protezione documenti**.

   Per utilizzare un'impostazione denominata, fare clic sul pulsante di opzione **Protezione denominata** e digitare il nome nel campo. Per definire una nuova impostazione, fare clic sul pulsante di opzione **In linea** e seguire le istruzioni (vedere il punto 6).

4. Scegliere un indirizzo richiedente (facoltativo).

   Diverse regole possono essere applicate a quelle richieste che derivano da indirizzi server diversi. Ad esempio, è possibile applicare una diversa impostazione di protezione alle richieste dei file di log se tali richieste provengono da indirizzi IP assegnati alla società.

Nota: Per visualizzare gli indirizzi dei richiedenti, è necessario abilitare la ricerca DNS. Vedere "DNS-Lookup — Indica di specificare se il server ricerca nomi host client" a pagina 201.

Se si desidera includere l'indirizzo del richiedente nella regola, inserirlo nel campo **Indirizzo IP server o nome host**.

5. Fare clic su **Inoltra**.

   Se è stata utilizzata un'impostazione di protezione denominata, non sono necessari ulteriori input. Se è stata selezionata un'impostazione di protezione in linea o è stata specificata un'impostazione denominata che non esiste, il sistema apre altri moduli.

6. Impostare i dettagli di protezione.

   Se non è stata specificata un'impostazione di protezione denominata già esistente, si apre un altro modulo sul quale è possibile specificare gli utenti che possono accedere ai documenti o alle directory che corrispondono alla maschera di richiesta e quali azioni possono eseguire tali utenti.

   - **Impostazioni di autenticazione password**—Specificare il file di password, il file di gruppo o entrambi da utilizzare per l'autenticazione utente. Specificare anche il nome utilizzato per identificare il server quando richiede il nome e la password del richiedente.

     Nota: Alcuni browser memorizzano nella cache gli ID utente e le password e li associano a un ID server. È opportuno utilizzare sempre lo stesso ID server con lo stesso file di password.

   - **Autorizzazioni**—Specificare quali utenti o gruppi sono autorizzati a leggere, scrivere o eliminare i file protetti.

7. Fare clic su **Inoltra**.
8. Riavviare il server.

Utilizzo delle direttive del file di configurazione per impostare la protezione

Per impostare la protezione modificando direttamente il file di configurazione di Caching Proxy, è necessario prima comprendere i seguenti problemi:

- Le differenze tra le direttive Protect, defProt e Protection
  - La direttiva Protect imposta la protezione collegando una maschera di richiesta ad un'impostazione di protezione. Per ulteriori informazioni, consultare "Protect — Indica di attivare un'impostazione di protezione predefinita per le richieste che corrispondono a una maschera" a pagina 240.
  - La direttiva defProt imposta un'impostazione di protezione predefinita per una particolare maschera di richiesta. Per ulteriori informazioni, consultare "DefProt — Indica di specificare un'impostazione di protezione predefinita per le richieste che corrispondono a una maschera" a pagina 193.
  - La direttiva Protection viene utilizzata per definire un'impostazione di protezione denominata. Per ulteriori informazioni, consultare "Protection — Indica di definire un'impostazione di protezione denominata nel file di configurazione" a pagina 244.
- Come la protezione interagisce con l'instradamento della richiesta

  Le direttive di instradamento della richiesta, come Map, Exec, Pass e Proxy, vengono utilizzate per controllare quali richieste accetta il server e come le reindirizza alle posizioni effettive del file. Le direttive di instradamento della richiesta utilizzano lo stesso tipo di maschere di richiesta delle direttive di protezione. Poiché vengono eseguite le direttive associate alla prima maschera

corrispondente di ciascuna richiesta, le direttive di protezione devono essere elencate prima di essere instradate nel file di configurazione affinché la protezione funzioni correttamente. Per ulteriori informazioni, vedere “Protect — Indica di attivare un’impostazione di protezione predefinita per le richieste che corrispondono a una maschera” a pagina 240.

- Differenza tra le impostazioni di protezione denominate e le impostazioni in linea

  La direttiva Protect può essere usata per specificare un’impostazione di protezione in linea o può indicare un’impostazione denominata esistente. La sintassi dei due tipi di istruzione è leggermente diversa. Per ulteriori informazioni, vedere “Protect — Indica di attivare un’impostazione di protezione predefinita per le richieste che corrispondono a una maschera” a pagina 240.

- Come scrivere un’impostazione di protezione

  Un’impostazione di protezione è costituita da una serie di istruzioni che utilizzano le direttive secondarie di protezione. Le informazioni sulla sintassi e quelle di riferimento relative alla scrittura delle impostazioni di protezione sono contenute in Appendice B, “Direttive del file di configurazione”, a pagina 165; consultare le seguenti sezioni di riferimento:

  – “Protect — Indica di attivare un’impostazione di protezione predefinita per le richieste che corrispondono a una maschera” a pagina 240
  – “Protection — Indica di definire un’impostazione di protezione denominata nel file di configurazione” a pagina 244
  – “Sottodirettive di protezione — Indica di specificare in che modo proteggere una serie di risorse” a pagina 245

Impostazioni di protezione predefinite

Il file di configurazione proxy predefinito include un’impostazione di protezione che richiede un ID amministratore e una password per poter accedere ai file nella directory /admin-bin/. Questa impostazione limita l’accesso ai moduli Gestione e configurazione.

Capitolo 26. SSL (Secure Sockets Layer)

SSL (Secure Sockets Layer) è un sistema che codifica automaticamente le informazioni prima di inviarle tramite Internet e le decodifica alla ricezione prima che vengano utilizzate. Protegge le informazioni riservate, come i numeri di carta di credito, quando vengono trasmesse via Internet.

Caching Proxy utilizza il sistema SSL per proteggere i server sostitutivi e per fornire un'amministrazione remota protetta come descritto nelle seguenti sessioni. L'SSL inoltre può essere utilizzato per proteggere le connessioni ai server di back-end (ad esempio, server delle applicazioni o dei contenuti) e per proteggere le comunicazioni tra il server proxy e i relativi client.

Sincronizzazione SSL

La protezione SSL viene avviata quando viene inviata una richiesta di connessione protetta da una macchina a un'altra—ad esempio, quando un browser invia una richiesta a un server proxy sostitutivo. La sintassi della richiesta https:// invece di http:// indica al browser di inviare la richiesta sulla porta 443, ossia la porta su cui è in ascolto il server per le richieste di connessione protetta (al posto della porta 80, per le richieste di ruotine). Per stabilire una sessione protetta tra il browser e il server, le due macchine eseguono uno scambio definito *sincronizzazione SSL* per accettare una specifica di cifratura e selezionare una chiave utilizzata per codificare e decodificare le informazioni. Le chiavi vengono generate automaticamente e scadono insieme alla sessione. Di seguito viene riportato uno scenario tipico (si suppone SSL Versione 3):

1. Client hello

   Il client avvia una sessione SSL con il Caching Proxy inviando un messaggio Client Hello che descrive le capacità di codifica del client.
2. Server hello

   Il server invia il certificato relativo al client e sceglie il pacchetto di crittografia da utilizzare per la codifica dei dati.
3. Client finish

   Il client invia le informazioni sulle chiavi di cifratura utilizzate per creare le chiavi di codifica simmetriche per i dati codificati. Questa documentazione relativa alle chiavi è nota come *premaster secret* ed è codificata con la chiave pubblica del server (ottenuta dal certificato del server; vedere "Gestione chiavi e certificati" a pagina 116). Sia il server che il client possono ricavare le chiavi di codifica simmetrica per la lettura e la scrittura da pre-master secret.
4. Server finish

   Il server invia una conferma finale e un MAC (Message Authentication Code) per l'intero protocollo di sincronizzazione.
5. Client validation

   Il client invia un messaggio per convalidare il messaggio Server finish.
6. Secure data flow

   Se il client convalida il messaggio Server finish, viene avviato il flusso di dati codificati.

Utilizzando Caching Proxy come endpoint per le connessioni protette, è possibile ridurre il carico sul server dei contenuti o delle applicazioni. Quando un Caching

Proxy mantiene una connessione protetta, esegue la codifica, la decodifica e la creazione della chiave, ossia tutte operazioni che occupano molta CPU. Il Caching Proxy, inoltre, consente di configurare i timeout delle sessioni SSL per massimizzare l'uso di ciascun chiave.

Limitazioni dell'SSL

Le seguenti limitazioni sono valide per l'SSL in WebSphere Application Server Caching Proxy:

- Il Caching Proxy stesso non può essere utilizzato come autorità di certificazione (vedere "Gestione chiavi e certificati").
- Alcuni browser potrebbero non supportare tutta la tecnologia di codifica utilizzata nel Caching Proxy.

Configurazione dell'amministrazione remota protetta

L'amministrazione remota del Caching Proxy si può ottenere utilizzando le funzioni di sicurezza fornite dall'SSL (Secure Sockets Layer) e l'autenticazione della password. Questo riduce in maniera significativa la possibilità di accesso al server proxy da parte di persone non autorizzate.

Per applicare l'SSL durante l'amministrazione remota del server, utilizzare una richiesta https:// invece di una richiesta http://, per aprire i moduli Gestione e configurazione. Ad esempio:

`https://nome.proprio.server/FrontPage.html`

Gestione chiavi e certificati

Come precedentemente osservato, prima di configurare l'SSL è necessario impostare un database di chiavi o creare un certificato. I certificati vengono utilizzati per autenticare le identità server. Utilizzare il programma di utilità IBM Key Management (a volte chiamato iKeyman) per impostare i file di certificazione. Questo programma di utilità fa parte del software GSKit, incluso nell'Application Server. GSKit, inoltre, comprende un'interfaccia grafica basata su Java per l'apertura dei file certificato.

Di seguito vengono riportate le fasi di base per impostare le chiavi SSL e i certificati.

1. Verificare che GSKit sia installato. Sulla maggior parte delle piattaforme, è installato automaticamente con il componente Caching Proxy. Il nome del pacchetto è gsk7ikm (gsk7ikm_gcc295 sui sistemi Linux per i386). GSKit, normalmente, viene installato nella directory ibm/gsk7/ (ibm/gskit/ sui sistemi AIX). Sulle piattaforme Windows, è possibile accedervi dal menu **Start**.

   Nota: in Windows, se GSKit non viene installato quando si utilizza InstallShield, verificare che il percorso della directory del supporto di installazione non contenga spazi.
2. Utilizzare il gestore chiavi per creare una chiave per le comunicazioni di rete protette e per ricevere un certificato da una relativa autorità. Nell'attesa del certificato dall'autorità, è possibile creare un'autocertificazione.
3. Creare un database di chiavi e specificare una password.

Nota: i file di chiave e keystash vengono disinstallati automaticamente ogni qualvolta viene disinstallato Caching Proxy. Per evitare di dover richiedere

un nuovo certificato all'autorità, salvare le copie di backup di questi due file in un'altra directory prima di disinstallare il software proxy.

Su tutti i sistemi operativi ad eccezione di Linux, se il certificato è scaduto, Caching Proxy non viene avviato correttamente e viene visualizzato un messaggio di errore che indica che il database di chiavi è scaduto. In Linux, il proxy sembra avviarsi ma il processo scompare rapidamente e non viene generato alcun messaggio di errore.

Autorità di certificazione

La chiave pubblica deve essere associata a un certificato con firma digitale da un'autorità di certificazione (CA) designata come CA root sicura sul server. È possibile acquistare un certificato firmato inoltrando una richiesta per un certificato al provider CA. Caching Proxy supporta le seguenti CA esterne:

- VeriSign
- Thawte

Per impostazione predefinita, le seguenti CA vengono designate come sicure:

- 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 (da VeriSign)
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA

Utilizzo del programma di utilità IBM Key Manager

Questa sezione offre un riferimento rapido per l'uso del programma di utilità IBM Key Manager (iKeyman). Utilizzare il gestore chiavi per creare il file database di chiavi SSL, la coppia di chiavi pubbliche-private e la richiesta di certificato. Dopo aver ricevuto il certificato firmato dalla CA, utilizzare il gestore chiavi per inserire il certificato nel database di chiavi in cui è stata creata la richiesta originale di certificato.

La documentazione più dettagliata dell'IBM Key Manager e GSKit viene fornita congiuntamente al software GSKit.

Impostazione del sistema per eseguire il gestore chiavi

Prima di avviare la GUI IKeyman, effettuare le seguenti operazioni:

1. Installare Java 2 Technology, versione 1.4.2 da 32 bit IBM o equivalente
2. Impostare JAVA_HOME sulla directory Java. Ad esempio:
   - Windows: `set JAVA_HOME=C:\Program Files\IBM\Java142`
   - Linux e UNIX: `export JAVA_HOME=/usr/opt/IBMJava2-142`
3. Rimuovere ibmjsse.jar e gskikm.jar (se presenti) e i file ibmjcaprovider.jar dalla directory JAVA_HOME/jre/lib/ext.

   Nota: in Sun, sostituire la directory JAVA_HOME/jre/lib/ext con la directory JAVA_HOME/lib/ext/.
4. Tutti i seguenti file jar si trovano in *GSKit_Installation_path*/classes/jre/lib/ext/.
   - Copiare i file jar specificati in JAVA_HOME/jre/lib/

     ```
     ibmjcefw.jar
     ibmpkcs11.jar
     ```
   - Copiare i file jar specificati in JAVA_HOME/jre/lib/ext

     ```
     ibmjceprovider.jar
     ibmpkcs.jar
     ```
   - Copiare i file jar specificati in JAVA_HOME/jre/lib/security

     ```
     local_policy.jar
     US_export_policy.jar
     ```
5. Registrare i provider di servizi IBM JCE, IBM CMS e/o IBMJCEFIPS:

   Aggiornare il file JAVA_HOME/jre/lib/security/java.security per aggiungere i provider IBM CMS successivamente al provider Sun. Ad esempio:

   ```
   security.provider.1=sun.security.provider.Sun
   security.provider.2=com.ibm.spi.IBMCMSProvider
   security.provider.3=com.ibm.crypto.provider.IBMJCE
   ```

   Un file di esempio java.security è disponibile in *GSKit_Installation_path*/classes/gsk_java.security.
   - Per abilitare l'operazione FIPS, aggiornare il file JAVA_HOME/jre/lib/security/java.security per aggiungere anche IBMJCEFIPS successivamente al provider Sun. Verificare che il provider IBMJCEFIPS sia stato registrato con una priorità superiore a IBMJCE. Ad esempio:

     ```
     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. (Facoltativo) In caso di utenti JSSE che utilizzano JSSE per accedere all'hardware crittografico, installare ibmpkcs11.jar nella directory JAVA_HOME/jre/lib e seguire le istruzioni presenti in *GSKit_Installation_path*/classes/native/native-support.zip per impostare le librerie condivise dell'hardware crittografico.

   Nota: è disponibile inoltre il file ibmpkcs11.jar nel pacchetto JSSE rilasciato dopo il 5 agosto, 2002. Per registrare un provider di servizi IBMPKCS11, viene riportato di seguito un esempio per l'aggiornamento del file 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
   ```

Avvio del gestore chiavi

Avviare l'interfaccia utente grafica (GUI) del gestore chiavi, come segue:

- Sulle piattaforme Linux e UNIX, inserire `gsk7ikm` su un prompt dei comandi.
- Sulle piattaforme Windows, fare clic su **Start –> Programmi –> IBM WebSphere –> Edge Components –> Caching Proxy –> Avvia programma di utilità gestione chiavi.**

Notare che se durante questa sessione viene creato un file database di chiavi, il file viene memorizzato nella directory da cui è stato avviato il gestore chiavi.

Creazione di un nuovo database di chiavi, password e file stash

Un database di chiavi è un file che il server utilizza per memorizzare una o più coppie di chiavi e certificati. È possibile utilizzare un database di chiavi per tutte le coppie di chiavi e per tutti i certificati, oppure è possibile creare più database. Il programma di utilità di gestione chiavi viene utilizzato per creare nuovi database di chiavi e per specificare le relative password e file stash.

Per creare un database di chiavi e un file stash:

1. Avviare il programma di utilità di gestione chiavi.
2. Dal menu principale, selezionare **File database di chiavi –> Nuovo**.
3. Nella finestra di dialogo **Nuovo**, verificare che sia selezionato il tipo di file **File database di chiavi CMS**. Digitare il nome del database di chiavi e la posizione del file oppure accettare l'impostazione predefinita, **key.kdb**. Fare clic su **OK**.
4. Nella finestra di dialogo **Richiesta password**, digitare e confermare la password per questo database. Fare clic su **OK**.
5. Selezionare la casella di controllo per eseguire lo stash del file password. Se richiesto, digitare e confermare una password per la verifica. Viene visualizzato il seguente messaggio: `Tipo-DB: File database di chiavi CMS` *`nome_database_filechiavi`*

   Nota: se non viene eseguito lo stash del file password, il server viene avviato ma non è in ascolto sulla porta 443.

La password specificata quando viene creato un nuovo database di chiavi protegge la chiave privata, ossia l'unica che dispone dell'autorizzazione necessaria per firmare i documenti o decodificare i messaggi codificati con la chiave pubblica.

Per specificare la password, utilizzare le seguenti istruzioni:

- La password deve essere costituita dalla serie di caratteri in inglese USA.
- La password deve contenere almeno sei caratteri e almeno due numeri non consecutivi. Verificare che password non sia composta da informazioni personali che si possono ottenere pubblicamente, come il nome, il cognome, le iniziali o la data di nascita.
- Eseguire lo stash della password.

Si consiglia di modificare la password del database di chiavi frequentemente. Tuttavia, se viene specificata una data di scadenza per la password, annotarla. Se la password scade prima che venga modificata, viene scritto un messaggio sul log degli errori e il server viene avviato ma le connessioni di rete non saranno protette.

Per modificare la password database di chiavi, seguire le fasi riportate sotto:

1. Dal menu principale, fare clic su **File database di chiavi –> Apri**.
2. Nella finestra di dialogo **Apri**, digitare il nome del database di chiavi o accettare l'impostazione predefinita, **key.kdb**. Fare clic su **OK**.

3. Nella finestra di dialogo **Richiesta password**, digitare la password stabilita e fare clic su **OK**.
4. Dal menu principale, fare clic su **File database di chiavi –> Modifica password**.
5. Nella finestra di dialogo **Modifica password**, digitare e confermare una nuova password. Fare clic su **OK**.

Per una connessione SSL tra un proxy e un server LDAP, collocare la password del database delle chiavi nel file pac_keyring.pwd. (Notare che il file pac_keyring.pwd non è un file stash generato da IKeyMan.)

Creazione di una nuova coppia di chiavi e della richiesta di certificato

Il database di chiavi memorizza le coppie di chiavi e le richieste di certificati. Per creare una coppia di chiavi pubbliche-private e una richiesta di certificato, seguire le fasi riportate sotto:

1. Se non è stato creato un database di chiavi, seguire le istruzioni riportate in "Creazione di un nuovo database di chiavi, password e file stash" a pagina 119.
2. Dal menu principale del programma di utilità di gestione chiavi, fare clic su **Database di chiavi –> File –> Apri**.
3. Nella finestra di dialogo **Apri**, digitare il nome del database di chiavi (oppure fare clic su **key.kdb**, se si sta utilizzando l'impostazione predefinita). Fare clic su **OK**.
4. Nella finestra di dialogo **Richiesta password**, digitare la password e fare clic su **OK**.
5. Dal menu principale, fare clic su **Crea –> Nuova richiesta certificato**.
6. Nella finestra di dialogo **Nuova chiave e richiesta certificato**, specificare quanto segue:
   - **Etichetta chiave:** digitare il nome (etichetta) utilizzato per identificare il certificato nel database: ad esempio, `autocertificazione dell'utente` o `www.companyA.com`.
   - **Dimensione chiave:** la dimensione della chiave, ad esempio `1024`. (Per poter usufruire della codifica a 128 bit, si consiglia una dimensione chiave di 1024.)
   - **Nome azienda:** il nome dell'azienda da associare alla chiave, ad esempio `Company A`.
   - **Unità organizzativa** (facoltativa)
   - **Località** (facoltativa)
   - **Stato/Provincia** (facoltativa)
   - **CAP** (facoltativo)
   - **Nazione:** il codice nazione. È necessario specificare almeno due caratteri, ad esempio `US`.
   - **Nome file richiesta certificato:** un nome per il file di richiesta. Facoltativamente, è possibile utilizzare un nome predefinito.
7. Fare clic su **OK**. Viene visualizzato un messaggio di conferma:

   `Una nuova richiesta di certificato è stata creata con esito positivo nel file` *`nome_database_filechiavi`*`.`
8. Fare clic su **OK**. Il nome dell'etichetta inserito deve essere visualizzato nell'intestazione **Richieste certificati personali**.

9. Nella finestra di dialogo **Informazioni**, fare clic su **OK**. Viene ricordato di inviare il file a un'autorità di certificazione.
10. A meno che non sia stata creata un'autocertificazione (consultare la sezione seguente, "Creazione di un'autocertificazione," per maggiori dettagli), inviare la richiesta di certificato a una CA:
    - Lasciare il gestore chiavi in esecuzione.
    - Avviare un browser Web ed inserire l'URL della CA da cui si desidera ottenere il certificato.
    - Seguire le istruzioni fornite dalla CA per inviare la richiesta di certificato.

    Le richieste di certificato possono impiegare tra due e tre settimane per essere soddisfatte. Mentre si attende che la CA elabori la richiesta di certificato, è possibile agire da CA e utilizzare iKeyman per creare l'autocertificazione per abilitare le sessioni SSL tra i client e il server Caching Proxy.

Creazione di un'autocertificazione

Utilizzare il programma di utilità di gestione chiavi per creare un'autocertificazione per abilitare le sessioni SSL tra i client e il server proxy durante l'attesa di un certificato. L'autocertificazione è utile per effettuare le prove.

Per creare un'autocertificazione, seguire la procedura riportata sotto:

1. Se non è stato creato un database di chiavi, seguire le istruzioni riportate in "Creazione di un nuovo database di chiavi, password e file stash" a pagina 119.
2. Dal menu principale del programma di utilità di gestione chiavi, fare clic su **Database di chiavi –> File –> Apri**.
3. Nella finestra di dialogo **Apri**, digitare il nome del database di chiavi (o accettare l'impostazione predefinita, **key.kdb**). Fare clic su **OK**.
4. Nella finestra di dialogo **Richiesta password**, digitare la password e fare clic su **OK**.
5. Nel frame dei contenuti **Database di chiavi**, selezionare **Certificati personali** e fare clic su **Crea nuova autocertificazione**.
6. Nella finestra **Crea nuova autocertificazione**, specificare quanto segue:
    - **Etichetta chiave:** un nome (etichetta) utilizzato per identificare la chiave e il certificato nel database: ad esempio `autocertificazione dell'utente`
    - **Dimensione chiave:** la dimensione della chiave, ad esempio `512`.
    - **Nome comune:** il nome host completo del server, ad esempio `www.myserver.com`
    - **Nome azienda:** il nome dell'azienda da associare alla chiave, ad esempio `Company A`.
    - **Unità organizzativa** (facoltativa)
    - **Località** (facoltativa)
    - **Stato/Provincia** (facoltativa)
    - **CAP** (facoltativo)
    - **Nazione:** il codice nazione. È necessario specificare almeno due caratteri, ad esempio US.
    - **Periodo di validità:** il periodo di tempo durante il quale è valido il certificato.
7. Fare clic su **OK**.

8. Registrare il database di chiavi con il server aggiungendo il file di chiavi e il file stash alle impostazioni di configurazione (vedere "Creazione di un nuovo database di chiavi, password e file stash" a pagina 119).

Esportazione di chiavi

Utilizzare questa procedura per esportare le chiavi in un altro database di chiavi:

1. Avviare il programma di utilità di gestione chiavi.
2. Dal menu principale, fare clic su **File database di chiavi –> Apri** .
3. Nella finestra di dialogo **Apri**, digitare il nome del database di chiavi (o accettare l'impostazione predefinita, **key.kdb**). Fare clic su **OK**.
4. Nella finestra di dialogo **Richiesta password**, digitare la password e fare clic su **OK**.
5. Nel frame dei contenuti **Database di chiavi**, selezionare **Certificati personali** e fare clic sul pulsante **Esporta/Importa** nell'etichetta.
6. Nella finestra **Esporta/Importa chiave**:
   - Selezionare **Esporta chiave**.
   - Selezionare il tipo di database di destinazione (ad esempio, **PKCS12**).
   - Digitare il nome file oppure fare clic su **Sfoglia** per selezionarlo.
   - Digitare la posizione corretta.
7. Fare clic su **OK**.
8. Nella finestra di dialogo **Richiesta password**, digitare la password corretta e digitarla nuovamente per confermarla, quindi fare clic su **OK** per esportare la chiave selezionata in un altro database.

Importazione di chiavi

Per importare le chiavi da un altro database di chiavi:

1. Avviare il programma di utilità di gestione chiavi.
2. Dal menu principale, selezionare **File database di chiavi –> Apri** .
3. Nella finestra di dialogo **Apri**, digitare il nome del database di chiavi (o accettare l'impostazione predefinita, **key.kdb**). Fare clic su **OK**.
4. Nella finestra di dialogo **Richiesta password**, digitare la password corretta e fare clic su **OK**.
5. Nel frame dei contenuti **Database di chiavi**, selezionare **Certificati personali** e fare clic sul pulsante **Esporta/Importa** nell'etichetta.
6. Nella finestra **Esporta/Importa chiave**:
   - Selezionare **Importa chiave**.
   - Selezionare il tipo di file database di chiavi (ad esempio, **PKCS12**).
   - Digitare il nome file oppure fare clic su **Sfoglia** per selezionarlo.
   - Selezionare la posizione corretta.
7. Fare clic su **OK**.
8. Nella finestra di dialogo **Richiesta password**, digitare la password corretta e fare clic su **OK**.
9. Nell'elenco **Seleziona da etichetta chiave**, selezionare il nome etichetta corretto e fare clic su **OK**.

Elenco autorità di certificazione

Per visualizzare un elenco di autorità di certificazione (CA) sicure in un database di chiavi:

1. Avviare il programma di utilità di gestione chiavi.
2. Dal menu principale, fare clic su **File database di chiavi –> Apri** .
3. Nella finestra di dialogo **Apri**, digitare il nome del database di chiavi (o accettare l'impostazione predefinita, **key.kdb**). Fare clic su **OK**.
4. Nella finestra di dialogo **Richiesta password**, digitare la password corretta e fare clic su **OK**.
5. Nel frame dei contenuti **Database di chiavi**, selezionare **Certificati firmatario**.
6. Fare clic su **Certificati firmatario**, **Certificati personali**, o **Richieste certificati** per visualizzare l'elenco di CA presenti nella finestra **Informazioni chiave**.

Ricezione di un certificato CA

Utilizzare questa procedura per ricevere un certificato inviato tramite posta elettronica da un'autorità di certificazione (CA) designata come CA sicura per impostazione predefinita (vedere l'elenco riportato in "Autorità di certificazione" a pagina 117). Se la CA che ha emesso il certificato non è una CA sicura nel database di chiavi, è necessario prima memorizzare il certificato della CA e definire questa CA come sicura. Successivamente, è possibile ricevere il certificato firmato dalla CA nel database. Non è possibile ricevere un certificato firmato da una CA che non è definita come sicura (vedere "Memorizzazione di un certificato CA").

per ricevere un certificato firmato da CA in un database di chiavi:

1. Avviare il programma di utilità di gestione chiavi.
2. Dal menu principale, selezionare **File database di chiavi –> Apri** .
3. Nella finestra di dialogo **Apri**, digitare il nome del database di chiavi (o accettare l'impostazione predefinita, **key.kdb**). Fare clic su **OK**.
4. Nella finestra di dialogo **Richiesta password**, digitare la password e fare clic su **OK**.
5. Verificare che il nome file nell'elenco **Tipo-DB** sia corretto.
6. Nella finestra **Database di chiavi**, selezionare **Certificati personali**, quindi fare clic su **Ricevi**.
7. Nella finestra di dialogo **Ricevi certificato da un file**, digitare il nome di un file di base codificato a 64 bit di base nel campo di testo **Nome file certificato**. Fare clic su **OK**.
8. Per chiudere il programma di utilità gestore chiavi, dal menu principale, fare clic su **File database di chiavi –> Esci**.

Memorizzazione di un certificato CA

Solo i certificati firmati dalle CA sicure vengono accettate per stabilire connessioni protette. Per aggiungere una CA all'elenco di autorità sicure, è necessario ottenere e memorizzare il relativo certificato come sicuro. Seguire questa procedura per memorizzare un certificato da una nuova CA, prima di riceverla nel database:

1. Avviare il programma di utilità di gestione chiavi.
2. Dal menu principale, fare clic su **File database di chiavi –> Apri** .
3. Nella finestra di dialogo **Apri**, digitare il nome del database di chiavi (o accettare l'impostazione predefinita, **key.kdb**). Fare clic su **OK**.
4. Nella finestra di dialogo **Richiesta password**, digitare la password e fare clic su **OK**.

5. Nel frame dei contenuti **Database di chiavi**, selezionare **Certificati firmatario** e fare clic su **Aggiungi**.
6. Nella finestra di dialogo **Aggiungi certificato CA da un file**, selezionare il nome del file certificato di dati ASCII codificato a 64 bit di base oppure utilizzare l'opzione **Sfoglia**. Fare clic su **OK**.
7. Nella finestra di dialogo **Etichetta**, digitare il nome etichetta e fare clic su **OK**.
8. Utilizzare la casella di controllo per designare il certificato come sicuro (predefinito).

   Nota: Visualizzare la casella di controllo *dopo* aver creato il certificato utilizzando il pulsante "Visualizza/Modifica". La casella di controllo viene elencata sul pannello ma non viene visualizzata durante l'aggiunta del certificato.

Visualizzazione della chiave predefinita in un database di chiavi

Visualizzare la voce chiave predefinita come segue:

1. Avviare il programma di utilità di gestione chiavi.
2. Dal menu principale, fare clic su **File database di chiavi –> Apri** .
3. Nella finestra di dialogo **Apri**, digitare il nome del database di chiavi (o accettare l'impostazione predefinita, **key.kdb**). Fare clic su **OK**.
4. Nella finestra di dialogo **Richiesta password**, digitare la password e fare clic su **OK**.
5. Nel frame dei contenuti **Database di chiavi**, selezionare **Certificati personali**, quindi il nome etichetta certificato CA.
6. Nella finestra **Informazioni chiave**, fare clic su **Visualizza/Modifica** per visualizzare le informazioni sulla chiave predefinita del certificato.

Specifiche di cifratura supportate

Gli algoritmi di codifica e i caratteri hash per le versioni SSL 2 e 3, sono elencati nelle tabelle seguenti.

Creazione coppie di chiavi: dimensioni chiave privata RSA 512–1024

SSL Versione 2

Versione USA	Versione esportazione
RC4 US	RC4 Export
RC2 US	RC2 Export
DES 56-bit	*non applicabile*
Triple DES US	*non applicabile*
RC4 Export	*non applicabile*
RC2 Export	*non applicabile*

SSL Versione 3

Versione USA	Versione esportazione
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-bit	*non applicabile*
DES CBC SHA	*non applicabile*
NULL SHA	*non applicabile*
NULL MD5	*non applicabile*
NULL NULL	*non applicabile*

Queste specifiche SSL possono essere anche configurate modificando direttamente il file di configurazione proxy. Per i dettagli, consultare le sezioni di riferimento in Appendice B, "Direttive del file di configurazione", a pagina 165 per le seguenti direttive:

- "V2CipherSpecs — Indica di elencare le specifiche di codifica supportate per SSL versione 2" a pagina 272
- "V3CipherSpecs — Indica di elencare le specifiche di codifica supportate per SSL versione 3" a pagina 272
- "FIPSEnable — Indica di abilitare la crittografia approvata FIPS (Federal Information Processing Standard) per SSLV3 e TLS" a pagina 208

Codifica a 128 bit per Caching Proxy

Attualmente viene distribuita solo la versione di codifica a 128 bit del Caching Proxy. La versione a 56 bit non è più disponibile. Se si sta installando una versione precedente, è possibile installare Caching Proxy direttamente sulla versione attuale a 128 bit o 56 bit. Se precedentemente si utilizzava un browser (esportazione) a 56 bit, è necessario effettuare l'aggiornamento a un browser a 128 bit per poter usufruire della codifica a 128 bit nel proxy.

Dopo un aggiornamento da una versione a 56 bit del Caching Proxy alla versione a 128 bit, se le dimensioni della chiave utilizzata per codificare i certificati sono impostate su 1024, non è necessaria alcuna modifica di configurazione. Tuttavia, se sono impostate su 512, per usufruire della codifica a 128 bit del proxy, è necessario creare nuovi certificati con dimensioni 1024. Creare le nuove chiavi utilizzando il programma di utilità IBM Key Manager (iKeyman).

1. Avviare il gestore chiavi.
   - Sulle piattaforme Linux e UNIX, inserire `gsk7ikm` su un prompt dei comandi.
   - Sui sistemi Windows, fare clic su **Start –> Programmi –> IBM WebSphere –> Edge Components –> Avvia programma di utilità gestione chiavi.**
2. Dal menu principale, fare clic su **File database di chiavi –> Apri** .
3. Nella finestra di dialogo **Apri**, digitare il nome del database di chiavi (oppure fare clic su **key.kdb**, se si sta utilizzando l'impostazione predefinita) e fare clic su **OK**.
4. Se si apre la finestra **Richiesta password**, digitare la password e fare clic su **OK**.
5. Dal menu principale, fare clic su **Crea –> Nuova richiesta certificato**.
6. Nella finestra **Nuova chiave e richiesta certificato**, specificare quanto segue:

- **Etichetta chiave**: digitare un nome utilizzato per identificare la chiave e il certificato nel database.
- **Dimensione chiave**: selezionare **1024**.
- **Nome azienda**: digitare il nome dell'azienda a cui associare la chiave.
- **Nazione:** digitare il codice nazione. È necessario specificare almeno due caratteri, ad esempio US.
- **Nome file richiesta certificato:** digitare un nome per il file di richiesta, oppure facoltativamente, utilizzare un nome predefinito.

7. Fare clic su **OK**.

Vedere "Gestione chiavi e certificati" a pagina 116 per un'analisi dettagliata del programma di utilità IBM Key Manager.

Notare che questa versione del prodotto non supporta la codifica su SUSE Linux.

Capitolo 27. Abilitazione del supporto hardware crittografico

Seguire questa procedura per consentire che la routine di sincronizzazione SSL venga scaricata su una scheda di hardware crittografico:

1. Installare la scheda di hardware crittografico in base alle istruzioni del produttore.
2. Abilitare SSL al caching proxy. Per ulteriori informazioni, fare riferimento a Capitolo 26, “SSL (Secure Sockets Layer)”, a pagina 115.
3. Modificare manualmente la direttiva SSLCryptoCard nel file di configurazione ibmproxy.conf. Nei moduli Gestione e configurazione non è presente alcuna voce per questa direttiva. Per maggiori informazioni, consultare il riferimento alla direttiva SSLCryptoCard “SSLCryptoCard — Indica di specificare la scheda crittografica installata” a pagina 265.

Capitolo 28. Utilizzo del plug-in di Tivoli Access Manager

Un plug-in di Caching Proxy viene fornito insieme a Tivoli Access Manager (in precedenza Tivoli Policy Director) che consente al Caching Proxy di utilizzare Access Manager per l'autenticazione e l'autorizzazione. Questo plug-in consente, a un'azienda che utilizza Access Manager per il controllo degli accessi al Web, di aggiungere la tecnologia Edge senza dover raddoppiare il lavoro, impostando degli schemi di autorizzazione separati per il server proxy.

Per maggiori informazioni su Tivoli Access Manager, visualizzare il sito Web del prodotto all'indirizzo http://www.ibm.com/software/tivoli/products/. Per informazioni sui requisiti software e hardware e sull'installazione del plug-in di Access Manager, fare riferimento alla documentazione fornita con Tivoli Access Manager.

Nota: Il plug-in di Tivoli Access Manager potrebbe non essere supportato su Linux Red Hat. Contattare Tivoli per le informazioni di supporto correnti sulle piattaforme Linux.

Configurazione

Insieme al plug-in di Access Manager viene fornito uno script di configurazione per il Caching Proxy.

Operazioni da eseguire prima di utilizzare lo script di configurazione

Prima di eseguire lo script, effettuare quanto segue:

- Installare tutto il software necessario.
- Verificare che il server proxy sia impostato per utilizzare la porta 80 (Questo è il valore predefinito).
- Configurare i componenti LDAP e Access Manager e verificare che siano in esecuzione durante la configurazione del plug-in di Access Manager.
- Verificare di avere a disposizione l'ID amministratore di Access Manager e il nome dell'amministratore LDAP. Questi valori sono necessari per impostare il server proxy.

Utilizzo dello script di configurazione

Lo script di configurazione è denominato **wslconfig.sh** e viene fornito nella directory /opt/pdweb-lite/bin/. Inserire l'ID amministratore di Access Manager e il nome dell'amministratore LDAP se richiesti.

Lo script di configurazione esegue automaticamente le seguenti operazioni:

- Imposta l'ID utente di Caching Proxy su `root` e l'ID gruppo su `altro`
- Imposta la direttiva noLog su `*`, in questo modo non viene scritta nessuna voce sul log di accesso del Caching Proxy
- Crea una direttiva ServerInit con le seguenti informazioni:

```
ServerInit /opt/pdweb-lite/lib/wesauth.so:WTESeal_Init
  /opt/pdweb-lite/etc/ibmwesas.conf
```

- Crea una direttiva PreExit con le seguenti informazioni:

```
PreExit /opt/pdweb-lite/lib/wesauth.so:WTESeal_PreExit
```

- Crea una direttiva Authorization con le seguenti informazioni:

  ```
  Authorization * /opt/pdweb-lite/lib/wesauth.so:WTESeal_Authorize
  ```

- Crea una direttiva ServerTerm con le seguenti informazioni:

  ```
  ServerTerm /opt/pdweb-lite/lib/wesauth.so:WTESeal_Term
  ```

  Crea un'istruzione Protect ed una configurazione Protection che inoltra tutte le richieste al processo di autenticazione di Access Manager, come riportato di seguito:

  ```
  Protection PROXY-PROT {
          ServerId WebSEAL-Lite
          Mask All@(*)
          AuthType Basic
          }
  Protect * PROXY-PROT
  ```

Avvio del Caching Proxy e del plug-in di Access Manager

Dopo aver configurato il server proxy e il plug-in di Access Manager, utilizzare il comando **wslstartwte** anziché il comando **ibmproxy start** per avviare il server proxy. Il comando **wslstartwte**carica automaticamente le variabili di ambiente richieste dal plug-in di Access Manager per effettuare l'inizializzazione. Se non si utilizza il comando **wslstartwte** all'avvio del server proxy, vengono visualizzati dei messaggi di errore relativi al plug-in di Access Manager. Il comando di arresto corrispondente, **ibmproxy stop**, è valido anche quando si utilizza il plug-in.

Capitolo 29. Utilizzo del Modulo di autorizzazione PAC-LDAP

Panoramica

Il Modulo di autorizzazione PAC-LDAP abilita Caching Proxy ad accedere al server LDAP (Lightweight Directory Access Protocol) durante l'esecuzione delle routine di autorizzazione o di autenticazione. Il modulo è costituito da due serie di componenti: una coppia di librerie condivise che aggiungono la funzionalità LDAP all'API Caching Proxy e un daemon PAC (Policy Authentication Control). Una direttiva ServerInit nel file ibmproxy.conf indica alla libreria condivisa di inizializzare uno o più daemon PAC all'avvio del Caching Proxy. Per determinare il numero e le caratteristiche dei daemon PAC, le librerie condivise leggono un file paccp.conf. Durante l'inizializzazione, il daemon legge i file pac.conf per le direttive di configurazione e pacpolicy.conf per le informazioni sulle politiche. Quindi, una direttiva di autenticazione nel file ibmproxy.conf indica al server proxy di richiamare la libreria condivisa ogni qualvolta sia necessaria l'autenticazione, oppure la direttiva di autenticazione utilizzerà il flusso di lavoro del Caching Proxy durante l'elaborazione della richiesta HTTP standard.

Autenticazione

Il processo di autenticazione determina se una serie di credenziali fornita – nome utente e password – è valida. Questo processo include la verifica della presenza di un utente nel registro e della password fornita, che deve corrispondere a quella memorizzata nel registro. Queste azioni vengono eseguite utilizzando il modulo PAC-LDAP durante la fase di autenticazione.

Quando il Modulo di autorizzazione PAC-LDAP viene abilitato per l'autenticazione, diventa il contenitore predefinito da cui richiamare gli ID utenti, le password e i gruppi. Quando una richiesta HTTP passa attraverso il flusso di lavoro del Caching Proxy, ciascuna direttiva Protect confronta l'URL della richiesta con il relativo modello di richiesta. In caso di corrispondenza, la direttiva Protect richiama uno schema di protezione che include l'ID server, il tipo di autenticazione da utilizzare, le regole relative alle maschere da applicare al client richiedente e le posizioni dei file password e gruppi. Se il file password non è definito, l'ID utente e la password vengono richiamati tramite il Modulo di autorizzazione PAC-LDAP. Le politiche di tipo 0, 1, 2 e 3 definiscono gli schemi di autenticazione. Se l'autenticazione viene inoltrata, la richiesta viene supportata; altrimenti, il Caching Proxy restituisce un errore 401 al client.

Autorizzazione

Il processo di autorizzazione determina se un utente dispone del permesso necessario per accedere a una risorsa protetta. Quando viene utilizzato il modulo PAC-LDAP, comprende l'applicazione delle regole di autorizzazione che risiedono nel file pacpolicy.conf per la richiesta HTTP.

Quando il Modulo di autorizzazione PAC-LDAP viene abilitato per l'autorizzazione, le relative regole presenti nel file pacpolicy.conf vengono applicate alla richiesta HTTP. Quando la richiesta HTTP passa attraverso il flusso di lavoro del Caching Proxy, ciascuna direttiva Protect confronta l'URL della richiesta con il relativo modello di richiesta. In caso di corrispondenza, la direttiva Protect richiama uno schema di protezione. In questo caso, lo schema di protezione è la routine di autorizzazione utilizzata dal Modulo di autorizzazione PAC-LDAP. La

direttiva Authorization confronta l'URL richiesto con il relativo modello di richiesta e, in caso di corrispondenza, viene richiamato il Modulo di autorizzazione PAC-LDAP. Le politiche di tipo 4 definite nel file pacpolicy.conf ridefiniscono ulteriormente l'autenticazione necessaria per le varie richieste URL.

LDAP (Lightweight Directory Access Protocol)

LDAP consente l'accesso interattivo alle directory X.500 con un consumo minimo di risorse del sistema. IANA ha assegnato la porta TCP 389 e la porta UDP 389 all'LDAP. Per ulteriori informazioni, fare riferimento all'RFC 1777, che definisce il LDAP.

Installazione

Tutti i componenti del Modulo di autorizzazione PAC-LDAP vengono installati automaticamente quando viene installato il sistema Caching Proxy di WebSphere Application Server, Versione 6.0.2. Sui sistemi Linux e UNIX, vengono creati una directory libreria (./lib/) Caching Proxy, una directory libreria (./lib/plugins/pac/) Modulo di autorizzazione PAC-LDAP, una directory binaria (./bin/) e una directory di configurazione (./etc/) all'interno della directory /opt/ibm/edge/cp/. Vengono quindi creati i collegamenti simbolici dalle directory /usr/lib/, /usr/sbin/ e /etc alle directory specifiche di questi prodotti.

Struttura della directory

Directory Linux e UNIX	Directory Windows	Contenuto
/opt/ibm/edge/cp/	\Program Files\IBM\edge\cp\	directory di base Caching Proxy (*cp_root*)
cp_root/sbin/	\Program Files\IBM\edge\cp\Bin\	File binari e script del Caching Proxy
/usr/sbin/		Collegamenti simbolici a *cp_root*/sbin/
cp_root/etc/	\Program Files\IBM\edge\cp\etc\	File di configurazione Caching Proxy
/etc/		Collegamenti simbolici a *cp_root*/etc/
cp_root/lib/	\Program Files\IBM\edge\cp\lib\ plugins\	Librerie Caching Proxy
cp_root/lib/ plugins/pac/	\Program Files\IBM\edge\ cp\lib\plugins\pac\	Librerie Modulo di autorizzazione PAC-LDAP
/usr/lib/		Collegamenti simbolici a *cp_root*/lib/ e *cp_root*/lib/ plugins/pac/
cp_root/server_root/pac/data/	\Program Files\IBM\ edge\cp\server_root\pac\data\	Memorizzazione dati Modulo di autorizzazione PAC-LDAP

Directory Linux e UNIX	Directory Windows	Contenuto
cp_root/server_root/pac/creds/	\Program Files\IBM\edge\cp\server_root\pac\creds\	Credenziali del Modulo di autorizzazione PAC-LDAP

File di plugin LDAP

Nome file Linux e UNIX	Nome file Windows	Descrizione
libpacwte.so	pacwte.dll	libreria condivisa
libpacman.so	pacman.dll	libreria condivisa
pacd_restart.sh	pacd_restart.bat	Script di riavvio daemon PAC
paccp.conf, pac.conf, pacpolicy.conf	paccp.conf, pac.conf, pacpolicy.conf	File di configurazione e delle politiche

Requisiti aggiuntivi per le connessioni protette del server PACD-LDAP

GSKit richiesto dal pacchetto client LDAP

Per abilitare le connessioni SSL protette tra il daemon PACD e il server LDAP, è necessario installare il pacchetto GSKit richiesto dal pacchetto client LDAP. GSKit 7 è richiesto e fornito per impostazione predefinita sulla macchina Caching Proxy ma potrebbe non avere la versione necessaria al client LDAP sulla macchina. È possibile utilizzare versioni differenti di GSKit sulla stessa macchina per processi differenti.

Posizionare il file di chiavi GSKit su `$pacd_creds_dir/pac_keyring.kdb` e la password su `$pacd_creds_dir/pac_keyring.pwd`.

Nota: per le informazioni sui requisiti GSKit sul server LDAP, fare riferimento alla documentazione relativa a IBM Directory Server sul seguente sito Web: http://www.ibm.com/software/tivoli/products/directory-server/

La variabile di ambiente LD_PRELOAD deve essere impostata per i sistemi Linux

Sui sistemi Linux, la variabile di ambiente LD_PRELOAD deve essere configurata come segue per abilitare le connessioni SSL tra il daemon PACD e il server LDAP. Impostare la variabile sul seguente valore:

```
LD_PRELOAD=/usr/lib/libstdc++-libc6.1-1.so.2
```

Il requisito GSKit a cui si è fatto riferimento precedentemente in questa sezione, è valido anche per i sistemi Linux.

Modifica del file ibmproxy.conf per abilitare il Modulo di autorizzazione PAC-LDAP

Tre direttive, ServerInit, Authorization o Authentication, e ServerTerm devono essere aggiunte alla sezione direttive API del file ibmproxy.conf per inizializzare il Modulo di autorizzazione PAC-LDAP. Per creare queste direttive, modificare manualmente il file ibmproxy.conf oppure, se il server proxy è già in esecuzione,

connettersi ai moduli di configurazione e amministrazione con un browser Internet ed aprire il modulo Elaborazione delle richieste API (fare clic su **Configurazione server** –> **Elaborazione richiesta**–> **Elaborazione richiesta API**). (Ciascuna direttiva deve comparire su un'unica riga nel file di configurazione proxy, indipendentemente da se contengono o meno delle interruzioni di riga per per facilitarne la lettura).

Le direttive prototipo (nel modulo dei commenti) vengono fornite nella sezione API del file ibmproxy.conf. Queste direttive API sono in un ordine stabilito. Se si aggiungono direttive API per abilitare nuove funzioni e moduli di plug-in, ordinare le direttive come illustrato nella sezione prototipi del file di configurazione. In alternativa, eliminare il commento o modificare se necessario le direttive API per includere il supporto per ogni funzione o plug-in desiderato.

La direttiva ServerInit ha due argomenti: (1) il percorso completo della libreria condivisa, (2) la chiamata di funzione e (3) il percorso completo del file paccp.conf. Il primo e il secondo argomento sono delimitati da due punti (:). Il secondo e il terzo argomento sono delimitati da uno spazio. Il primo e il terzo argomento sono specifici del sistema e dipendono dal punto in cui sono stati installati i componenti plugin. Il secondo argomento è hard-coded nella libreria condivisa e deve essere digitato esattamente come illustrato.Durante la creazione di una direttiva ServerInit utilizzare il modulo Elaborazione richiesta API, è necessario inserire sia il secondo che il terzo argomento nel campo **Nome funzione**. Il terzo argomento viene visualizzato nella colonna **Modello IP**.

La direttiva Authorization ha tre argomenti: (1) un modello di richiesta, (2) il percorso completo della libreria condivisa e (3) il nome della funzione. Le richieste HTTP vengono confrontate con il modello di richiesta per stabilire se viene richiamata la funzione dell'applicazione. Il modello di richiesta può includere un protocollo, un dominio e un host; può essere proceduto da una barra (/); e può utilizzare un asterisco (*) come carattere jolly. Ad esempio, /front_page.html , http://www.ics.raleigh.ibm.com, /pub*, /* e * sono tutti validi. Il nome della funzione è il nome dato alla funzione dell'applicazione all'interno del programma. È codificato in modo permanente e deve essere digitato esattamente come mostrato. I primi due argomenti sono delimitati da uno spazio. Gli ultimi due sono delimitati da due punti (:).

La direttiva Authentication ha due argomenti: (1) il percorso completo della libreria condivisa e (2) il nome della funzione. Questi argomenti sono delimitati da due punti (:). Il primo argomento è specifico del sistema e dipende dall'installazione della libreria condivisa. Il modello URL per il primo argomento deve avviare la root del documento (/) quando si utilizza il Caching Proxy come proxy inverso. Il secondo argomento è hard-coded nella libreria condivisa e deve essere digitato esattamente come illustrato.

La direttiva ServerTerm ha due argomenti: (1) il percorso completo della libreria condivisa e (2) il nome della funzione. Questi argomenti sono delimitati da due punti (:). Il primo argomento è specifico del sistema e dipende dall'installazione della libreria condivisa. Il secondo argomento è hard-coded nella libreria condivisa e deve essere digitato esattamente come illustrato.Questa direttiva termina il daemon PAC quando il server proxy viene arrestato. Se il proprietario del daemon è differente dal quello del server proxy, il server proxy potrebbe non essere in grado di arrestare il daemon e il daemon deve essere arrestato manualmente da un amministratore.

```
ServerInit path_of_shared_library:pacwte_auth_init path_of_conf_policy_file
```

Esempio di Linux e UNIX:

```
ServerInit /usr/lib/libpacwte.so:pacwte_auth_init /etc/pac.conf
```

Esempio di Windows:

```
ServerInit C:\Progra ~1\IBM\edge\cp\lib\plugins\
  pac\pacwte.dll:pacwte_auth_init C:\Progra ~1\IBM\edge\cp
```

Modello di richiesta autorizzazione *path_of_shared_library*:pacwte_auth_policy

Esempio di Linux e UNIX:

```
Authorization http://* /usr/lib/libpacwte.so:pacwte_auth_policy
```

Esempio di Windows:

```
Authorization http://* C:\Program Files\IBM\edge\cp\lib\plugins\
  pac\pacwte.dll:pacwte_auth_policy
```

Authentication BASIC *path_of_shared_library*:pacwte_auth_policy

Esempio di Linux e UNIX:

```
Authentication BASIC /usr/lib/plugins/pac/libpacwte.so:pacwte_auth_policy
```

Esempio di Windows:

```
Authentication BASIC C:\Program Files\IBM\edge\cp\lib\plugins\
  pac\pacwte.dll:pacwte_auth_policy
```

ServerTerm *path_of_shared_library*:pacwte_shutdown

Esempio di Linux e UNIX:

```
ServerTerm /usr/lib/libpacwte.so:pacwte_shutdown
```

Esempio di Windows:

```
ServerTerm BASIC C:\Program Files\IBM\edge\cp\lib\plugins\
  pac\bin\pacwte.dll:pacwte_shutdown
```

Modifica dei file di configurazione del Modulo di autorizzazione PAC-LDAP

I file di configurazione e delle politiche del Modulo di autorizzazione PAC-LDAP devono essere modificate manualmente da un editor di testo. Un nome direttiva è separato dal primo argomento da due punti (:). Più argomenti sono delimitati da virgole (,). Nel file di configurazione e delle politiche sono incluse le note per facilitare la modifica. Le direttive delle politiche delle chiavi sono mostrate di seguito.

paccp.conf

Il file paccp.conf viene letto dalle librerie condivise durante l'inizializzazione del Caching Proxy e contiene le definizioni (stanza [PAC_MAN_SERVER]) di ciascun daemon PAC che verrà avviato. Ciascun daemon PAC deve disporre della propria stanza [PAC_MAN_SERVER].

```
[PAC_MAN_SERVER]
hostname:                    # nome del daemon PAC
port:                        # porta su cui è in ascolto pacd

[PACWTE_PLUGIN]
hostname_check:[true|false]  # consente la ricerca DNS. Deve avere
                             # la ricerca DNS attivata per ibmproxy per funzionare.
```

pac.conf

Il file pac.conf specifica il server LDAP con cui il daemon PAC tenta di eseguire la connessione.

```
[PAC_MAN_SERVER]
hostname:                    # nome del daemon PAC
port:                        # porta su cui è in ascolto pacd
conn_type:ssl                # impostare come commento se non viene utilizzato SSL
authentication_sequence: [primary|secondary|none]
authorization_sequence:  [primary|secondary|none]

[LDAP_SERVER]
hostname:                    # nome host server LDAP
port:389                     # Porta su cui è in ascolto LDAP
ssl_port:636                 # Porta SSL utilizzata dal server LDAP
admin_dn:                    # Utente con autorizzazione ad accedere al server LDAP
                             # specificare admin_dn:NULL per abilitare il collegamento anonimo
search_base:                 # Parte struttura ad albero LDAP per cercare le info
                             # Se non richiesto, specificare search_base:NULL
search_key:                  # Campo ID da ricercare

[CACHE]
cred_cache_enabled [TRUE|FALSE] # attivare la cache delle credenziali
cred_cache_min_size:100      # num. min. di credenziali da memorizzare nella cache in pacd
cred_cache_max_size:64000    # num. max. di credenziali da memorizzare nella cache in pacd
cred_cache_expiration:86400  # quando una credenziale scade
policy_cache_enabled:[TRUE|FALSE] # attivare/disattivare la cache delle politiche
policy_cache_min_size:100    # numero min. di voci correl. a politiche da memorizzare in cache
policy_cache_max_size:64000  # numero max. di voci correl. a politiche da memorizzare in cache
policy_cache_expiration:86400 # quando una voce correlata alle politiche scade
```

pacpolicy.conf

Tutte le politiche LDAP utilizzano il seguente modello nel file di configurazione e delle politiche. Ciascuna politica deve iniziare con la parola chiave POLICY in maiuscolo tra parentesi.

```
[POLICY]
default_policy:[grant|deny]  # descrive la politica predefinita per gli utenti
                             # che non sono descritti nella sezione POLICY
pac_client_hotname:          # le istanze Caching Proxy che dispongono dell'autorizzazione
                             # all'uso di un elenco delle politiche
id:                          # l'ID per la voce LDAP o ip/hostname
                             # (caratteri jolly, ad esempio *.ibm.com, supportati)
grant:[true|false]           # true consente l'accesso, false
                             # lo nega
type:[0|1|2|3|4]             # 0 voce LDAP che rappresenta il gruppo,
                             # 1 voce LDAP che non rappresenta un gruppo,
                             # 2 indirizzo IP
                             # 3 nome host
                             # 4 URL
propagate:[true|false]       # true indica che i diritti di accesso (concedi
                             # o nega) verranno propagati a tutti
                             # i discendenti o membri
stop_entry:[entry|NULL]      # La propagazione di questo diritto di accesso si ferma
                             # a questa voce. Se l'ID è un gruppo,
                             # stop_entry deve essere impostata su NULL.
                             # stop_entry può essere applicata a un indirizzo IP
                             # o a un nome host. Ciascuna stop_entry
                             # deve essere contenuta sulla propria riga
exception_entry:[entry|NULL] # L'assegnazione del diritto di accesso ignora
                             # queste voci ma continua attraverso il relativo
                             # sottoalbero, che potrebbe essere un elenco di voci
                             # exception_entry può essere applicata a un gruppo,
```

```
                                # un indirizzo IP o un nome host. Ciascuna
                                # exception_entry deve essere contenuta nella propria riga.
Exception_type:
Eccezione:
```

Il carattere jolly (*) è supportato solo per l'ultima posizione di un indirizzo IP o per la prima posizione di un nome host nelle direttive `id` e `stop_entry`. I caratteri jolly non sono supportati nella `exception_entry`. I caratteri jolly non sono supportati per le voci LDAP in qualsiasi campo.

Sono supportate più politiche e il valore false ha la priorità in caso di politiche in conflitto. In altre parole, una singola negazione in una qualsiasi politica blocca l'accesso. L'ordine in cui le politiche vengono elencate nel file di configurazione e delle politiche è irrilevante e non stabilisce una priorità.

Per una serie di esempi di politiche, fare riferimento al file pacpolicy.conf nella directory dei file di configurazione.

Nota: i gruppi nidificati non ereditano le politiche dai gruppi parent. Le uniche politiche applicate a un gruppo sono quelle di cui il gruppo è un membro esplicito.

Creazione di pac_ldap.cred

Creare un file di testo normale denominato pac_ldap.cred in */cp_root*/server_root/pac/creds. Questo file contiene la password corrispondente al nome utente nella direttiva admin_dn, che si trova nel file pac.conf.

Nota: per abilitare il collegamento anonimo, modificare la direttiva admin_dn in pac.conf su admin_dn:NULL e inserire una stringa fittizia nel file pac_ldap.cred.

Il daemon PAC codifica la password la prima volta che legge il file.

Per creare il file pac_ldap.cred sulle piattaforme Linux e UNIX, immettere i seguenti comandi:

```
cd cp_root/server_root/pac/creds
echo "password" > pac_ldap.cred
chown nobody pac_ldap.cred
chgrp nobody pac_ldap.cred
(su SUSE Linux, utilizzare chgrp nogroup pac_ldap.cred.)
```

Per creare il file su una piattaforma Windows, digitare la password in un file di testo e memorizzare il file nella directory server_root\pac\creds\.

Avvio e arresto di pacd

Il daemon di autorizzazione LDAP viene eseguito come processo pacd. È possibile riavviare il daemon di autorizzazione LDAP senza interrompere il Caching Proxy, utilizzando gli script forniti. Eseguire lo script pacd come segue:

- Sulle piattaforme Linux e UNIX:

  ```
  /usr/sbin/pacd_restart.sh pacd_user_id
  ```

- Sulle piattaforme Windows:

  ```
  C:\Program Files\IBM\edge\cp\Bin\pacd_restart.bat CP_install_root
  ```

Nota: il processo pacd può rimanere in esecuzione dopo l'arresto del server Caching Proxy utilizzando il comando **stopsrc -ibmproxy** sui sistemi AIX o il comando **ibmproxy -stop** sui sistemi Linux o Solaris HP-UX. Il processo pacd può essere arrestato in sicurezza utilizzando il comando **kill** nel modo seguente:

```
kill -15 pacd_process_ID
```

Su HP-UX: il plugin PAC-LDAP e pacd potrebbero non caricare tutte le librerie condivise dipendenti al runtime. Prima di utilizzarle, verificare che le variabili di sistema siano impostate come segue

```
SHLIB_PATH=/usr/lib:/usr/IBMldap/lib
PATH=/usr/IBMldap/bin:$PATH
PATH=/usr/IBMldap/bin
```

/usr/IBMldap/ è il percorso di installazione per il client LDAP su HP-UX. Se il clientLDAP è installato in una posizione differente, regolare PATH e SHLIB_PATH di conseguenza. *Se non vengono impostate* queste variabili, potrebbero verificarsi i seguenti errori:

- Dopo aver abilitato il plugin PAC-LDAP, nel log degli errori viene visualizzato il seguente messaggio

  ```
  "Errore Serverinit:
  il server non ha caricato le funzioni dal modulo DLL
  /opt/ibm/edge/cp/lib/plugins/pac/libpacwte.sl"
  ```

- Al tentativo di avvio /usr/sbin/pacd viene visualizzato il seguente errore di collegamento

  ```
  "/usr/lib/dld.sl: Impossibile
  trovare il percorso per la libreria condivisa: libibmldap.sl
   /usr/lib/dld.sl: Nessuna interruzione di file o
   directory"
  ```

Su Linux: per SUSE Linux Enterprise Server 9, l'ldd pacd può riportare che libldap.so non è stato trovato. Per risolvere il problema, creare la seguente stringa simbolica:

```
ln -s /usr/lib/libldap.so.19  /usr/lib/libldap.so
```

Su AIX: all'avvio di pacd con IBM Tivoli Directory Server 5.2, il modulo PAC-LDAP potrebbe non essere in grado di caricare quanto risulta dal seguente errore:

```
exec(): 0509-036 Impossibile caricare il programma
/usr/sbin/pacd a causa dei seguenti errori:
        0509-022 Impossibile caricare il modulo /usr/lib/libpacman.a.
        0509-150 Impossibile caricare il modulo dipendente libldap.a.
        0509-022 Impossibile caricare il modulo libldap.a.
```

Per risolvere il problema, creare la seguente stringa simbolica:

```
ln -s /usr/lib/libibmldap.a /usr/lib/libldap.a
```

Nota: Dopo aver configurato il Caching Proxy per utilizzare l'autenticazione LDAP, verrà visualizzato il seguente errore:

```
Impossibile estrarre un valore per: Uid, codice di ritorno:3
```

Questo errore viene visualizzato anche quando l'autenticazione LDAP funziona correttamente e può essere ignorata.

Parte 6. Monitoraggio di Caching Proxy

Questa sezione fornisce istruzioni per il monitoraggio di Caching Proxy mediante log e Controllo attività del server.

Di seguito vengono forniti i titoli di ciascun capitolo di questa sezione:

Capitolo 30. Configurazione della registrazione

Per personalizzare la registrazione, è possibile utilizzare i moduli Gestione e configurazione o modificare le direttive nel file di configurazione del proxy. È possibile impostare le seguenti opzioni:

- Percorsi e nomi file da memorizzare nei file di log
- Filtri per includere ed escludere informazioni dai file di log di accesso
- Manutenzione delle opzioni per archiviare o eliminare i log

Informazioni sui log

Il Caching Proxy può creare tre tipi di log di accesso, oltre al log eventi e degli errori:

- Log di accesso:
  - **Log di accesso**—Traccia le richieste di gestione locali sul Caching Proxy.
  - **Log di accesso cache**—Traccia le richieste degli oggetti che sono nella cache.
  - **Log di accesso proxy**—Traccia le richieste inviate tramite proxy dai server di origine.
- **Log eventi**—Traccia i messaggi di informazione della cache.
- **Log degli errori**—Traccia i messaggi di errore correlati al Caching Proxy.

Il Caching Proxy crea nuovi file di log ogni giorno a mezzanotte. Se il proxy non è in esecuzione a mezzanotte, al suo primo riavvio in quel giorno vengono creati nuovi log. È possibile specificare la directory e il prefisso del nome file di ciascun file di log; ogni file di log creato contiene un suffisso data in formato *.Mmmddyyyy* (ad esempio, .Apr142000).

Poiché i file di log possono utilizzare una grande quantità di spazio, memorizzare i file di log su un dispositivo di memorizzazione separato dal sistema operativo e dalla cache per evitare errori. Inoltre, configurare le routine di manutenzione dei log, come indicato in "Manutenzione e archiviazione dei log" a pagina 145.

Nomi file di log e opzioni di base

Per specificare la configurazione di base dei log del server proxy, nei moduli Gestione e configurazione, selezionare **Configurazione server –> Registrazione –> File di log**. Specificare il percorso e il nome file di ciascun file di log che si desidera utilizzare. Il nome file corrente di ciascun log viene visualizzato nella casella di testo corrispondente; se non è stato specificato alcun percorso, viene visualizzato il percorso predefinito.

Le informazioni registrate nei log del proxy non vengono scritte automaticamente sul log di sistema, me è possibile configurare il Caching Proxy in modo da poter scrivere sul log di sistema insieme o al posto dei log di cui dispone. Sul modulo **File di log**, selezionare la casella di controllo **Informazioni di log su Syslog**. Il log di sistema deve essere creato prima che questa opzione venga selezionata.

Per specificare che le informazioni di log del server proxy vengono scritte solo sul log di sistema, è necessario modificare il file di configurazione proxy; consultare la

sezione di riferimento per "LogToSyslog — Indica di specificare l'invio delle informazioni di accesso al log di sistema (solo Linux e UNIX)" a pagina 224.

Direttive di file di configurazione correlati

Per impostare i log mediante i file di configurazione proxy, consultare le sezioni di riferimento in Appendice B, "Direttive del file di configurazione", a pagina 165 per le seguenti direttive:

- "AccessLog — Indica di denominare il percorso del file di log accessi" a pagina 167
- "CacheAccessLog — Indica di specificare il percorso ai file di log accessi cache" a pagina 179
- "ErrorLog — Indica di specificare il file dove sono registrati gli errori server" a pagina 202
- "EventLog — Indica di specificare il percorso al file di log eventi" a pagina 204
- "LogToSyslog — Indica di specificare l'invio delle informazioni di accesso al log di sistema (solo Linux e UNIX)" a pagina 224
- "ProxyAccessLog — Indica di denominare il percorso al file di log accessi proxy" a pagina 248

Filtri log di accesso

I log di accesso registrano l'attività della macchina host, del proxy e della cache. Per ogni richiesta di accesso ricevuta dal proxy, una voce del log di accesso appropriato include le seguenti informazioni:

- Cosa è stato richiesto
- Quando è stato richiesto
- Chi ha effettuato la richiesta
- Il metodo della richiesta
- Il tipo di file che il server ha inviato in risposta alla richiesta
- Il codice di ritorno, che indica se la richiesta ha avuto esito positivo o meno
- La dimensione dei dati inviati

Gli errori di accesso vengono registrati nel log degli errori del server.

Motivi per controllare cosa è stato registrato

Esistono diversi motivi per limitare quanto è stato registrato:

- Per ridurre la dimensione del log

  La dimensione dei file di log di un server occupato può aumentare fino a completare lo spazio del disco del server. Per impostazione predefinita, tutte le richieste di accesso vengono registrate, ciò vuol dire che le voci di log vengono create non solo per una pagina HTML ma per ogni immagine di quella pagina. Includendo solo le richieste di accesso più importanti, è possibile ridurre in modo significativo il numero di voci nel log. Ad esempio, è possibile configurare i log di accesso in modo da includere le voci di log per le richieste di accesso della pagina HTML, ma non per le richieste delle immagini GIF.

- Per raggruppare le informazioni destinate

  Ad esempio, se si desidera sapere chi accede dal server da una sede esterna alla società, è possibile filtrare le richieste di accesso che hanno origine dagli indirizzi IP all'interno della società. Se si desidera sapere il numero di visitatori di un determinato sito Web, è possibile creare un log di accesso che mostra solo le richieste di accesso di quell'URL.

Le informazioni escluse da quei log di accesso non sono registrate in nessun report di accesso e non sono disponibili per essere utilizzate in futuro. Per questo motivo, se si è sicuri della quantità di informazioni di accesso che si devono tracciare, applicare i filtri di esclusione con prudenza fino ad acquisire una certa esperienza nel controllo del server.

Configurazione dei filtri dei log di accesso

Le voci dei log di accesso possono essere filtrate in base ai seguenti attributi:

- URL (file o directory)
- Indirizzo IP o nome host
- Agenti utente
- Metodo
- Tipo MIME
- Codice di ritorno

Per specificare i filtri, nei moduli Gestione e configurazione selezionare **Configurazione server –> Registrazione –> Esclusioni log di accesso**. Specificare solo le esclusioni desiderate. Non è necessario utilizzare tutte le categorie.

- Nella sezione intitolata **Non registrare le richieste sulle seguenti Directory o File nel log di accesso**, elencare i percorsi URL per i quali si desidera escludere le voci di log.
- Nella sezione intitolata **Non registrare richieste dai seguenti agenti utente**, elencare gli agenti proxy per i quale si desidera escludere le voci di log.
- Nella sezione intitolata **Non registrare richieste dai seguenti nomi host e indirizzi IP**, elencare i nomi host o gli indirizzi IP per i quali si desidera escludere le voci di log.
- Nella sezione intitolata **Non registrare richieste con i seguenti metodi:**, selezionare le caselle dei metodi per i quali si desidera escludere le voci di log.
- Nella sezione intitolata **Non registrare richieste dei file dei seguenti tipi MIME**, selezionare le caselle dei tipi MIME per i quali si desidera escludere le voci di log.

  Nota: Questa direttiva influisce solo sul log di accesso del Proxy. Non è possibile filtrare un log che elenca questi oggetti memorizzati nella cache per tipo di MIME. Utilizzare AccessLogExcludeURL per eseguire questa operazione.
- Nella sezione intitolata **Non registrare richieste con i seguenti codici di ritorno**, selezionare le caselle dei codici di ritorno delle richieste per i quali si desidera escludere le voci di log.

Fare clic su **Inoltra**.

Direttive di file di configurazione correlati

Per impostare i filtri dei log di accesso mediante i file di configurazione proxy, consultare le sezioni di riferimento in Appendice B, “Direttive del file di configurazione”, a pagina 165 per le seguenti direttive:

- “AccessLogExcludeMethod — Indica di eliminare le voci log di file o directory richieste da un determinato metodo” a pagina 168
- “AccessLogExcludeMimeType — Indica di eliminare le voci log accessi proxy per tipi MIME specifici” a pagina 169

- "AccessLogExcludeReturnCode — Indica di eliminare le voci log di specifici codici di ritorno" a pagina 169
- "AccessLogExcludeURL — Indica di eliminare le voci log di specifici file o directory" a pagina 170
- "AccessLogExcludeUserAgent — Indica di eliminare le voci log da browser specifici" a pagina 170
- "NoLog — Indica di eliminare le voci di log per host o domini specifici che corrispondono a una maschera" a pagina 231

Impostazioni di log predefinite

- **Percorsi predefiniti**

  Tutti i log sono abilitati nella configurazione predefinita del Caching Proxy. Vengono memorizzati nella sottodirectory logs/ della directory di installazione. I percorsi predefiniti sono i seguenti:
  - Log di accesso locali (di gestione):
    - Linux e UNIX: /opt/ibm/edge/cp/server_root/logs/local
    - Windows: *unità*:\Programmi\IBM\edge\cp\logs\local
  - Log di accesso cache:
    - Linux e UNIX: /opt/ibm/edge/cp/server_root/logs/cache
    - Windows: *unità*:\Programmi\IBM\edge\cp\logs\cache
  - Log di accesso proxy:
    - Linux e UNIX: /opt/ibm/edge/cp/server_root/logs/proxy
    - Windows: *unità*:\Programmi\IBM\edge\cp\logs\proxy
  - Log degli errori:
    - Linux e UNIX: /opt/ibm/edge/cp/server_root/logs/error
    - Windows: *unità*:\Programmi\IBM\edge\cp\logs\error
  - Log eventi:
    - Linux e UNIX: /opt/ibm/edge/cp/server_root/logs/event
    - Windows: *unità*:\Programmi\IBM\edge\cp\logs\event

  Ogni nome di file di log è una combinazione del nome di base e di un suffisso data nel formato *.Mmmddyyyy*, ad esempio, proxy.Feb292000.
- **Formati predefiniti**

  I log vengono memorizzati nel formato file comune per impostazione predefinita. È disponibile anche un formato di log combinato e può essere impostato aggiungendo la seguente riga al file di configurazione proxy (ibmproxy.conf).

  ```
  LogFileFormat combinato
  ```

  Il formato di log combinato è simile al formato comune ma ha dei campi aggiunti che mostrano le informazioni sulla provenienza, sull'agente utente e sui cookie. Il formato dell'ora locale è quello predefinito.
- **Contenuto predefinito**

  Per impostazione predefinita, tutte le richieste di accesso vengono registrate nel log di accesso corretto mentre nel log di sistema non viene registrata alcuna informazione di accesso. Le informazioni sul log degli errori vengono scritte solo nel log degli errori, mentre quelle sul log eventi vengono scritte solo sul log eventi.
- **Manutenzione predefinita**

Nella configurazione predefinita, i log non vengono archiviati o eliminati.

Manutenzione e archiviazione dei log

Il Caching Proxy utilizza un plug-in per gestire i log. Per maggiori informazioni, consultare la pagina di riferimento in Appendice B, "Direttive del file di configurazione", a pagina 165 per la direttiva del file di configurazione "Midnight — Indica di specificare il plugin dell'API utilizzato per archiviare i log" a pagina 229.

È possibile specificare come archiviare e rimuovere giornalmente i log. Le opzioni di base sono:

- Comprimere e rimuovere i log che hanno superato la durata specificata.
- Rimuovere i log una volta che hanno raggiunto il limite di durata specificato o dopo che la categoria di log ha raggiunto una dimensione collettiva specifica.
- Eseguire il programma a mezzanotte, ogni notte, per conservare e archiviare i log.

Per impostazione predefinita, i log del giorno corrente e di quello precedente non vengono mai eliminati dall'agente di manutenzione. Tutti i log del giorno corrente e i log di accesso della cache del giorno precedente non vengono mai compressi dall'agente di manutenzione.

Per configurare la manutenzione dei log, nei moduli Gestione e configurazione, selezionare **Configurazione server –> Registrazione –> Archiviazione log**. In questo modulo, utilizzare la casella a discesa per specificare il metodo di manutenzione.

- Se è stato selezionato **Elimina**, impostare la durata, la dimensione file o entrambe per stabilire quali log eliminare. Se i file vengono eliminati per durata e dimensione, i file che hanno superato la durata massima vengono eliminati prima di quelli la cui dimensione supera quella massima impostata. Se i file vengono eliminati per dimensione, i file meno aggiornati vengono eliminati per primi.
- Se si seleziona **Comprimi**, impostare la durata dei log da comprimere e il comando da utilizzare per comprimere i file di log (includere tutti i parametri). Impostare anche la durata massima dei log. Dopo aver compresso i log, l'agente di manutenzione elimina i log compressi che hanno superato la durata massima.

Direttive di file di configurazione correlati

Per configurare l'archiviazione dei log mediante il file di configurazione proxy, consultare le pagine di riferimento in Appendice B, "Direttive del file di configurazione", a pagina 165 per le seguenti direttive:

- "CompressAge — Indica di specificare quando comprimere i log" a pagina 190
- "CompressDeleteAge — Indica di specificare quando eliminare i log" a pagina 192
- "CompressCommand — Indica di specificare il comando di compressione e i parametri" a pagina 191
- "LogArchive — Indica di specificare il funzionamento dell'archiviazione log" a pagina 223
- "Midnight — Indica di specificare il plugin dell'API utilizzato per archiviare i log" a pagina 229
- "PurgeAge — Indica di specificare la durata di un log" a pagina 252

- "PurgeSize — Indica di specificare il limite della dimensione dell'archivio log" a pagina 253.

Scenario file di log

Il seguente esempio mostra come personalizzare la registrazione in base alle proprie esigenze. Si supponga di avere appena acquistato e installato il Caching Proxy. Se si desidera impostare il server in base alle informazioni sui log di accesso e degli errori con i seguenti requisiti:

- I log devono disporre di un indicatore di data e ora locale e avere un formato file di log comune.
- I log di accesso devono essere eliminati se la loro durata ha superato i 30 giorni o se hanno raggiunto una dimensione collettiva di 25 MB.
- I seguenti tipi di richiesta non devono essere registrati sui log di accesso:
  - Richieste di immagini GIF
  - Richieste da host con indirizzi IP che corrispondono al modello 130.128.*.*
  - Richieste di reindirizzamento (queste richieste consentono di ottenere un codice di ritorno tra 300 e 399)

Per configurare il Caching Proxy in modo da conservare i log in base a questi criteri, nei moduli Gestione e configurazione, selezionare **Configurazione server –> Registrazione**.

1. Facoltativamente, selezionare il **modulo File di log** per specificare i percorsi per i file di log di accesso. (Vengono forniti i percorsi predefiniti).
2. Utilizzare il modulo **Archiviazione log** per specificare come archiviare i file:
   - Specificare **Elimina** come metodo di archiviazione.
   - In **Uso dell'eliminazione**, compilare i campi nel seguente modo:
     - **Elimina log con durata superiore a** `30` **Giorni**
     - **Elimina log con dimensione superiore a** `25` **MB**
3. Utilizzare il modulo **Esclusioni log di accesso** per filtrare le voci di log nel seguente modo:
   - Nell'elenco **Non registrare le richieste provenienti dai seguenti nomi host e indirizzi IP**, aggiungere `130.128.*.*` nel campo **Host escluso**.
   - In **Non registrare le richieste di file dei seguenti tipi di MIME**, selezionare la casella di controllo **immagine/gif**.
   - In **Non registrare le richieste con i seguenti codici di ritorno**, selezionare la casella di controllo **(3xx) Reindirizzamento**.

Queste direzioni producono le seguenti righe nel file di configurazione proxy:

```
LogArchive purge
PurgeAge 30
PurgeSize 25
AccessLogExcludeURL *.gif
NoLog 130.128.*.*
AccessLogExcludeReturnCode 300
```

Capitolo 31. Utilizzo del controllo attività del server

Tramite il Controllo attività del server del Caching Proxy è possibile visualizzare le statistiche sulle prestazioni del server e della rete, lo stato del server e della rete e le voci dei log di accesso. Il controllo può essere utilizzato in remoto e non è necessario che si trovi sulla stessa macchina su cui è in esecuzione il server proxy. Il Controllo attività del server è abilitato per impostazione predefinita e non richiede configurazione.

Esistono due modi per avviare il Controllo attività del server:

- In un qualsiasi browser Web collegato, inserire il seguente URL, utilizzando il nome completo del server dove indicato.

  `http://your.server.name/Usage/Initial`
- Nei moduli Gestione e configurazione, selezionare **Controllo attività del server**.

A differenza di altri moduli del client di configurazione, i moduli di questa categoria non impostano le configurazioni del server, ma visualizzano i dati relativi all'uso del server. Questi moduli forniscono delle informazioni molto importanti che possono essere visualizzate in un'unica finestra di console.

Le seguenti sezioni mostrano il tipo di informazioni fornite dal **Controllo attività del server** e suggerisce come utilizzarle per ottimizzare le prestazioni.

Sono disponibili diverse pagine di **Controllo attività del server**:

- **Statistiche delle attività**
- **Statistiche di rete**
- **Statistiche di accesso**
- **Statistiche di accesso proxy**
- **Statistiche cache**
- **Riepilogo aggiornamento cache**

Ogni pagina ha un pulsante **Aggiorna** che può essere utilizzato per aggiornare le informazioni.

Statistiche delle attività

Tabella 4 mostra un esempio della pagina delle **Statistiche di attività**.

Tabella 4. Statistiche delle attività

Statistiche delle attività	
Connessioni	1 Attiva, 431 massimo
Tempo di risposta	Non disponibile
Velocità di trasmissione	0 connessioni/secondo
Richieste elaborate oggi	0
Numero totale di richieste elaborate	114
Errori di richiesta	3

Le statistiche delle attività del server possono essere utilizzate per controllare il traffico del server in termini di numero di richieste di accesso, tempo di risposta,

velocità di trasmissione, richieste elaborate oggi, numero totale di richieste elaborate ed errori. Le seguenti modifiche, apportate alla configurazione, influiscono sulle statistiche sulla pagina **Attività**.

- **Numero di thread attivi**—Specifica il numero di thread da utilizzare per le richieste del server. È possibile diminuire o aumentare il numero di thread disponibili in base alla quantità di memoria disponibile. Per modificare il numero di thread attivi, nei moduli Gestione e configurazione, selezionare **Configurazione server –> Gestione server –> Prestazioni** oppure modificare la direttiva MaxActiveThreads nel file di configurazione. (Consultare "MaxActiveThreads — Indica di specificare il numero massimo di thread attivi" a pagina 226.)
- **Connessioni permanenti**—Se il proxy consente delle connessioni permanenti con un client, si possono avere degli effetti sulla velocità di trasmissione della rete. Per modificare questa impostazione nei moduli Gestione e configurazione, selezionare **Configurazione proxy –> Prestazioni proxy** per abilitare o meno le connessioni permanenti e selezionare **Configurazione server –> Gestione server** per definire le modalità di manutenzione delle connessioni. Per modificare tali impostazioni utilizzando il file di configurazione, consultare le sezioni di riferimento delle seguenti direttive:
  - "MaxPersistRequest — Indica di specificare il numero massimo di richieste da ricevere su una connessione permanente" a pagina 227
  - "PersistTimeout — Indica di specificare il tempo di attesa del client prima di inviare un'altra richiesta" a pagina 236
  - "ProxyPersistence — Indica di autorizzare connessioni permanenti" a pagina 250

Statistiche di rete

Tabella 5 mostra un esempio della pagina delle **Statistiche di rete**.

Tabella 5. Statistiche di rete

Statistiche di rete	
Dati in uscita:	1K byte/secondi
Dati in entrata:	1K byte/secondi
Larghezza di banda ridotta:	3 K byte (0K byte/secondi)
Larghezza di banda ridotta oggi:	0 K byte (0 byte/secondi)

Il modulo **Statistiche di rete** fornisce le informazioni sulla rete su cui è in esecuzione il proxy, includendo la velocità di dati per i byte inviati e ricevuti.

Statistiche di accesso

La pagina delle **Statistiche di accesso** visualizza le 20 voci più recenti nei log di accesso. Questa pagina visualizza le voci recenti nel log di accesso proxy (tipo in nero) e nel log di accesso cache (tipo in blu). È possibile personalizzare ciò che è visualizzato personalizzando ciò che è registrato. Per maggiori informazioni sulle statistiche del log di accesso, consultare "Filtri log di accesso" a pagina 142.

Statistiche di accesso proxy

Il modulo **Statistiche di accesso proxy** fornisce informazioni sull'attività del proxy, come ad esempio gli URL che sono stati richiesti e se sono stati forniti dalla cache.

Oltre agli URL, sono presenti i codici di ritorno forniti ai client e la dimensione file in byte. Le seguenti impostazioni possono migliorare le statistiche di accesso proxy:

- Utilizzare l'aggiornamento automatico della cache per aumentare la probabilità che un documento richiesto si trovi nella cache. Consultare Capitolo 20, "Configurazione dell'agente cache per il precaricamento e l'aggiornamento automatici", a pagina 91 per maggiori dettagli.
- Aumentare la durata di conservazione minima dei file memorizzati nella cache. Consultare "Configurazione aggiornamento cache" a pagina 88 per maggiori dettagli.
- Non memorizzare file di cache provenienti dal dominio locale. Sebbene questa impostazione tenda a diminuire il numero di richieste fornite dalla cache, non si verifica un calo delle prestazioni se i file vengono forniti dalla rete intranet locale con la stessa rapidità con cui vengono forniti dalla cache (in alcuni casi, in modo più rapido). Consultare Capitolo 18, "Controllo degli elementi memorizzati nella cache", a pagina 81 per maggiori dettagli.

Statistiche cache

Se la memorizzazione nella cache è abilitata, la pagina **Statistiche cache** mostra le informazioni di accesso cache più recenti. Fornisce le informazioni sulla cache e sull'indice, incluso quanto segue:

- Se la cache è, al momento, operativa o se è stata eseguita la reindicizzazione dall'avvio di un server
- Se è in esecuzione la raccolta dati inutili
- Media delle occorrenze della cache

Molte opzioni di configurazione della cache modificano i risultati delle statistiche di cache (consultare Parte 4, "Configurazione della cache di server proxy", a pagina 71).

Riepilogo aggiornamento cache

Se l'agente cache è configurato per precaricare i file nella cache, la pagina **Riepilogo aggiornamento cache** mostra le informazioni sull'esecuzione più recente dell'agente cache. L'agente cache deve essere stato eseguito almeno una volta affinché queste informazioni vengano visualizzate. Per modificare la modalità di funzionamento dell'agente di aggiornamento cache, considerare quanto segue:

- Se la maggior parte del traffico di intranet non è su siti Web locali, è opportuno disabilitare la memorizzazione nella cache del dominio locale. Consultare Capitolo 18, "Controllo degli elementi memorizzati nella cache", a pagina 81 per maggiori dettagli.
- Se molti client richiedono una pagina che non viene visualizzata nel log di accesso della cache, è possibile configurare manualmente il precaricamento dell'URL. Consultare "Direttive di file di configurazione proxy correlati" a pagina 95 per le istruzioni.
- Regolare il numero di URL noti da precaricare. Consultare "Direttive di file di configurazione proxy correlati" a pagina 95 per le istruzioni.
- Specificare il periodo di tempo minimo in cui l'agente cache può essere in esecuzione. Consultare "Direttive di file di configurazione proxy correlati" a pagina 95 per le istruzioni.

Appendice A. Utilizzo dei comandi del Caching Proxy

In questa appendice viene fornito un riferimento ai comandi del server proxy.

Comando cgiparse

Scopo

Utilizzare il comando **cgiparse** per analizzare la variabile di ambiente QUERY_STRING degli script CGI. Se la variabile di ambiente QUERY_STRING non è impostata, il comando legge i caratteri CONTENT_LENGTH dall'input standard. Tutti gli output restituiti vengono scritti sull'output standard.

Formato

```
cgiparse -Flag [Modificatore]
```

Parametri

Gli indicatori, i relativi equivalenti di un carattere (-k -f -v -r -i -s -p -c -q -P) e le funzioni, includono:

-keywords | -k
Analizza QUERY_STRING per le parole chiave. Le parole chiave vengono codificate e scritte su output standard, uno per ogni riga.

-form | -f
Analizza QUERY_STRING come richiesta formato. Restituisce una stringa che, se valutata dalla shell, imposta le variabili shell con il prefisso FORM_ seguito da un nome campo. I valori campo sono i contenuti delle variabili.

-value *nome-campo* **| -v** *nome-campo*
Analizza QUERY_STRING come richiesta formato. Restituisce solo il valore del *nome-campo*.

-read | -r
Legge i caratteri CONTENT_LENGTH dall'input standard e li scrive sull'output standard.

-init | -i
Se QUERY_STRING non è impostato, legge i valori dell'input standard e restituisce un'istruzione SET che imposta QUERY_STRING su questo valore. Questo può essere utilizzato con entrambi i metodi GET e POST. Un uso comune è:

```
eval 'cgiparse -init'
```

Questo imposta la variabile di ambiente QUERY_STRING, senza considerare se è stato utilizzato il metodo GET o POST.

cgiparse può essere richiamato più volte nello stesso script se si utilizza il metodo GET, ma deve essere richiamato una sola volta se si utilizza il metodo POST. Con il metodo POST, una volta letto l'input standard, il successivo **cgiparse** trova l'input standard vuoto e attende per un periodo indefinito.

-sep *separatore* **| -s** *separatore*
Specifica la stringa utilizzata per separare più valori. Se si utilizza l'indicatore **-value**, il separatore predefinito è nuova riga. Se si utilizza l'indicatore **-form**, il separatore predefinito è una virgola (,).

-prefix *prefisso* **| -p** *prefisso*
Utilizzato con **-POST** e **-form**, specifica il prefisso da utilizzare durante la creazione di nomi di variabili di ambiente. Il valore predefinito è ″FORM_″.

-count | -c
Utilizzato con **-keywords**, **-form** e **-value**, restituisce un numero di elementi correlati a questi indicatori.

-keywords | -k
Restituisce il numero di parole chiave.

-form | -f
Restituisce il numero di campi univoci (i valori multipli vengono contati come unici).

-value *nome-campo* **| -v** *nome-campo*
Restituisce il numero di valori del *nome-campo* (se non esiste alcun campo denominato *nome-campo*, l'output è `0`).

-*numero*
Utilizzato con **-keywords**, **-form** e **-value**, restituisce l'occorrenza specifica correlata a questi indicatori.

-keywords
Restituisce la parola chiave numero *n*. (Ad esempio, **-2 -keywords** restituisce la seconda parola chiave).

-form
Restituisce tutti i valori del campo numero *n*. (Ad esempio, **-2 -form** restituisce tutti i valori del secondo campo).

-value *nome-campo*
Restituisce il valore numero *n* di più valori del campo *nome-campo*. (Ad esempio, **-2 -value -whatsit** restituisce il secondo valore del campo **whatsit**).

-quiet | -q
Elimina tutti i messaggi di errore. (Lo stato di uscita diverso da zero indica ancora la presenza di errori).

-POST | -P
Le informazioni dell'input standard (o, se si considera un nome file, il file stdin) vengono codificate e analizzate direttamente nelle variabili shell, QUERY_STRING non viene utilizzata. **-POST** equivale all'uso consecutivo delle opzioni **-init** e **-form**.

Esempi

I seguenti esempi ignorano il fatto che, in realtà, QUERY_STRING è già impostata dal server. Nei seguenti esempi, $ è il prompt di shell Bourne.

- Ricerca parola chiave

```
$ QUERY_STRING="is+2%2B2+really+four%3F"
$ export QUERY_STRING
$ cgiparse -keywords
is
2+2
really
four?
$
```

- Analisi di tutti i campi formato

```
$ export QUERY_STRING="name1=Value1&name2=Value2%3f+That%27s+right%21";
$ cgiparse -form
FORM_name1='Value1'; FORM_name2='Value2? That'\''s right!'
$ eval `cgiparse -form`
```

```
$ set | grep FORM
FORM_name1="Value1"
FORM_name2="Value2? That's right!"
$
```

- Estrazione di un unico valore campo

```
$ QUERY_STRING="name1=value1&name2=Second+value%3F+That'\''s%27s
$ cgiparse -value name1
value1
$ cgiparse -value name2
Second value? That's right!
$
```

Risultati

0 Riuscito

1 Riga comandi non valida

2 Variabili di ambiente non impostate correttamente

3 Impossibile ottenere le informazioni richieste (ad esempio, tale campo non esiste oppure QUERY_STRING contiene parole chiave quando vengono richiesti i valori del campo formato)

Nota: Se si riceve uno di questi codici di errore, si possono ricevere anche altri messaggi informativi. Il comando varia in base al messaggio emesso.

Comando cgiutils

Scopo

Utilizzare il comando **cgiutils** nei programmi nph (no-parse header) per produrre una risposta HTTP 1.0 completa.

Nota: Se si desidera fornire i programmi nph (no-parse header) per poter restituire i valori di ritorno, il nome del programma deve iniziare con **nph-**. In questo modo si evita che l'intestazione del server sovrascriva il valore di ritorno con il valore di ritorno standard del server.

Formato

```
cgiutils -Flag [Modificatore]
```

Se *Modificatore* contiene degli spazi vuoti, includerli tra virgolette (″″).

Parametri

-version
Restituisce informazioni sulla versione.

-nodate
Non restituisce l'intestazione **Date:**.

-noel
Non restituisce una riga vuota dopo le intestazioni. È utile se si desiderano altre intestazioni MIME dopo le righe intestazione iniziali.

-status *nnn*
Restituisce la risposta HTTP completa con il codice stato *nnn*, anziché un'unica serie di intestazioni HTTP. Non utilizzare questo indicatore se si desidera solo l'intestazione **Expires:**.

-reason *spiegazione*
Specifica la riga per la risposta HTTP. È possibile utilizzare solo questo indicatore con l'indicatore **-status** *nnn*.

-ct [*tipo/sottotipo***]**
Specifica l'intestazione Content-Type MIME. Questo esempio specifica un tipo di contenuto MIME di text/html:

```
cgiutils -ct text/html
```

Se si omette *tipo/sottotipo*, il tipo di contenuto MIME è impostato su text/plain predefinito. Questo esempio imposta il tipo di contenuto MIME su text/plain.

```
cgiutils -ct
```

-ce *codifica*
Specifica l'intestazione Content-Encoding MIME. Ad esempio:

```
cgiutils -ce  x-compress
```

-cl *codice-lingua*
Specifica l'intestazione Content-Language MIME. Ad esempio:

```
cgiutils -cl en_UK
```

-length *nnn*
Specifica l'intestazione Content-Length MIME.

-expires *Spec-tempo*
Specifica l'intestazione **Expires:** MIME. Questo indicatore specifica la durata (la data di scadenza di un documento) in qualsiasi combinazione di giorni, ore, minuti e secondi. È il periodo di tempo per cui il documento è considerato valido. Ad esempio:

```
   cgiutils
-expires 2 giorni 12 ore
```

Il comando **cgiutils** aggiunge l'ora specificata sulla GMT (Greenwich Mean Time) corrente per determinare l'ora di scadenza. L'ora di scadenza è inserita nell'intestazione **Expires:** nel formato HTTP.

-expires now
Produce un'intestazione **Expires:** che corrisponde all'intestazione **Date:**.

-uri *URI*
Specifica l'URI (Universal Resource Identifier) del documento restituito. URI può essere considerato uguale all'URL.

-extra *xxx: yyy*
Specifica un'intestazione extra, che non potrebbe essere specificata altrimenti, per il comando **cgiutils**.

Esempi

- Questo esempio calcola la data di scadenza dell'intestazione **Expires:**.

  ```
  cgiutils
  -expires "1 anno 3 mesi 2 settimane 4 giorni 12 ore 30 minuti"
  ```

- Il seguente esempio specifica il codice stato e la causa e imposta l'intestazione **Expires:** allo stesso modo dell'intestazione **Date:**.

  ```
  cgiutils -status 200 -reason "Virtual doc follows" -expires now
  ```

  Potrebbero essere prodotte intestazioni simili alle seguenti:

  ```
  HTTP/1.0 200 Virtual doc follows
  Versione MIME: 1.0
  Server: IBM-ICS
  Data: Mar, 05 gennaio 1996 03:43:46 GMT
  Scadenza: Mar, 05 gennaio 1996 03:43:46 GM
  ```

  Il comando cgiutils produce automaticamente l'intestazione **Server:** perché disponibile nell'ambiente CGI. Inoltre, il campo **Data:** viene generato automaticamente a meno che non sia specificato l'indicatore **-nodate**.

  Ciò include una riga vuota dopo l'output per indicare la fine della sezione dell'intestazione MIME. Se si desidera seguire questa intestazione insieme ad altre, utilizzare l'indicatore **-noel** (NO-Empty-Line) come illustrato nel seguente esempio.

- Se non si desidera alcuna riga vuota dopo la riga dell'intestazione, utilizzare l'indicatore **-noel**:

  ```
  cgiutils -noel -expires "2 days" -nodate
  ```

  ```
  HTTP/1.0 200 Virtual doc follows
  Versione MIME: 1.0
  Server: IBM-ICS
  Scadenza: Mar, 07 gennaio 1996 03:43:46 GMT
  ```

Comando htadm

Scopo

Utilizzare il comando **htadm** per controllare i file di password del server. Il server utilizza i file di password per controllare l'accesso ai file. È possibile aggiungere un nome utente ad un file di password, eliminare un utente da un file di password, verificare una password utente' e creare un file di password vuoto. È inoltre possibile modificare la password di un utente eliminando prima la password dell'utente e creandone, poi, una nuova.

Nota: Se si utilizza il comando **htadm** per aggiungere un utente, modificare o controllare una password, è necessario inserire quest'ultima sulla riga comandi. Poiché il comando elimina il prima possibile la password dalla riga comandi, è molto improbabile che si possa visualizzare una password utente ' esaminando l'elenco dei processi sulla macchina (ad esempio, con il comando **ps**).

Formato

```
htadm -Flag[Modificatore]
```

Parametri

-adduser *nome-utente file-password* **[***password* **[***nome reale***]]**

Aggiunge un utente e una password al file di password. Se si inserisce il comando solo con *file-password*, verranno richiesti altri parametri.

file-password

Il percorso e il nome del file di password al quale si desidera aggiungere l'utente.

nome-utente

Il nome dell'utente che si desidera aggiungere.

Per il nome utente utilizzare solo caratteri alfanumerici; non usare caratteri speciali.

Il comando non funziona se nel file di password esiste già un utente con lo stesso nome.

password

La password che si desidera definire per il nome utente.

Le password possono avere fino a 32 caratteri. Per la password utilizzare solo caratteri alfanumerici; non usare caratteri speciali.

Note:

1. Alcuni browser non possono leggere e inviare password con più di otto caratteri. A causa di questa limitazione, se si definisce una password con più di otto caratteri, il server riconosce come valida la password completa o solo i primi otto caratteri.
2. Il nome utente e la password per l'amministratore prevedono la distinzione tra maiuscole e minuscole, anche se il sistema operativo non la prevede. Durante l'accesso ai moduli di Gestione e configurazione, accertarsi di digitare il nome utente e la password esattamente come sono stati immessi mediante il comando `htadm`.

nome-reale
Un commento o un nome che si desidera utilizzare per identificare il nome utente che si sta aggiungendo. Qualsiasi elemento immesso verrà scritto nel file di password.

-deluser *file-password* **[***nome-utente***]**
Elimina un utente dal file di password. Se si inserisce il comando solo con *file-password*, verrà richiesto il parametro *nome-utente*.

file-password
Il percorso e il nome del file di password dal quale si desidera eliminare un utente.

nome-utente
Il nome dell'utente che si desidera eliminare. Il comando ha esito negativo se il nome utente specificato non esiste nel file di password.

-passwd *file-password* **[***nome-utente* **[** *password***]]**
Modifica la password di un nome utente già definito nel file di password. Se si inserisce il comando solo con *file-password*, verranno richiesti altri parametri.

file-password
Il percorso e il nome del file di password che contiene il nome utente di cui si desidera modificare la password.

nome-utente
Il nome utente di cui si desidera modificare la password.Il comando ha esito negativo se il nome utente specificato non esiste nel file di password.

password
La nuova password che si desidera definire per il nome utente.

Le password possono avere fino a 32 caratteri. Per la password utilizzare solo caratteri alfanumerici; non usare caratteri speciali.

Note:

1. Alcuni browser non possono leggere e inviare password con più di otto caratteri. A causa di questa limitazione, se si definisce una password con più di otto caratteri, il server riconosce come valida la password completa o solo i primi otto caratteri.
2. Il nome utente e la password per l'amministratore prevedono la distinzione tra maiuscole e minuscole, anche se il sistema operativo non la prevede. Durante l'accesso ai moduli di Gestione e configurazione, accertarsi di digitare il nome utente e la password esattamente come sono stati immessi mediante il comando `htadm`.

-check *file-password* **[***nome-utente* **[** *password***]]**
Verifica la password di un nome utente già definita nel file di password e indica se è corretta o meno. Se si inserisce il comando solo con *file-password*, verranno richiesti altri parametri.

file-password
Il percorso e il nome del file di password che contiene il nome utente di cui si desidera verificare la password.

nome-utente
Il nome utente di cui si desidera verificare la password.Il comando ha esito negativo se il nome utente specificato non esiste nel file di password.

password
La password che si desidera verificare. Se la password inserita è quella definita per il nome utente, il comando scrive `Correct` sull'output standard

e termina con codice di ritorno `0`. Se la password non è quella definita per il nome utente, il comando scrive `Incorrect` sull'output standard.

-create *file-password*
Creare un file di password vuoto.

file-password
Il percorso e il nome del file di password che si desidera creare.

Esempi

- Per aggiungere un utente al file di password:
  - Sistemi Linux e UNIX:

    ```
    htadm -adduser /opt/ibm/edge/cp/server_root/protect/heroes.pwd
    clark superman "Clark Kent"
    ```

  - Sistemi Windows:

    ```
    htadm -adduser "C:\Program Files\IBM\edge\cp\server_root\protect\
    heroes.pwd" clark superman "Clark Kent"
    ```

  Nota: Il comando **htadm** deve trovarsi su un'unica riga. In questo esempio, per agevolare la lettura, il comando è su più di una riga. Inserire il comando effettivo su una riga con almeno uno spazio tra `clark` e `superman`.
- Per eliminare un utente da un file di password:
  - Sistemi Linux e UNIX:

    ```
    htadm -deluser /opt/ibm/edge/cp/server_root/protect/
         heroes.pwd clark superman "Clark Kent"
    ```

  - Sistemi Windows:

    ```
    htadm -deluser "C:\Program Files\IBM\edge\cp\server_root\protect\
    heroes.pwd" clark superman "Clark Kent"
    ```

comando htcformat

Scopo

Utilizzare il comando **htcformat** per preparare un file o un'unità non formattata per contenere la cache proxy. Questo comando di formato deve essere utilizzato prima che l'unità venga indicata per l'uso con la cache proxy.

Il percorso unità deve specificare l'unità non formattata. Consultare la documentazione del file system per informazioni su come accedere alle unità non formattate. In Parte 4, "Configurazione della cache di server proxy", a pagina 71 sono disponibili degli esempi.

Nota: I kernel Linux 2.2 non supportano la memorizzazione nella cache delle unità non formattate. Sulle piattaforme Linux, per la memoria cache si possono utilizzare solo i file e la memoria.

La dimensione minima per una cache del Caching Proxy è 16392 KB, ovvero 2049 blocchi.

Formato

```
htcformat unità [-blocksize
<dimensione blocco>] [-blocks numero di blocchi]
htcformat -file percorsofile [-blocksize
dimensione blocco] -blocks numero di blocchi
```

Parametri

-blocksize
Imposta la dimensione dei blocchi nel supporto del dispositivo cache. La dimensione blocco è in byte. Il valore predefinito è 8192 e dovrebbe essere utilizzato per tutte le situazioni.

-blocks
Numero di blocchi da creare sull'unità o nel file. Durante la formattazione di un file, questo argomento è obbligatorio per poter specificare la dimensione file. Questo argomento può essere utilizzato per limitare la quantità di un'unità o di partizione particolare da utilizzare per la memoria cache. Se non viene specificato alcun argomento blocchi, verranno creati tanti blocchi quanti ne potrà contenere la partizione.

-file
Formatta un file anziché un'unità di memoria.

Uso

Il sistema di memorizzazione nella cache isola i file o i dispositivi cache in contenitori per l'indicizzazione e la raccolta dati inutili. La dimensione dei contenitori è impostata su un certo numero di blocchi; tale dimensione non può essere configurata. Affinché venga eseguita la raccolta dati inutili, sono necessari almeno due contenitori; la dimensione minima di cache è 16392 KB.

Il comando **htcformat** rifiuta una richiesta di formato che fornisce un dispositivo cache con meno di due contenitori.

Esempi

Nel seguente esempio viene formattata una partizione disco chiamata c0t0d0s0 su Solaris.

```
htcformat /dev/rdsk/c0t0d0s0
```

Nel seguente esempio viene formattata una partizione disco chiamata lv02 su AIX.

```
htcformat /dev/rlv02
```

Nel seguente esempio viene formattata una partizione disco chiamata d: su Windows.

```
htcformat \\.\d:
```

Nel seguente esempio viene formattato un file denominato filecache con una dimensione di circa 1 GB.

```
htcformat -file /opt/ibm/edge/cp/filecache -blocks 131072
```

Comando ibmproxy

Scopo

Utilizzare il comando **ibmproxy** per avviare il server.

È possibile impostare tutti questi indicatori (tranne **-r**) mediante le direttive nel file di configurazione del server.

Normalmente si crea un file denominato README contenente le istruzioni o le notifiche utili per chi utilizza questa directory per la prima volta. Per impostazione predefinita, il comando **ibmproxy** include qualsiasi file README nella versione ipertestuale di una directory. Le istruzioni del file README possono essere impostate anche con la direttiva di configurazione DirReadme.

Formato

```
ibmproxy [-Flag [-Flag [-Flag..]]]
```

Parametri

-nobg
Esegue il server come un processo in primo piano e non come un processo in background. Il valore predefinito prevede un processo in background.

-nosnmp
Disattiva il supporto SNMP.

-p *numero-porta*
È in ascolto su questo numero di porta. Il numero di porta predefinito è 80. Questo indicatore sovrascrive la direttiva Port specificata nel file di configurazione. Per utilizzare il valore predefinito o il valore specificato nel file di configurazione, omettere questo indicatore.

-r *file-configurazione*
Specifica il file da utilizzare come file di configurazione. È necessario utilizzare questo indicatore se si desidera avviare il server con un file di configurazione diverso da quello predefinito. Questo consente di utilizzare più file di configurazione.

-restart
Riavvia un server attualmente in esecuzione. Il comando **ibmproxy** ottiene il numero di processi del server in esecuzione da PidFile e invia il numero di processi al segnale HangUP (HUP). Quindi, ricarica i file di configurazione e riapre i file di log. Per evitare eventuali danni, non eseguire due istanze del server contemporaneamente usando lo stesso PidFile, i file di log e la cache proxy.

Poiché il daemon **http** deve leggere il file di configurazione che il server sta utilizzando per accedere a PidFile, è necessario specificare lo stesso file di configurazione al riavvio. Se è stato utilizzato l'indicatore **-r** e un file di configurazione specifico quando al riavvio del server, è necessario specificare questo indicatore e lo stesso file con **-restart**.

-snmp
Attiva il supporto SNMP.

-unload
Su AIX, scarica l'estensione kernel proxy trasparente. Su Linux, rimuove le regole firewall associate.

Le opzioni di gestione del segnale sono presenti anche sulle piattaforme Linux e UNIX. Sulle piattaforme Linux e UNIX, sono disponibili le seguenti opzioni.

SIGTERM
Il comando **ibmproxy** si arresta e si chiude una volta completato. Per terminare immediatamente, utilizzare SIGKILL o CANCEL.

SIGHUP
Se in esecuzione, il comando **ibmproxy** riavvia, ricarica il file di configurazione e continua l'elaborazione.

Esempi

- Per avviare il server sulla porta 8080, mediante il file di configurazione /usr/etc/ibmproxy.conf, anziché quello predefinito /etc/ibmproxy.conf, immettere:

  ```
  ibmproxy -p 8080 -r /usr/etc/ibmproxy.conf
  ```

- Su AIX, per riavviare un server con il file di configurazione predefinito mediante System Resource Controller, immettere:

  ```
  startsrc -s ibmproxy
  ```

  Se il file di configurazione predefinito non esiste, il comando **ibmproxy** esporta la struttura ad albero della directory /Public. Questa struttura ad albero può contenere dei collegamenti non permanenti ad altre strutture ad albero della directory.

Appendice B. Direttive del file di configurazione

Questa appendice descrive le direttive contenute nel file di configurazione ibmproxy.conf.

- **Su sistemi Linux e UNIX.** Queste direttive risiedono nel file di configurazione ibmproxy.conf nella directory /etc/.
- **Su sistemi Windows.**Normalmente, queste direttive risiedono su C:\Programmi\IBM\edge\cp\.

Utilizzare queste informazioni come riferimento se si intende configurare il server modificando il file ibmproxy.conf. Se si utilizzano i moduli Gestione e configurazione, non è necessario fare riferimento a questo capitolo.

Le direttive sono elencate in ordine alfabetico.

Direttive non modificate al riavvio

Alcune direttive non vengono aggiornate quando il server viene riavviato. Se le direttive riportate di seguito vengono modificate mentre il server è in esecuzione, è necessario arrestare e riavviare il server manualmente. (Consultare Capitolo 5, “Avvio e arresto di Caching Proxy”, a pagina 15.)

Tabella 6. Direttive non aggiornate al riavvio

Gruppo direttive	Direttive
CGI	DisinheritEnv, InheritEnv
Memorizzazione nella cache	Caching
Registrazione	AccessLog, CacheAccessLog, ErrorLog, ProxyAccessLog, ServerRoot
Accesso alla rete	BindSpecific, Hostname, ListenBacklog, Port
Prestazioni	MaxActiveThreads
RTSP	Tutte le direttive RTSP
SSL	Tutte le direttive SSL
Controllo processi Linux e UNIX	GroupId, UserId
Varie	TransparentProxy

Panoramica delle direttive

Questa appendice contiene le seguenti informazioni per ciascuna direttiva:

- Un’intestazione con il nome e una breve descrizione della direttiva
- Istruzioni per l’uso
- Il formato della direttiva che segue la sintassi generale:

  ```
  NomeDirettiva valore
  ```

- Dove possibile, un esempio di impostazione della direttiva nel file di configurazione

Nota: gli esempi nelle direttive con percorsi Windows contengono, a volte, *server_root*, ossia la directory root del server selezionato durante l'installazione.

- Il valore o i valori predefiniti della direttiva

  I valori originali codificati nel file di configurazione predefinito. Modificare solo le parti del file di configurazione che si desidera differenziare dai valori predefiniti. Una direttiva che non presenta valori predefiniti inizialmente codificati compare nel file come preceduta da un indicatore di commento (#). Se si intende specificare un valore per la direttiva, eliminare l'indicatore di commento e aggiungere il valore alla riga nel file di configurazione.

Valori validi

L'elenco riportato di seguito contiene i valori validi nel file di configurazione:

- Nelle informazioni di riferimento di alcune direttive, la parte *valore* contiene maschere per richieste, nomi percorso o nomi host. Se non diversamente indicato, nelle maschere è possibile utilizzare il carattere asterisco (*). Per la maschera da confrontare, è possibile sostituire l'asterisco con qualsiasi stringa di caratteri o singolo carattere.
- Le direttive di configurazione che consentono di inserire una stringa positiva, accettano i seguenti valori:
  - `Yes`
  - `On`
  - `OK`
  - `Enable`
- Le direttive di configurazione che consentono di inserire una stringa negativa, accettano i seguenti valori:
  - `No`
  - `Off`
  - `None`
  - `Disable`
- Le direttive di configurazione che consentono di specificare un intervallo di tempo, accettano qualsiasi combinazione dei seguenti valori:
  - *hh*—ore
  - *hh*`:`*mm*—ore e minuti
  - *hh*`:`*mm*`:`*ss*—ore, minuti e secondi
  - *n* `years`—numero di anni di 365 giorni
  - *n* `months`—numero di mesi di 30 giorni
  - *n* `weeks`—numero di settimane di 7 giorni
  - *n* `days`—numero di giorni di 24 ore
  - *n* `hours`—numero di ore di 60 minuti
  - *n* `minutes`—numero di minuti di 60 secondi
  - *n* `seconds`—numero di secondi
  - *n* `fortnights`—numero di intervalli di 14 giorni

  Tutte le voci vengono convertite in secondi, quindi unite.
- I caratteri vuoti non sono consenti nel nome di un file specificato nel file di configurazione. Gli spazi sono considerati come delimitatori.

Sintassi dei record del file di configurazione

Durante la modifica del file di configurazione, tenere presente quanto segue:

- Ciascuna direttiva deve iniziare su una nuova riga.
- Separare i valori utilizzando almeno uno spazio. Non esiste distinzione tra carattere spazio e tabulazione.
- L'inizio di un commento viene indicato da un simbolo #. Tutti i caratteri tra il simbolo # e la fine della riga vengono ignorati.
- Per specificare un numero o uno spazio per una direttiva, farlo precedere da una barra rovesciata (\) utilizzata come carattere di Escape. Un carattere di Escape indica che il carattere seguente deve essere interpretato come carattere e non come comando; ad esempio, se una riga contiene \#, il server lo interpreta come simbolo # e non come inizio di un commento, quindi prosegue la lettura dei caratteri. Se una riga contiene il carattere \, il server lo interpreta come uno spazio e non come un delimitatore e continua la lettura dei caratteri per creare il valore.

Direttive Caching Proxy

Di seguito vengono riportate le direttive Caching Proxy.

AcceptAnything — Indica di supportare tutti i file

Utilizzare questa direttiva per supportare i file per il client anche se il tipo MIME del file non corrisponde a un'intestazione `ACCEPT:` inviata dal client. Se questa direttiva è impostata su `OFF`, i file i cui tipi MIME differiscono dai tipi accettabili dal client non possono essere visualizzati. Perciò, viene visualizzata una pagina di errore.

Formato

```
AcceptAnything  {on | off}
```

Esempio

```
AcceptAnything off
```

Impostazione predefinita

```
AcceptAnything on
```

AccessLog — Indica di denominare il percorso del file di log accessi

Utilizzare questa direttiva per specificare la directory e il file in cui si intende registrate le statistiche di accesso al log. Per impostazione predefinita, il server scrive una voce in questo log ogni volta che un client invia al server una richiesta relativa ai dati memorizzati sul server locale. Normalmente, queste voci contengono solo le richieste provenienti dal client di configurazione o gli accessi, quando la macchina Caching Proxy viene utilizzata come server di origine. Questo log non contiene informazioni sull'accesso proxy o cache.

Utilizzare la direttiva NoLog per specificare i client le cui richieste non devono essere registrate. Per una descrizione della direttiva NoLog, fare riferimento a "NoLog — Indica di eliminare le voci di log per host o domini specifici che corrispondono a una maschera" a pagina 231.

Il server avvia un nuovo file di log ogni giorno a mezzanotte, se in esecuzione. In caso contrario, questo si verifica appena il server viene avviato. Quando il file

viene creato, il server utilizza il nome del file specificato, a cui appone un suffisso data. Questo è nel formato *Mmmddyyyy*, dove *Mmm* si riferisce alle prime tre lettere del mese, *dd* al giorno e *yyyy* all'anno.

Nota: se si modificano i valori predefiniti del server relativamente a ID utente, ID gruppo o percorsi di directory log, creare le nuove directory, quindi aggiornarne autorizzazioni e proprietà. Per fare in modo che il server scriva le informazioni su una directory log definita dall'utente, l'autorizzazione per tale directory deve essere impostata su 755 mentre l'ID del server definito dall'utente deve essere impostato su proprietario. Ad esempio, se l'ID utente del server viene modificato dal valore predefinito al valore jdoe e la directory logs predefinita viene modificata in server_root/account, quest'ultima deve disporre dell'autorizzazione 755 ed essere di proprietà di jdoe.

È opportuno eliminare i file di log meno recenti in quanto occupano una significativa quantità di spazio sul disco rigido.

Formato

```
AccessLog  /percorso_directory/nome_filelog
```

Esempio

```
AccessLog  /logs/accesslog
```

Impostazioni predefinite

- **Sistemi Linux e UNIX:** `AccessLog /opt/ibm/edge/cp/server_root/logs/local`
- **Sistemi Windows:** `AccessLog drive:\Programmi\IBM\edge\cp\logs\local`

AccessLogExcludeMethod — Indica di eliminare le voci log di file o directory richieste da un determinato metodo

Utilizzare questa direttiva per non registrare le richieste effettuate da uno specifico metodo per accedere a file o directory. Ad esempio, non si desidera registrare le richieste DELETE per file o directory.

È possibile disporre di più occorrenze di questa direttiva nel file di configurazione. Inoltre, è possibile inserire più metodi sulla stessa direttiva, purché vengano separati da uno o più spazi.

Formato

```
AccessLogExcludeMethod metodo  [...]
```

Esempi

```
AccessLogExcludeMethod GET
AccessLogExcludeMethod PUT
AccessLogExcludeMethod POST
AccessLogExcludeMethod DELETE
AccessLogExcludeMethod GET   PUT
```

Impostazione predefinita

Nessuna. Nel log accessi, il server include i file e le directory richiesti da tutti i tipi di metodi.

AccessLogExcludeMimeType — Indica di eliminare le voci log accessi proxy per tipi MIME specifici

Utilizzare questa direttiva per specificare che non si intende registrare nel log accessi proxy le richieste di accesso a directory o file di un tipo MIME specificato. (Esempi di tipi MIME sono text/html, image/gif e image/jpeg.) Ad esempio, non si intende registrare richieste di accesso a immagini GIF.

È possibile disporre di più occorrenze di questa direttiva nel file di configurazione. Inoltre, è possibile inserire più tipi MIME sulla stessa direttiva, purché vengano separati da uno o più spazi.

Nota: questa direttiva interessa esclusivamente il log accessi proxy. Non è possibile filtrare un log che elenca questi oggetti memorizzati nella cache per relativi tipi MIME. Per effettuare questa operazione, utilizzare AccessLogExcludeURL.

Formato

```
AccessLogExcludeMimeType tipo_MIME  [...]
```

Esempio

```
AccessLogExcludeMimeType image/gif
AccessLogExcludeMimeType text/html
AccessLogExcludeMimeType image/gif   text/html
```

Impostazione predefinita

Nessuna. Il log accessi include richieste inviate al server relative a file e directory di tutti i tipi MIME.

AccessLogExcludeReturnCode — Indica di eliminare le voci log di specifici codici di ritorno

Utilizzare questa direttiva per specificare che non si intende registrare le richieste di accesso che rientrano all'interno di uno specifico intervallo di numeri di codici di errore. Questi numeri sono codici di stato del server proxy. Non è possibile specificare singoli codici. Ad esempio, il valore 300, indica che si intende escludere le richieste di accesso con codici di ritorno di reindirizzamento (301, 302, 303 e 304).

È possibile disporre di più occorrenze di questa direttiva nel file di configurazione. Inoltre, è possibile inserire più codici di ritorno sulla stessa direttiva purché vengano separati da uno o più spazi.

Formato

```
AccessLogExcludeReturnCode intervallo
```

Esempio

```
AccessLogExcludeReturnCode 300
```

Impostazione predefinita

Nessuna. Il log accessi include tutte le richieste inviate al server, indipendentemente dal codice.

AccessLogExcludeURL — Indica di eliminare le voci log di specifici file o directory

Utilizzare questa direttiva se non si intende registrare le richieste di accesso a specifici file o directory che corrispondono a una maschera URL specificata. Ad esempio, non si intende registrare le richieste di accesso ai file GIF o a uno specifico file o directory sul server.

È possibile disporre di più occorrenze di questa direttiva nel file di configurazione. Inoltre, è possibile inserire più voci sulla stessa direttiva, purché vengano separate da uno o più spazi.

Formato

```
AccessLogExcludeURL  file_o_tipo [...]
```

Esempi

```
AccessLogExcludeURL  *.gif
AccessLogExcludeURL  /Freebies/*
AccessLogExcludeURL  *.gif   /Freebies/*
```

Impostazione predefinita

Nessuna. Il server registra le richieste di accesso a tutti i file e directory.

AccessLogExcludeUserAgent — Indica di eliminare le voci log da browser specifici

Utilizzare questa direttiva per specificare che non si intende registrare le richieste di accesso eseguite da specifici agenti utente (ad esempio, Internet Explorer 5.0).

È possibile disporre di più occorrenze di questa direttiva nel file di configurazione. Inoltre, è possibile inserire più voci sulla stessa direttiva, purché vengano separate da uno o più spazi.

Formato

```
AccessLogExcludeUserAgent agente_utente [...]
```

Esempio

```
AccessLogExcludeUserAgent  *Mozilla/2.0
AccessLogExcludeUserAgent  *MSIE 5*
```

Impostazione predefinita

Per impostazione predefinita, il file ibmproxy.conf contiene le seguenti definizioni per la direttiva AccessLogExcludeUserAgent:

```
AccessLogExcludeUserAgent IBM_Network_Dispatcher_HTTP_Advisor
AccessLogExcludeUserAgent IBM_Network_Dispatcher_WTE_Advisor
```

Gli agenti utente sopra elencati sono quelli definiti per determinati advisor Load Balancer che normalmente si trovano davanti al server Caching Proxy. Per migliorare le prestazioni e ridurre il numero di operazioni di scrittura nel log, questi agenti utente non vengono registrati. Per impostazione predefinita, il server registra le richieste di accesso eseguite da tutti gli altri agenti utente.

AddBlankIcon — Indica di specificare l'URL dell'icona utilizzata per allineare le intestazioni degli elenchi directory

Utilizzare questa direttiva per specificare un'icona da utilizzare per allineare le intestazioni sugli elenchi directory restituiti quando il server funge da proxy per le richieste FTP. Le icone vengono visualizzate accanto ai file associati per aiutare gli utenti a distinguerli.

L'icona può essere vuota o meno, in base a quanto specificato sulle intestazioni degli elenchi directory. Per il corretto allineamento, l'icona deve utilizzare la stessa dimensione delle altre icone utilizzate sull'elenco directory.

Formato

`AddBlankIcon` *`URL_icona`* *`testo_alternativo`*

`URL_icona`

Specifica l'ultima parte dell'URL dell'icona. Il server aggiunge questo valore alla directory /icons/ per creare la richiesta URL completa. Se la richiesta è destinata a un file locale, il server la converte mediante le direttive di mappatura. Per poter richiamare l'icona, le direttive di mappatura devono consentire l'inoltro della richiesta.

Se il server viene utilizzato come proxy, la richiesta deve essere un URL completo che punta al server.

`testo_alternativo`

Specifica il testo alternativo da utilizzare per l'icona, se il browser richiedente non visualizza la grafica.

Esempio

```
AddBlankIcon logo.gif  logo
```

Impostazioni predefinite

- **Linux e UNIX:** `AddBlankIcon blank.m.pm.gif`
- **Windows:** `AddBlankIcon blank.gif`

Il valore predefinito non specifica testo alternativo poiché l'icona è vuota.

AddDirIcon — Indica di specificare l'URL dell'icona per le directory sugli elenchi directory

Utilizzare questa direttiva per specificare un'icona che rappresenta una directory su un elenco directory.

Formato

`AddDirIcon` *`URL_icona`* *`testo_alternativo`*

`URL_icona`

Specifica l'ultima parte dell'URL dell'icona. Il server aggiunge questo valore alla directory /icons/ per creare la richiesta URL completa. Se la richiesta è destinata a un file locale, il server la converte mediante le direttive di mappatura. Per poter richiamare l'icona, le direttive di mappatura devono consentire il trasferimento della richiesta.

Se il server viene utilizzato come proxy, la richiesta deve essere un URL completo che punta al server. È necessario mappare l'URL su un file locale e verificare che le direttive di mappatura consentano di trasferire l'URL.

testo_alternativo
Specifica il testo alternativo da utilizzare per l'icona, se il browser richiedente non visualizza la grafica.

Esempio

```
AddDirIcon  direct.gif  DIR
```

Impostazioni predefinite

- **Linux e UNIX:** `AddDirIcon dir.m.pm.gif  DIR`
- **Windows:** `AddDirIcon dir.gif DIR`

AddEncoding — Indica di specificare la codifica del contenuto MIME di file con particolari suffissi

Utilizzare questa direttiva per collegare i file con uno specifico suffisso a un tipo di codifica MIME. Questa direttiva viene utilizzata di rado.

Formato

```
AddEncoding .estensione  codifica
```

.estensione
Specifica il modello di suffisso file.

codifica
Specifica il tipo di codifica MIME che si intende associare ai file che corrispondono al modello di suffisso.

Esempio

```
AddEncoding .qp   quoted_printable
```

Impostazione predefinita

```
AddEncoding .Z  x-compress
```

AddIcon — Indica di associare un'icona a un tipo di codifica o di contenuto MIME

Utilizzare questa direttiva per specificare le icone per rappresentare i file con uno specifico tipo di codifica o di contenuto MIME. Il server utilizza le icone sugli elenchi directory, compresi elenchi directory FTP.

Formato

```
AddIcon URL_icona  testo_alternativo  maschera_tipo_MIME
```

URL_icona

Specifica l'ultima parte dell'URL dell'icona. Il server aggiunge questo valore alla directory /icons/ per creare la richiesta URL completa. Se la richiesta è destinata a un file locale, il server la converte mediante le direttive di mappatura. Per poter richiamare l'icona, le direttive di mappatura devono consentire il trasferimento della richiesta.

Se il server viene utilizzato come proxy, la richiesta deve essere un URL completo che punta al server. È necessario mappare l'URL su un file locale e verificare che le direttive di mappatura consentano di trasferire l'URL.

testo_alternativo
Specifica il testo alternativo da utilizzare per l'icona, se il browser richiedente non visualizza la grafica.

maschera_tipo
Specifica una maschera content-type o encoding-type MIME. Le maschere content-type contengono sempre una barra (/). Le maschere encoding-type non contengono mai barre.

Esempio

```
AddIcon   video_file.m.pm.gif    MOV    video/*
```

Impostazioni predefinite

Nel file di configurazione ibmproxy.conf sono impostati molti valori predefiniti per la direttiva AddIcon.

AddParentIcon — Indica di specificare l'URL dell'icona che rappresenta una directory parent su elenchi directory

Utilizzare questa direttiva per specificare un'icona che rappresenti una directory parent su elenchi directory.

Formato

```
AddParentIcon   URL_icona   testo_alternativo
```

URL-icona

Specifica l'ultima parte dell'URL dell'icona. Il server aggiunge questo valore alla directory /icons/ per creare la richiesta URL completa. Se la richiesta è destinata a un file locale, il server la converte mediante le direttive di mappatura. Per poter richiamare l'icona, le direttive di mappatura devono consentire il trasferimento della richiesta.

Se il server viene utilizzato come proxy, la richiesta deve essere un URL completo che punta al server. È necessario mappare l'URL su un file locale e verificare che le direttive di mappatura consentano di trasferire l'URL.

testo_alternativo
Specifica il testo alternativo da utilizzare per l'icona, se il browser richiedente non visualizza la grafica.

Esempio

```
AddParentIcon  parent.gif  UP
```

Impostazione predefinita

```
AddParentIcon   dir-up.gif    UP
```

AddType — Indica di specificare il tipo dati di file con particolari suffissi

Utilizzare questa direttiva per associare i file con uno specifico suffisso a un tipo e sottotipo MIME. È possibile disporre di più occorrenze di questa direttiva nel file di configurazione. Il server fornisce i valori predefiniti per i suffissi più utilizzati.

Formato

```
AddType .estensione tipo/sottotipo codifica
[qualità[ set_caratteri]]
```

.estensione
Il modello di suffisso file. È possibile utilizzare il carattere jolly (*) solo sui due tipi di suffissi speciali riportati di seguito:

. Tutti i nomi file che contengono il carattere punto (.) e che non sono soggetti ad altre regole.

***** Tutti i nomi file che non contengono il carattere punto (.) e che non sono soggetti ad altre regole.

tipo/sottotipo
Il tipo e il sottotipo MIME che si intende associare ai file che corrispondono al modello di suffisso.

codifica
La codifica del contenuto MIME a cui sono stati convertiti i dati. La codifica viene utilizzata anche da un server proxy FTP per determinare se il file viene richiamato in modalità binaria. Nella maggior parte dei casi, la codifica appropriata è `7bit`, `8bit` o `binaria` e viene determinata come di seguito:

7bit I dati vengono tutti rappresentati come righe di dati ASCII 8859-1 brevi (inferiori ai 1000 caratteri). Il file di codice sorgente e di testo rientrano in questa categoria. I file contenenti caratteri grafici o accentati rappresentano delle eccezioni.

8bit I dati vengono rappresentati come righe brevi ma possono contenere caratteri con un'elevata serie di bit (ad esempio, caratteri grafici o accentati). I file PostScript e di testo di siti europei rientrano in questa categoria.

binaria
Questa codifica può essere utilizzata per tutti i tipi di dati. I dati possono contenere non solo caratteri diversi da ASCII ma anche righe lunghe (superiori ai 1000 caratteri). Quasi tutti i file di tipo `image/*`, `audio/*` e `video/*` rientrano in questa categoria, come i file di dati binari di tipo `application/*`.

Ogni altro valore di codifica viene considerato come binario e trasferito alle intestazioni MIME come intestazione MIME content-encoding. La specifica a `7bit` e a `8bit` non viene inviata alle intestazioni MIME.

qualità
Specifica un indicatore opzionale di valore relativo (su una scala da 0,0 a 1,0) per il tipo di codifica. Il valore qualità viene utilizzato se una una richiesta confronta più rappresentazioni di un file. Il server seleziona il file associato al valore qualità più elevato. Ad esempio, se viene richiesto il file internet.ps e il server presenta le seguenti direttive AddType, allora il server utilizzerà la riga `application/postscript` poiché il valore qualità è il più alto.

```
AddType  .ps application/postscript  8bit  1.0
AddType  *.* application/binary   binary 0.3
```

set_caratteri
Un indicatore opzionale del set di caratteri che si intende associare ai file di testo. Per i file a cui viene assegnato un set di caratteri, il server indica ai browser client il set di caratteri da utilizzare quando si visualizza il file. Se si imposta un valore per il campo *set_caratteri*, è necessario includere anche un valore per il campo *qualità*.

Esempio

```
AddType .bin  application/octet-stream binary  0.8
```

Impostazioni predefinite

Molte impostazioni predefinite per la direttiva AddType sono contenute nel file di configurazione (ibmproxy.conf).

AddUnknownIcon — Indica di specificare l'URL dell'icona per tipi file sconosciuti sugli elenchi directory

Utilizzare questa direttiva per specificare un'icona che rappresenti un tipo file sconosciuto su un elenco directory.

Formato

```
AddUnknownIcon   URL_icona   testo_alternativo
```

URL_icona

Specifica l'ultima parte dell'URL dell'icona. Il server aggiunge questo valore a `/icons/` per creare la richiesta URL completa. Se la richiesta è destinata a un file locale, il server la converte mediante le direttive di mappatura. Per poter richiamare l'icona, le direttive di mappatura devono consentire il trasferimento della richiesta.

Se il server viene utilizzato come proxy, la richiesta deve essere un URL completo che punta al server. È necessario mappare l'URL su un file locale e verificare che le direttive di mappatura consentano di trasferire l'URL.

testo_alternativo
Specifica il testo alternativo da utilizzare per l'icona, se il browser richiedente non visualizza la grafica.

Esempio

```
AddUnknownIcon saywhat.gif  unknown
```

Impostazioni predefinite

- **Linux e UNIX:** `AddUnknownIcon  unknown.gif   ???`
- **Windows:** `AddUnknownIcon  unknown.gif   ???`

AdminPort — Indica di specificare la porta per richiedere moduli o pagine di amministrazione

Utilizzare questa direttiva per specificare una porta che può essere utilizzata dagli amministratori per accedere ai moduli di configurazione o alle pagine relative allo stato del server. Le richieste inviate a questa porta non vengono accodate insieme a tutte le altre richieste in entrata sulla porta (o porte) standard definita con la direttiva Port. Tuttavia, le richieste su AdminPort sono sottoposte alle stesse normali regole di controllo degli accessi e di mappatura delle richieste, ad esempio, Pass, Exec, Protect.

Nota: la porta di gestione *non* deve essere identica alla porta o alle porte standard definite con la direttiva Port.

Formato

```
AdminPort numero_porta
```

Esempio

```
AdminPort 2001
```

Impostazione predefinita

```
AdminPort 8008
```

AggressiveCaching — Indica di specificare la memorizzazione nella cache di file non memorizzabili nella cache

Utilizzare questa direttiva per specificare se i file restituiti dal server di origine e contrassegnati come non memorizzabili nella cache devono essere memorizzati comunque. I file non memorizzabili nella cache, memorizzati in base a queste direttive, sono contrassegnati come `must revalidate`. Ogni volta che il file viene richiesto, il server proxy invia una richiesta `If-Modified-Since` al server di origine per riconvalidare la risposta prima che questa possa essere supportata dalla cache. Attualmente, gli unici file non memorizzabili nella cache interessati da questa direttiva sono le risposte provenienti dal server di origine contenenti un'intestazione `cache-control: no-cache`. Questa direttiva può essere specificata più volte.

Formato

```
AggressiveCaching modello_url
```

Esempi

```
AggressiveCaching http://www.hosta.com/*
AggressiveCaching http://www.hostb.com/*
```

Per la compatibilità con le versioni precedenti, la sintassi di questa direttiva (`AggressiveCaching {on | off}`) viene ora trattata come segue:

`AggressiveCaching on` viene trattata come `AggressiveCaching * .`

`AggressiveCaching off` viene ignorata.

Nota: se si specifica sia `AggressiveCaching off` che `AggressiveCaching modello_url`, `AggressiveCaching off` viene ignorata e compare un messaggio di avvertenza.

Impostazione predefinita

Nessuna

AlwaysWelcome — Indica di specificare se ricercare la directory richiesta per i file di benvenuto

Per richieste contenenti un nome directory ma non un nome file, la direttiva AlwaysWelcome controlla se il server ricerca nella directory un file di benvenuto da restituire. Per impostazione predefinita, AlwaysWelcome è impostata su `on`. In altre parole, il server ricerca sempre nella directory richiesta un file che corrisponde a un nome specificato nella direttiva Welcome. In caso di corrispondenza, il file viene restituito al richiedente. Se il server riscontra più di una corrispondenza tra i file di una directory e i nomi file sulle direttive Welcome, l'ordine delle direttive Welcome determina quale file verrà restituito. Il server utilizza la direttiva Welcome più vicina all'inizio del file di configurazione.

Formato

```
AlwaysWelcome on | off
```

Impostazione predefinita

```
AlwaysWelcome on
```

Direttive correlate

• "Welcome — Indica di specificare i nomi dei file di benvenuto" a pagina 274

appendCRLFtoPost — Indica di aggiungere CRLF a richieste POST

Utilizzare questa direttiva per specificare gli URL per cui Caching Proxy aggiunge i caratteri di ritorno a capo e di avanzamento riga alla fine del corpo di una richiesta POST. Questa direttiva può essere specificata più volte.

Nota: specificare questa direttiva solo per gli URL che presentano un problema noto durante l'elaborazione delle richieste POST.

Formato

`appendCRLFtoPost` *`modello_url`*

Esempio

```
appendCRLFtoPost http://www.hosta.com/
```

Impostazione predefinita

Nessuna

ArrayName — Indica di denominare la matrice di cache remota

Utilizzare questa direttiva per specificare la matrice di cache remota che deve essere condivisa dai server.

Nota: durante l'impostazione di una matrice, configurare la direttiva Hostname in modo identico su tutti i membri della matrice.

Formato

`ArrayName` *`nome_matrice`*

Impostazione predefinita

Nessuna

Authentication — Indica di personalizzare la fase Autenticazione

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata che il server deve richiamare durante la fase Autenticazione del processo di richiesta server. Questo codice viene eseguito in base allo schema di autenticazione. È supportata esclusivamente l'autenticazione `BASIC`.

Nota: l'autenticazione fa parte del processo di autorizzazione e si verifica solo quando quest'ultima viene richiesta.

Formato

`Authentication` *`tipo /percorso/file`*`:`*`nome_funzione`*

`tipo`
Specifica uno schema di autenticazione che determina ulteriormente se la funzione applicativa viene richiamata. L'asterisco (`*`) e `BASIC` sono entrambi valori validi.

`/percorso/file`
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome da assegnare alla funzione applicativa all'interno del programma.

Esempio
```
Authentication BASIC /ics/api/bin/icsextpgm.so:basic_authentication
```

Impostazione predefinita
Nessuna

Authorization — Indica di personalizzare la fase Autorizzazione

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata richiamata dal server durante la fase Autorizzazione del processo di richiesta server. Questo codice verifica se l'oggetto richiesto può essere supportato per il client.

Formato
```
Authorization maschera_richiesta /percorso/file:nome_funzione
```

maschera_richiesta
Specifica una maschera per richieste che determina ulteriormente se la funzione applicativa viene chiamata. La specifica include il protocollo, il dominio e l'host; può essere preceduta da un carattere barra (/) ed è possibile utilizzare l'asterisco (*) come carattere jolly. Ad esempio, `/front_page.html`, `http://www.ics.raleigh.ibm.com`, `/pub*`, `/*` e `*` sono tutti validi. La maschera della richiesta deve cominciare dalla root del documento (/) quando si utilizza Caching Proxy come proxy inverso.

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome da assegnare alla funzione applicativa all'interno del programma.

Esempio
```
Authorization /index.html /api/bin/icsextpgm.so:auth_url
```

Impostazione predefinita
Nessuna

AutoCacheRefresh — Indica di specificare se utilizzare o meno l'aggiornamento cache

Utilizzare questa direttiva per attivare o disattivare l'aggiornamento cache. Se attivato, il contenuto della cache viene aggiornato automaticamente. In caso contrario, l'agente cache non viene richiamato, quindi tutte le relative impostazioni vengono ignorate. Se l'agente cache viene avviato da un altro metodo, ad esempio, utilizzando un lavoro **cron** su sistemi Linux e UNIX, impostare questa direttiva su `off`.

Formato
```
AutoCacheRefresh {on | off}
```

Impostazione predefinita

```
AutoCacheRefresh On
```

BindSpecific — Indica di specificare se il server è associato a uno o a tutti gli indirizzi IP

Utilizzare questa direttiva su un sistema multihome per specificare se il server è in ascolto su un solo indirizzo di rete. Se il valore viene impostato su `On`, il server viene associato all'indirizzo IP specificato nella direttiva Hostname, anziché a tutti gli indirizzi IP locali.

Se la direttiva non è specificata, il server viene associato al nome host predefinito.

Se la direttiva viene modificata, è necessario arrestare manualmente il server, quindi riavviarlo. La modifica non ha effetto se il server viene semplicemente riavviato. (Consultare Capitolo 5, "Avvio e arresto di Caching Proxy", a pagina 15.)

Formato

```
BindSpecific {on | off}  [OutgoingSrcIp indir_ip | nome_host]
```

[OutgoingSrcIp *indir_ip* | *nome_host***]**

Le opzioni OutgoingSrcIp consentono a Caching Proxy di utilizzare uno specifico indirizzo IP di origine quando si creano connessioni in uscita. Può essere utile per impostazioni Caching Proxy in DMZ e quando specifiche regole firewall lo richiedono.

Impostazione predefinita

```
BindSpecific Off
```

BlockSize — Indica di specificare la dimensione dei blocchi nella cache

Questa direttiva specifica la dimensione (in byte) dei blocchi nel supporto dell'unità di memorizzazione. Per impostazione predefinita, il valore è 8192. Dal momento che si tratta dell'unica dimensione supportata, non modificare questo valore. Per ulteriori informazioni, vedere la sezione di riferimento "comando htcformat" a pagina 160.

Formato

```
BlockSize dimensione
```

Impostazione predefinita

Per impostazione predefinita, non sono presenti impostazioni per BlockSize nel file di configurazione. (Il valore predefinito è 8192.)

CacheAccessLog — Indica di specificare il percorso ai file di log accessi cache

Utilizzare questa direttiva per specificare il percorso e il nome del file in cui il server deve memorizzare un log accessi alla cache proxy. Questa direttiva è valida solo se il server è in esecuzione come proxy. Per ulteriori informazioni, consultare "CacheRefreshTime — Indica di specificare quando avviare l'agente cache" a pagina 188.

Per attivare la registrazione delle richieste nella cache proxy, la direttiva Caching deve essere impostata su `ON` ed è necessario stabilire dei valori per le direttive

CacheMemory e CacheAccessLog. Facoltativamente, è possibile definire uno o più dispositivi cache utilizzando la direttiva CacheDev.

Il valore di CacheAccessLog può essere un percorso assoluto o relativo a ServerRoot. (Per ciascuno, è illustrato un esempio.)

Formato

```
CacheAccessLog  percorso/file
```

Esempi

```
CacheAccessLog  /absolute/path/logfile
CacheAccessLog  /logs/logfile
```

Impostazioni predefinite

- **Sistemi Linux e UNIX:** `CacheAccessLog /opt/ibm/edge/cp/server_root/logs/cache`
- **Sistemi Windows:** `CacheAccessLog drive:\Programmi\IBM\edge\cp\logs\cache`

CacheAlgorithm — Indica di specificare l'algoritmo cache

Utilizzare questa direttiva per specificare l'algoritmo cache utilizzato dal server durante la raccolta di dati inutili.

Formato

```
CacheAlgorithm  {bandwidth | responsetime | blend}
```

bandwidth
Tenta di risparmiare al massimo la larghezza di banda della rete.

responsetime
Tenta di ridurre al minimo il tempo di risposta utente.

blend
Utilizza una combinazione bilanciata di `bandwidth` e `responsetime`.

Impostazione predefinita

`Larghezza di banda CacheAlgorithm`

CacheByIncomingUrl — Indica di specificare la base per la creazione di nomi file di cache

Utilizzare questa direttiva per specificare se i nomi file di cache creati si basano sull'URL in entrata della richiesta.

Se questa direttiva è impostata su `on`, i nomi file di cache vengono creati in base all'URL in entrata. Se questa direttiva è impostata su `off`, l'URL in entrata passerà innanzitutto attraverso tutti i plugin di conversione nome adatti, regole MAP e regole PROXY, quindi il nome file di cache generato sarà basato sull'URL risultante.

Nota: quando si definiscono i filtri cache, in uno scenario con proxy inverso per filtri cache basati su URL, utilizzare un formato che comincia con una root documento di tipo / (barra rovesciata). Ad esempio: `/test/index.html`. Il formato *non* dovrebbe contenere protocolli, ad esempio, *http://*.

Formato

```
CacheByIncomingUrl {on | off}
```

Impostazione predefinita

```
CacheByIncomingURL off
```

CacheClean — Indica di specificare per quanto tempo conservare i file memorizzati nella cache

Utilizzare questa direttiva per specificare per quanto tempo il server deve conservare i file memorizzati nella cache. Durante l'esecuzione della raccolta di dati inutili, il server elimina i file memorizzati nella cache che hanno oltrepassato questo valore, indipendentemente dalla data di scadenza. Ogni volta che viene richiesto un file conservato nella cache per un periodo superiore a quello specificato, il server deve riconvalidarlo per verificare che sia valido, prima di poterlo utilizzare.

Formato

```
CacheClean  specifica_durata
```

Esempio

```
CacheClean 2 weeks
```

Impostazione predefinita

```
CacheClean 1 month
```

CacheDefaultExpiry — Indica di specificare la scadenza predefinita dei file

Utilizzare questa direttiva per impostare una scadenza predefinita per i file per cui il server non ha fornito un'intestazione `Expires` o `Last-Modified`. Specificare una maschera URL e la scadenza dei file che presentano URL corrispondenti alla maschera. È possibile includere più occorrenze di questa direttiva nel file di configurazione. Includere una direttiva separata per ciascuna maschera. La maschera URL deve contenere il protocollo. Per specificare la scadenza, può essere utilizzata qualsiasi combinazione di mesi, settimane, giorni e ore.

Formato

```
CacheDefaultExpiry maschera_URL
data_scadenza
```

Impostazioni predefinite

```
CacheDefaultExpiry ftp:*  1 day
CacheDefaultExpiry gopher:*  2 days
CacheDefaultExpiry http:*  0 days
```

Nota: la scadenza predefinita del protocollo HTTP è `0 days`. Si consiglia di lasciare invariato questo valore poiché molti programmi script non forniscono la data di scadenza e il relativo output scade subito. Con un valore diverso da `0`, i client potrebbero visualizzare contenuto non aggiornato.

CacheDev — Indica di specificare un dispositivo di memorizzazione per la cache

Utilizzare questa direttiva per specificare un dispositivo di memorizzazione cache. È possibile specificare un file o una partizione su disco non formattata. Su piattaforme AIX, è possibile specificare un volume logico non formattato. (Se non si utilizza una cache in memoria, la memorizzazione nella cache su disco non formattato assicura le migliori prestazioni.)

Notare che è necessario predisporre i dispositivi cache prima di specificarli. Per predisporre un dispositivo cache, formattarlo per mezzo del comando **htcformat**. Per ulteriori informazioni, vedere “comando htcformat” a pagina 160.

È possibile specificare più dispositivi cache. Ciascun dispositivo viene associato agli stessi valori CacheMemory e BlockSize. Tuttavia, ciascuno di essi va incontro a un sovraccarico di memoria di circa 8 MB nella macchina server proxy. Un numero minore di dispositivi di grandi dimensioni è sicuramente più efficiente di un numero maggiore di dispositivi di dimensioni più piccole. Per ottenere il massimo dell'efficienza, utilizzare un disco intero come unica grande partizione e nient'altro. Per ulteriori informazioni sulla memorizzazione nella cache, consultare “Ottimizzazione delle prestazioni della cache su disco” a pagina 105.

Formato

```
CacheDev  {partizione_disco_nonformattata |
file}
```

Esempi

AIX: `CacheDev /dev/rlv02`

HP-UX: `CacheDev /dev/rdsk/c1t15d0`

Linux: `CacheDev /opt/IBMWTE/filecache1`

Solaris: `CacheDev /dev/rdsk/c1t3d0s0`

Windows: `CacheDev \\.\E:`

Impostazioni predefinite

Nessuna

CacheExpiryCheck — Indica di specificare se il server restituisce file scaduti

Utilizzare questa direttiva per specificare se il server restituisce file memorizzati nella cache scaduti. Impostare questo valore su `Off` per fare in modo che il server possa restituire file scaduti. Utilizzare il valore predefinito `On` se un client richiede un file scaduto e si desidera che il proxy controlli che nel server di origine sia disponibile una versione più aggiornata del file stesso. Generalmente, gli amministratori non desiderano che il server restituisca file scaduti se non durante una dimostrazione, in cui il contenuto non è importante.

Formato

```
CacheExpiryCheck {on | off}
```

Impostazioni predefinite

```
CacheExpiryCheck On
```

CacheFileSizeLimit — Indica di specificare la dimensione massima dei file da memorizzare nella cache

Utilizzare questa direttiva per specificare la dimensione massima dei file da memorizzare nella cache. I file la cui dimensione supera questo valore non verranno memorizzati. Il valore può essere specificato in byte (B), kilobyte (K), megabyte (M) o gigabyte (G). La specifica può contenere o meno spazi tra il numero e l'unità di misura (B, K, M, G).

Formato

```
CacheFileSizeLimit dimensione massima {B
| K | M
| G}
```

Impostazione predefinita

```
CacheFileSizeLimit 4000 K
```

CacheLastModifiedFactor — Indica di specificare il valore per determinare le date di scadenza

Utilizzare questa direttiva per specificare il valore da adoperare per calcolare le date di scadenza di determinati URL o di tutti gli URL corrispondenti a una maschera.

Di frequente, i server HTTP forniscono la data/ora dell'ultima modifica ma non la data di scadenza. Allo stesso modo, i file FTP possono indicare la data/ora dell'ultima modifica ma non la data di scadenza. Caching Proxy calcola una data di scadenza per questi file in base alla data/ora dell'ultima modifica. Quest'ultima viene utilizzata per determinare il tempo trascorso dall'ultima modifica al file, che viene poi moltiplicato per il valore su una direttiva CacheLastModifiedFactor. Il risultato di questo calcolo indica la durata del file o l'intervallo di tempo prima che il file diventi obsoleto.

È anche possibile specificare `off` o `-1` per disattivare la direttiva e non calcolare la data di scadenza. Il server proxy legge le direttive CacheLastModifiedFactor nell'ordine in cui compaiono nel file di configurazione e utilizza la prima direttiva applicabile al file memorizzato nella cache.

Formato

```
CacheLastModifiedFactor url fattore
```

url
: Specifica l'URL completo, incluso il protocollo, del file da memorizzare nella cache. È possibile utilizzare una maschera URL con asterischi (*) come caratteri jolly, per applicare una maschera.

fattore
: Specifica il fattore da utilizzare nel calcolo. È inoltre possibile specificare i valori `off` o `-1`.

Esempi

```
CacheLastModifiedFactor  *://hosta/*    off
CacheLastModifiedFactor  ftp://hostb/*  0.30
CacheLastModifiedFactor  ftp://*        0.25
CacheLastModifiedFactor  http://*       0.10
CacheLastModifiedFactor  *              0.50
```

Impostazioni predefinite

```
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
```

Con il valore predefinito 0.14, i file modificati una settimana fa scadranno in un giorno.

CacheLocalDomain — Indica di specificare se memorizzare nella cache il dominio locale

Utilizzare questa direttiva per specificare se memorizzare nella cache gli URL degli host nello stesso dominio del proxy. Normalmente, i siti locali su una rete intranet non devono essere memorizzati nella cache, in quanto la larghezza di banda interna è sufficiente a caricare gli URL velocemente. Se i siti locali non vengono memorizzati nella cache sarà possibile risparmiare lo spazio per quegli URL che impiegano più tempo per essere richiamati.

Formato

```
CacheLocalDomain {on | off}
```

Impostazione predefinita

```
CacheLocalDomain on
```

CacheMatchLanguage — Indica di specificare la preferenza lingua per il contenuto cache restituito

Se il server di backend può restituire ai clienti le varianti lingua dello stesso URL, utilizzare questa direttiva per supportare la memorizzazione nella cache delle varie lingue del medesimo URL. La direttiva consente a Caching Proxy di verificare la preferenza lingua nelle richieste con la lingua della risposta memorizzata nella cache.

Quando si attiva CacheMatchLanguage, prima che Caching Proxy carichi il contenuto memorizzato nella cache, viene visualizzata la preferenza lingua nell'intestazione Accept-Language della richiesta, in cui compare la lingua del contenuto memorizzato nella cache. Caching Proxy confronta inoltre la distanza tra le preferenze. Se questa è inferiore al limite specificato, restituisce la copia memorizzata nella cache; in caso contrario, il proxy inoltra la richiesta al server di backend per ottenere una copia aggiornata nella lingua richiesta.

Formato

```
CacheMatchLanguage {on | off}
limite-distanza-lingua-preferenza
id-speciale-per-tutte-le-lingue
```

limite-distanza-lingua-preferenza
Specificare un valore compreso nell'intervallo 0.001 – 0.9999.

id-speciale-per-tutte-le-lingue
Specificare una stringa di lingua restituita dal server nell'intestazione Content-Language per comunicare al proxy che la risposta può essere utilizzata per tutte le preferenze lingua.

Esempi

Di seguito è riportato un esempio di configurazione della direttiva, dell'oggetto cache e della richiesta.

```
CacheMatchLanguage On 0.2
```

Se l'oggetto cache è in cinese semplificato (zh_cn) e la richiesta è:

```
GET / HTTP/1.1
...
Accept-Language: en_US;q=1.0, zh_cn;q=0.7, ja;q=0.3
....
```

Per questa richiesta, il cliente chiede una pagina in inglese (con codice e qualità en_US/1.0), quindi in cinese semplificato (con codice e qualità zh_cn/0.7), infine in giapponese (con codice e qualità ja/0.3). L'oggetto memorizzato nella cache è in cinese semplificato. La distanza tra le preferenze tra la migliore qualità prevista e la qualità della lingua corrispondente è 1.0 - 0.7 = 0.3. Poiché il limite è impostato su 0.2 dalla direttiva CacheMatchLanguage e 0.3 è superiore al limite, il proxy chiede al server una nuova copia di quell'URL invece di restituire l'oggetto memorizzato nella cache.

Quando il server restituisce una risposta, se non specifica una lingua o un id-speciale-per-tutte-le-lingue nell'intestazione Content-Language, nel momento in cui arriva un'altra richiesta, il proxy non esegue il confronto con la preferenza lingua e restituisce la copia memorizzata nella cache.

Impostazione predefinita

```
CacheMatchLanguage off
```

CacheMaxExpiry — Indica di specificare la durata massima per i file memorizzati nella cache

Utilizzare questa direttiva per definire l'intervallo di tempo massimo in cui i file possono rimanere nella cache. La durata di un file memorizzato nella cache definisce l'intervallo di tempo entro il quale il file può essere supportato dalla cache senza che l'origine venga controllata per verificare la presenza di eventuali aggiornamenti. In alcuni casi, la durata calcolata per un file memorizzato nella cache può essere superiore rispetto a quella desiderata per la conservazione del file. La durata del file, specificata dall'origine o calcolata da Caching Proxy, non può superare il limite specificato dalla direttiva CacheMaxExpiry.

Sono consentite più occorrenze di questa direttiva nel file di configurazione. Includere una direttiva separata per ciascuna maschera.

Formato

```
CacheMaxExpiry URL durata
```

URL
: Specifica l'URL completo, incluso il protocollo, del file da memorizzare nella cache. È possibile utilizzare una maschera URL con asterischi (*) come caratteri jolly, per applicare una maschera.

durata
: Specifica la durata massima dei file memorizzati nella cache che corrispondono alla maschera URL. La durata può essere specificata in una qualsiasi combinazione di mesi, settimane, giorni, ore, minuti o secondi.

Esempi

```
CacheMaxExpiry ftp:* 1 month
CacheMaxExpiry http://www.santaclaus.np/* 2 days 12 hours
```

Impostazione predefinita

```
CacheMaxExpiry 1 month
```

CacheMemory — Indica di specificare la RAM cache

Utilizzare questa direttiva per specificare la quantità di memoria da associare alla cache. Per ottenere prestazioni ottimali delle cache su disco, è consigliabile un valore di memoria cache minimo di 64 MB per il supporto dell'infrastruttura cache, incluso l'indice di cache. Con l'aumento della dimensione di cache, aumenta anche l'indice di cache e, di conseguenza, è necessaria più memoria per memorizzare l'indice. Un valore di memoria cache di 64 MB è sufficiente per supportare l'infrastruttura cache e memorizzare un indice di cache di una cache su disco con una dimensione di circa 6,4 GB. Per cache su disco di dimensioni superiori, la memoria cache deve essere l'1% della dimensione cache.

Se si utilizza la cache in memoria, impostare questa direttiva per includere sia la cache che la quantità di memoria necessaria per l'indice cache.

Il valore massimo consigliato per questa direttiva è 1600 MB. Questo limite è determinato dal fatto che Caching Proxy, come applicazione a 32 bit, può utilizzare al massimo 2 GB di memoria. Se la quantità di memoria necessaria per la cache sommata a quella utilizzata per l'elaborazione di routine si avvicina o supera i 2 GB, Caching Proxy non funzionerà correttamente.

La quantità può essere specificata in una delle seguenti unità: byte (B), kilobyte (K), megabyte (M) e gigabyte (G).

Formato

```
CacheMemory quantità {B | K | M | G}
```

Impostazioni predefinite

```
CacheMemory 64 M
```

CacheMinHold — Indica di specificare l'intervallo di tempo entro il quale i file saranno disponibili

Utilizzare questa direttiva per specificare gli URL dei file la cui scadenza deve essere ignorata. Alcuni siti impostano la scadenza dei file prima del termine della loro validità e, così facendo, il server deve richiedere il file più di frequente. La direttiva CacheMinHold consente di conservare nella cache il file scaduto per l'intervallo di tempo specificato prima che venga nuovamente richiesto. Questa direttiva può essere specificata più volte.

Nota: se le date di scadenza vengono ignorate, i file nella cache possono diventare obsoleti o non aggiornati.

Esempio

```
CacheMinHold http://www.cachebusters.com/* 1 hour
```

Impostazione predefinita

Nessuna

CacheNoConnect — Indica di specificare la modalità cache autonoma

Utilizzare questa direttiva per specificare se il server proxy richiama i file da server remoti. Il valore predefinito (`Off`) consente al server di richiamare i file da server remoti. Il valore `On` fa sì che il server venga eseguito in modalità cache autonoma. In questo modo, il server può restituire esclusivamente i file già memorizzati nella

cache. Normalmente, quando il server viene eseguito in questa modalità, è anche possibile impostare la direttiva CacheExpiryCheck su `Off`.

L'esecuzione del server in modalità cache autonoma può essere utile quando si utilizza il server a scopo dimostrativo. Se tutti i file da utilizzare per la dimostrazione sono memorizzati nella cache, non è necessaria una connessione di rete.

Formato

```
CacheNoConnect  {on | off}
```

Impostazione predefinita

```
CacheNoConnect Off
```

CacheOnly — Indica di memorizzare solo i file con gli URL corrispondenti a una maschera

Utilizzare questa direttiva per specificare di memorizzare nella cache solo i file con URL corrispondenti a una maschera specificata. È possibile utilizzare più occorrenze di questa direttiva nel file di configurazione. Includere una direttiva separata per ciascuna maschera. La maschera URL deve contenere il protocollo. Se per questa direttiva non è impostato alcun valore, è possibile memorizzare nella cache qualsiasi URL che non corrisponde a una direttiva NoCaching. Se le direttive CacheOnly e NoCaching non sono incluse nel file di configurazione, è possibile memorizzare nella cache qualsiasi URL.

Formato

`CacheOnly` *`modello_url`*

Esempio

```
CacheOnly http://realstuff/*
```

Impostazione predefinita

Nessuna

CacheQueries — Indica di specificare le risposte cache agli URL contenenti un carattere punto interrogativo (?)

Utilizzare questa direttiva per specificare gli URL per cui le risposte alle richieste di query sono state memorizzate nella cache. Se viene utilizzato il valore `PUBLIC` *`modello_url`*, le risposte a richieste GET che contengono un carattere punto interrogativo nell'URL vengono memorizzate nella cache se il server di origine contiene l'intestazione `cache-control: public` e la risposta è comunque memorizzabile nella cache. Se viene specificato il valore `ALWAYS`*`modello_url`*, le risposte a richieste GET che contengono un carattere punto interrogativo nell'URL vengono memorizzate nella cache se le risposte sono comunque memorizzabili.

Questa direttiva può essere specificata più volte.

```
CacheQueries {ALWAYS | PUBLIC}
modello_url
```

Esempi

```
CacheQueries ALWAYS http://www.hosta.com/*
CacheQueries PUBLIC http://www.hostb.com/*
```

Nota: Per compatibilità con le versioni precedenti, la sintassi `CacheQueries {ALWAYS | PUBLIC | NEVER}` viene considerata come segue:

- `CacheQueries ALWAYS` e `CacheQueries PUBLIC` vengono considerati come `CacheQueries ALWAYS * e CacheQueries PUBLIC *`.
- `CacheQueries NEVER` viene ignorato.
- Se si specifica sia `CacheQueries NEVER` che `CacheQueries` *`modello_url`*, `CacheQueries NEVER` viene ignorato ma compare un messaggio di avvertenza.

Impostazione predefinita
Nessuna

CacheRefreshInterval — Indica di specificare l'intervallo di tempo per riconvalidare gli oggetti memorizzati nella cache

Utilizzare questa direttiva per specificare quando verificare il server di origine per determinare se i file memorizzati nella cache sono stati modificati.

Sebbene la direttiva CacheClean sembra simile a questa, c'è una differenza. CacheRefreshInterval specifica solo che il proxy riconvalida un file prima di utilizzarlo mentre la direttiva CacheClean consente di eliminare il file dalla cache dopo un determinato periodo di tempo.

Formato
- Il formato riportato di seguito specifica l'intervallo di aggiornamento per i file corrispondenti al modello URL:

  ```
  CacheRefreshInterval
  modello_URL periodo_tempo
  ```

- Il formato riportato di seguito specifica l'intervallo di aggiornamento per i file che *non* corrispondono a un modello URL. È specificato solo un intervallo di aggiornamento.

  ```
  CacheRefreshInterval
  periodo_tempo
  ```

Esempi
```
CacheRefreshInterval *.gif 8 hours
CacheRefreshInterval 1 week
```

Impostazione predefinita
```
CacheRefreshInterval 2 weeks
```

CacheRefreshTime — Indica di specificare quando avviare l'agente cache

Utilizzare questa direttiva per specificare quando avviare l'agente cache. È possibile avviare l'agente cache in uno specifico momento.

Formato
`CacheRefreshTime` *`HH:MM`*

Impostazioni predefinite
```
CacheRefreshTime 03:00
```

CacheTimeMargin — Indica di specificare la durata minima per la memorizzazione di un file nella cache

La direttiva CacheTimeMargin specifica la durata minima di un file necessaria per memorizzarlo nella cache.

Caching Proxy calcola una data di scadenza per ciascun file. Se si ritiene improbabile di ricevere un'altra richiesta per il file prima che questo raggiunga la data di scadenza, Caching Proxy considera la durata del file insufficiente per poterlo memorizzare. Per impostazione predefinita, Caching Proxy non memorizza nella cache i file la cui durata è inferiore ai 10 minuti. Se la cache non è prossima alla propria capacità massima, lasciare questa direttiva al valore iniziale. Se la cache ha quasi raggiunto la capacità totale, aumentare il valore della durata minima.

Formato

```
CacheTimeMargin durata_minima
```

Impostazioni predefinite

```
CacheTimeMargin 10 minutes
```

Nota: se si imposta questa direttiva su un valore superiore alle quattro ore, l'efficienza della cache si riduce significativamente.

CacheUnused — Indica di specificare per quanto tempo conservare nella cache i file non utilizzati

Utilizzare questa direttiva per impostare l'intervallo di tempo massimo entro il quale il server deve conservare nella cache i file non utilizzati che presentano URL che corrispondono a una maschera specificata. Il server elimina i file non utilizzati, che presentano URL corrispondenti alla maschera, dopo averli conservati nella cache per un determinato periodo di tempo, indipendentemente dalla data di scadenza. È possibile includere più occorrenze di questa direttiva nel file di configurazione. Includere una direttiva separata per ciascuna maschera. La maschera URL deve contenere il protocollo. Per specificare la scadenza, può essere utilizzata qualsiasi combinazione di mesi, settimane, giorni e ore.

Formato

```
CacheUnused maschera_url
intervallo_tempo
```

Esempi

```
CacheUnused ftp:* 3 weeks
CacheUnused gopher:* 3 days 12 hours
CacheUnused * 4 weeks
```

Impostazioni predefinite

```
CacheUnused ftp:* 3 days
CacheUnused gopher:* 12 hours
CacheUnused http:* 2 days
```

Caching — Indica di abilitare la cache del proxy

Utilizzare questa direttiva per abilitare la memorizzazione dei file nella cache. Se la memorizzazione nella cache è attivata, il server proxy memorizza i file che richiama da altri server in una cache locale. Il server proxy quindi risponde alle successive richieste per gli stessi file senza doverli richiamare da altri server.

Formato

```
Caching {on | off}
```

Impostazione predefinita

```
Caching On
```

Nota: se si modifica la direttiva Caching, è necessario arrestare manualmente il server, quindi riavviarlo. (Consultare Capitolo 5, "Avvio e arresto di Caching Proxy", a pagina 15.)

CdfAware — Indica di designare questa istanza di Caching Proxy come parte di Content Distribution Framework

Utilizzare questa direttiva per specificare se Caching Proxy fa parte di Content Distribution Framework.

Formato

```
CdfAware {yes | no}
```

Impostazione predefinita

```
CdfAware no
```

CdfRestartFile — Indica di specificare il file per memorizzare una mappatura nome file-url

Utilizzare questa direttiva per designare il nome del file su cui memorizzare i dati della mappatura nome file-URL in modo che siano permanenti su più istanze di ibmproxy in Content Distribution Framework. Caching Proxy conserva una tabella mappatura che associa un URL richiesto al nome file corrispondente sul server Web. Questo file fornisce una memoria permanente di questa tabella a ogni operazione di riavvio. Utilizzare questa direttiva solo se la direttiva CdfAware è impostata su `yes`.

Formato

```
CdfRestartFile percorso/nomefile
```

Esempio

- **Linux e UNIX:** `CdfRestartFile /opt/ibm/edge/cd/cdfRestartFile`
- **Windows:** `CdfRestartFile C:\progra~1\ibm\edge\cd\cdfRestartFile.txt`

Impostazione predefinita

Nessuna

CompressAge — Indica di specificare quando comprimere i log

Utilizzare questa direttiva per specificare la durata oltre la quale i log vengono compressi. I log vengono compressi quando la relativa durata supera il valore impostato per CompressAge. Se CompressAge è impostato su `0`, i log non vengono mai compressi. I log del giorno precedente e seguente non vengono mai compressi.

Formato

```
CompressAge numero_di_giorni
```

Impostazione predefinita

```
CompressAge 1
```

Direttive correlate

- "CompressDeleteAge — Indica di specificare quando eliminare i log" a pagina 192
- "CompressCommand — Indica di specificare il comando di compressione e i parametri" a pagina 191

- "LogArchive — Indica di specificare il funzionamento dell'archiviazione log" a pagina 223
- "Midnight — Indica di specificare il plugin dell'API utilizzato per archiviare i log" a pagina 229
- "PurgeAge — Indica di specificare la durata di un log" a pagina 252
- "PurgeSize — Indica di specificare il limite della dimensione dell'archivio log" a pagina 253

CompressCommand — Indica di specificare il comando di compressione e i parametri

Utilizzare questa direttiva per creare un comando che identifichi il programma di utilità di compressione utilizzato per comprimere i log e che trasferisca i parametri a quel programma di utilità. Includere il percorso ai log archiviati.

Il programma di utilità di compressione deve essere installato in una directory elencata nel percorso di quella macchina.

Formato

`CompressCommand` *comando*

comando
Include il comando e i parametri che si intende utilizzare, immessi in una sola riga. Normalmente, tra i parametri sono inclusi `%%LOGFILES%%` e `%%DATE%%`.

`%%LOGFILES%%`
Specifica l'elenco dei file di log disponibili per uno specifico parametro `%%DATE%%`.

`%%DATE%%`
Specifica la data/ora su un file di log.

Esempi

- **Linux e 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: il comando e tutti i parametri devono essere specificati su una sola riga. Nei primi due esempi riportati in precedenza, i comandi sono stati divisi per facilitarne la lettura.

- **Windows:**

```
CompressCommand pkzip -q d:\logarchs\log%%DATE%%.tar  %%LOGFILES%%
```

Impostazione predefinita

Nessuna

Direttive correlate

- "CompressAge — Indica di specificare quando comprimere i log" a pagina 190
- "CompressDeleteAge — Indica di specificare quando eliminare i log" a pagina 192
- "LogArchive — Indica di specificare il funzionamento dell'archiviazione log" a pagina 223

- "Midnight — Indica di specificare il plugin dell'API utilizzato per archiviare i log" a pagina 229
- "PurgeAge — Indica di specificare la durata di un log" a pagina 252
- "PurgeSize — Indica di specificare il limite della dimensione dell'archivio log" a pagina 253

CompressDeleteAge — Indica di specificare quando eliminare i log

Utilizzare questa direttiva per specificare quando eliminare un log in seguito a compressione. Un log viene eliminato quando la relativa durata ha superato il numero di giorni impostato per il valore di CompressDeleteAge. Se CompressDeleteAge è impostato su `0` o se il valore è inferiore a quello impostato per la direttiva CompressAge, il log non viene eliminato.

Nota: il plugin di compressione non elimina mai i log del giorno corrente o precedente.

Formato

```
CompressDeleteAge numero_di_giorni
```

Impostazione predefinita

```
CompressDeleteAge 7
```

Direttive correlate

- "CompressAge — Indica di specificare quando comprimere i log" a pagina 190
- "CompressCommand — Indica di specificare il comando di compressione e i parametri" a pagina 191
- "LogArchive — Indica di specificare il funzionamento dell'archiviazione log" a pagina 223
- "Midnight — Indica di specificare il plugin dell'API utilizzato per archiviare i log" a pagina 229
- "PurgeAge — Indica di specificare la durata di un log" a pagina 252
- "PurgeSize — Indica di specificare il limite della dimensione dell'archivio log" a pagina 253

ConfigFile — Indica di specificare il nome di un file di configurazione aggiuntivo

Utilizzare questa direttiva per specificare il nome e il percorso di un file di configurazione aggiuntivo. Le direttive presenti nel file di configurazione specificato vengono elaborate dopo il file di configurazione corrente.

Nota: assicurarsi che il file di configurazione aggiuntivo disponga dell'autorizzazione alla `lettura` per l'utente `nobody`, per consentire all'agente cache di leggere il file.

Esempi

- **Linux e UNIX:** `ConfigFile /etc/rca.conf`
- **Windows:** `ConfigFile c:\WINNT\rca.conf`

Impostazione predefinita

Nessuna

ConnThreads — Indica di specificare il numero di thread di connessione da utilizzare per la gestione delle connessioni

Utilizzare questa direttiva per definire il numero di thread di connessione da utilizzare per la gestione delle connessioni.

Formato

```
ConnThreads numero
```

Impostazione predefinita

```
ConnThreads 5
```

Direttive correlate

- "MaxActiveThreads — Indica di specificare il numero massimo di thread attivi" a pagina 226

ContinueCaching — Indica di specificare la parte di un file necessaria per la memorizzazione nella cache

Utilizzare questa direttiva per specificare la parte di un file necessario che deve essere trasferita per consentire a Caching Proxy di completare la creazione del file di cache, anche se la connessione client è stata chiusa. I valori validi per questa variabile sono numeri interi compresi nell'intervallo 0 – 100.

Ad esempio, se si specifica `ContinueCaching 75`, Caching Proxy continua a trasferire il file dal server di contenuti e genera il file di cache se almeno il 75% del file è stato trasferito prima che Caching Proxy si accorga che la connessione client è terminata.

Formato

```
ContinueCaching percentuale
```

Impostazione predefinita

```
ContinueCaching 75
```

DefinePicsRule — Indica di fornire una regola content-filtering

Utilizzare questa direttiva per fornire al proxy le informazioni necessarie per filtrare il contenuto degli URL, comprese le informazioni sul servizio di restrizione. È possibile utilizzare questa direttiva più volte.

Formato

```
DefinePicsRule "nome_filtro"  {
```

Impostazione predefinita

```
DefinePicsRule "RSAC Example" {
```

DefProt — Indica di specificare un'impostazione di protezione predefinita per le richieste che corrispondono a una maschera

Utilizzare questa direttiva per associare un'impostazione di protezione predefinita alle richieste che corrispondono a un modello.

Nota: per far funzionare correttamente la protezione, le direttive DefProt e Protect devono essere posizionate prima di qualsiasi direttiva Pass o Exec nel file di configurazione.

Formato

```
DefProt maschera_richiesta  nome_impostazione [FOR
indirizzo_IP_server | nome_host]
```

maschera_richiesta
Specifica una maschera per le richieste da associare a un'impostazione di protezione predefinita. Il server confronta le richieste client in entrata con la maschera e, in caso di corrispondenza, associa un'impostazione di protezione.

La protezione non è attualmente attivata per le richieste che corrispondono alla maschera, a meno che la richiesta non corrisponda anche a una maschera su una successiva direttiva Protect. Vedere "Protect — Indica di attivare un'impostazione di protezione predefinita per le richieste che corrispondono a una maschera" a pagina 240 per una spiegazione sull'uso della direttiva Protect con DefProt.

setup
L'impostazione di protezione denominata, definita nel file di configurazione, che si intende associare alle richieste che corrispondono a *maschera_richiesta*. L'impostazione di protezione viene definita con sottodirettive di protezione. Questo parametro può assumere uno dei tre formati riportati di seguito:

- Un percorso completo e un nome file che specificano un file separato contenente le sottodirettive di protezione.
- Un nome etichetta impostazione di protezione che corrisponde a un nome precedentemente definito su una direttiva Protection. La direttiva Protection contiene le sottodirettive di protezione.
- Le sottodirettive di protezione effettive. Le sottodirettive vanno racchiuse tra parentesi ({}). Il carattere parentesi sinistra deve essere l'ultimo carattere sulla stessa riga della direttiva DefProt. Ciascuna sottodirettiva deve proseguire sulla propria riga. Il carattere parentesi destra deve trovarsi sulla propria riga, di seguito alla riga dell'ultima sottodirettiva. Tra le parentesi non sono consentite righe di commenti. Per le descrizioni delle sottodirettive di protezione, consultare:
  - "AuthType — Indica di specificare il tipo di autenticazione" a pagina 245
  - "DeleteMask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a eliminare i file" a pagina 245
  - "GetMask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a richiamare i file" a pagina 245
  - "GroupFile — Indica di specificare la posizione del file gruppo associato" a pagina 245
  - "Mask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a eseguire richieste HTTP" a pagina 246
  - "PasswdFile — Indica di specificare la posizione del file di password associato" a pagina 246
  - "PostMask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a inviare i file" a pagina 246
  - "PutMask — Indica di specificare i nomi degli utenti, i gruppi e gli indirizzi autorizzati a inserire file" a pagina 246
  - "ServerID — Indica di specificare un nome da associare al file di password" a pagina 247

[FOR *indirizzo_IP_server* | *nome_host*]
se si utilizzano più indirizzi IP o host virtuali, utilizzare questo parametro per specificare un indirizzo IP o un nome host. Il server utilizza la direttiva esclusivamente per le richieste inviate al server su questo indirizzo IP o per

questo host. Per un indirizzo IP, si tratta dell'indirizzo della connessione di rete del server e non dell'indirizzo del client richiedente.

È possibile specificare un indirizzo IP (ad esempio, `FOR 240.146.167.72`) o un nome host (ad esempio, `FOR hostA.bcd.com`).

Questo parametro è opzionale. Senza questo parametro, il server utilizza la direttiva per tutte le richieste a prescindere dall'indirizzo IP su cui è stata ricevuta la richiesta o dal nome host nell'URL.

Note:

1. È possibile utilizzare questo parametro solo con il parametro *setup*, specificato sotto forma di percorso e nome file o etichetta impostazione di protezione. Non è possibile utilizzare questo parametro con il parametro *setup* specificato sotto forma di sottodirettive di protezione reali racchiuse tra parentesi.
2. Per utilizzare questo parametro, è necessario inserire `FOR` o alcune altre stringhe di caratteri (senza spazi), tra il parametro *setup* e l'*indirizzo_IP* o il *nome_host*.

Per un indirizzo IP del server non è possibile specificare un carattere jolly.

Nota: la direttiva deve essere specificata su una riga.

Esempi

- Nell'esempio riportato di seguito viene illustrato un file separato contenente le sottodirettive di protezione.

```
DefProt   /secret/* /server/protect/setup1.acc
```

- L'esempio riportato di seguito utilizza un nome etichetta per indicare le sottodirettive di protezione. Il nome etichetta deve corrispondere al nome etichetta su una direttiva Protection. La direttiva Protection deve precedere la direttiva DefProt.

```
DefProt   /secret/*   SECRET-PROT
```

- Nell'esempio riportato di seguito, le sottodirettive di protezione sono incluse come parte della direttiva DefProt.

```
DefProt   {
  AuthType Basic
  ServerID restricted
  PasswdFile /docs/etc/WWW/restrict.password
  GroupFile /docs/etc/WWW/restrict.group
  GetMask authors
  PutMask authors
  }
```

- Nell'esempio riportato di seguito viene utilizzato il parametro dell'indirizzo IP opzionale. Se il server riceve richieste che iniziano con `/secret/`, associa alla richiesta una differente impostazione di protezione predefinita, in base all'indirizzo IP della connessione di rete su cui è stata ricevuta la richiesta. Per le richieste ricevute su 0.67.106.79, il server associa la richiesta alla protezione predefinita stabilita su una direttiva Protection con un'etichetta `CustomerA-PROT`. Per le richieste ricevute su 0.83.100.45, il server associa la richiesta alla protezione predefinita stabilita su una direttiva Protection con un'etichetta `CustomerB-PROT`.

```
DefProt   /secret/*   CustomerA-PROT   0.67.106.79
DefProt   /secret/*   CustomerB-PROT   0.83.100.45
```

- Nell'esempio riportato di seguito viene utilizzato il parametro del nome host opzionale. Se il server riceve richieste che iniziano con `/secret/`, associa alla richiesta una differente impostazione di protezione predefinita, in base al nome

host nell'URL. Per le richieste ricevute su hostA, il server associa la richiesta alla protezione predefinita stabilita su una direttiva Protection con un'etichetta `CustomerA-PROT`. Per le richieste ricevute su hostB, il server associa la richiesta alla protezione predefinita stabilita su una direttiva Protection con un'etichetta `CustomerB-PROT`.

```
DefProt   /secret/*   CustomerA-PROT   hostA.bcd.com
DefProt   /secret/*   CustomerB-PROT   hostB.bcd.com
```

Impostazione predefinita

Nessuna

DelayPeriod — Indica di specificare un periodo di interruzione tra le richieste

Utilizzare questa direttiva per specificare se l'agente cache attende tra l'invio delle richieste al server di destinazione. Se si specifica un intervallo di tempo tra una richiesta e l'altra è possibile ridurre il carico sulla macchina proxy e sul collegamento di rete, oltre che sui server di destinazione. In caso contrario, l'agente cache sarà in esecuzione alla massima velocità. Per connessioni Internet a bassa velocità, è preferibile non specificare alcun intervallo per poter utilizzare al massimo la rete.

Nota: se la velocità di connessione a Internet è superiore a 128 kbps, impostare DelayPeriod su `On` per evitare di inviare troppe richieste a una velocità estremamente sostenuta a siti in fase di aggiornamento.

Formato

```
DelayPeriod {on | off}
```

Impostazione predefinita

```
DelayPeriod On
```

DelveAcrossHosts — Consente di specificare la memorizzazione nella cache tra domini

Utilizzare questa direttiva per specificare se l'agente cache segue i collegamenti ipertestuali tra gli host. Se un URL memorizzato nella cache contiene collegamenti ad altri server, il server può ignorare il collegamento o seguirlo. Se la direttiva DelveInto è impostata su `never`, non verrà applicata.

Formato

```
DelveAcrossHosts {on | off}
```

Impostazione predefinita

```
DelveAcrossHosts Off
```

DelveDepth — Indica di specificare fino a che punto seguire i collegamenti durante la memorizzazione nella cache

Utilizzare questa direttiva per specificare il numero di livelli di collegamento da seguire mentre si ricercano le pagine da caricare nella cache. Se la direttiva DelveInto è impostata su `never`, non verrà applicata.

Formato

```
DelveDepth numero_di_livelli
```

Impostazione predefinita

```
DelveDepth 2
```

DelveInto — Indica di specificare se l'agente cache deve seguire i collegamenti

Utilizzare questa direttiva per specificare se l'agente cache carica le pagine collegate dagli URL memorizzati nella cache.

Formato

```
DelveInto {always | never | admin | topn}
```

always
L'agente cache segue i collegamenti da tutti gli URL precedentemente memorizzati nella cache.

never
L'agente cache ignora tutti i collegamenti sugli URL.

admin
L'agente cache segue i collegamenti solo sugli URL specificati nelle direttive LoadURL

topn
L'agente cache segue i collegamenti solo dai file richiamati più di frequente nella cache.

Impostazione predefinita

```
DelveInto always
```

DirBackgroundImage — Indica di specificare un'immagine di sfondo per gli elenchi directory

Utilizzare questa direttiva per applicare un'immagine di sfondo per gli elenchi directory creati dal server proxy. Gli elenchi directory vengono generati quando il server proxy viene utilizzato per ricercare siti FTP.

Specificare un percorso assoluto all'immagine di sfondo. Se l'immagine risiede su un altro server, l'immagine di sfondo deve essere specificata come URL completo. Se non viene specificata alcuna immagine di sfondo, viene utilizzato un semplice sfondo bianco.

Formato

```
DirBackgroundImage /percorso/file
```

Esempi

```
DirBackgroundImage /images/corplogo.png
DirBackgroundimage http://www.somehost.com/graphics/embossed.gif
```

Impostazione predefinita

Nessuna

DirShowBytes — Indica di visualizzare il conteggio byte per file di piccole dimensioni sugli elenchi directory

Utilizzare questa direttiva per specificare se gli elenchi directory includono un conteggio byte esatto per file con dimensioni inferiori a un 1 KB. Un valore `Off` indica che l'elenco directory visualizza la dimensione di 1 KB per tutti i file con dimensione minore o uguale a 1 KB.

Formato

```
DirShowBytes {on | off}
```

Impostazione predefinita

```
DirShowBytes Off
```

DirShowCase — Indica di utilizzare la distinzione tra caratteri maiuscoli/minuscoli quando si ordinano i file sugli elenchi directory

Utilizzare questa direttiva per specificare se gli elenchi directory devono distinguere tra caratteri maiuscoli e minuscoli durante l'ordinamento dei nomi file.

Un valore `On` indica che i caratteri maiuscoli precedono i caratteri minuscoli nell'elenco dei file.

Formato

```
DirShowCase {on | off}
```

Impostazione predefinita

```
DirShowCase On
```

DirShowDate — Indica di visualizzare la data dell'ultima modifica sugli elenchi directory

Utilizzare questa direttiva per specificare se gli elenchi directory includono la data dell'ultima modifica per ciascun file.

Formato

```
DirShowDate {on | off}
```

Impostazione predefinita

```
DirShowDate On
```

DirShowDescription — Indica di visualizzare le descrizioni dei file sugli elenchi directory

Utilizzare questa direttiva per specificare se gli elenchi directory includono le descrizioni dei file HTML. Le descrizioni vengono acquisite dalle tag dei file HTML `<title>`.

Le descrizioni degli elenchi directory FTP illustrano i tipi MIME dei file, se è possibile determinarli.

Formato

```
DirShowDescription {on | off}
```

Impostazione predefinita

```
DirShowDescription On
```

DirShowHidden — Indica di visualizzare i file sugli elenchi directory

Utilizzare questa direttiva per specificare se gli elenchi directory contengono dei file nascosti nella directory. Il server considera i file il cui nome inizia con un punto (.) come file nascosti.

Formato

```
DirShowHidden {on | off}
```

Impostazione predefinita

```
DirShowHidden On
```

DirShowIcons — Indica di visualizzare le icone negli elenchi directory

Utilizzare questa direttiva per specificare se il server contiene icone negli elenchi directory. Le icone possono essere utilizzate per fornire una rappresentazione grafica del tipo di contenuto dei file nell'elenco. Le stesse icone vengono definite dalle direttive AddBlankIcon, AddDirIcon, AddIcon, AddParentIcon e AddUnknownIcon.

Formato

```
DirShowIcons {on | off}
```

Impostazione predefinita

```
DirShowIcons On
```

DirShowMaxDescrLength — Indica di specificare la lunghezza massima delle descrizioni sugli elenchi directory

Utilizzare questa direttiva per impostare il numero massimo di caratteri da visualizzare nel campo relativo alla descrizione sugli elenchi directory.

Formato

```
DirShowMaxDescrLength numero_di_caratteri
```

Impostazione predefinita

```
DirShowMaxDescrLength 25
```

DirShowMaxLength — Indica di specificare la lunghezza massima dei nomi file sugli elenchi directory

Utilizzare questa direttiva per impostare il numero massimo di caratteri utilizzati per i nomi file sugli elenchi directory.

Formato

```
DirShowMaxDescrLength numero_di_caratteri
```

Impostazione predefinita

```
DirShowMaxLength 25
```

DirShowMinLength — Indica di specificare la lunghezza minima dei nomi file sugli elenchi directory

Utilizzare questa direttiva per impostare il numero minimo di caratteri sempre riservati ai nomi file sugli elenchi directory. I nomi file nella directory possono oltrepassare questo numero. Tuttavia, non possono superare il numero specificato sulla direttiva DirShowMaxLength.

Formato

```
DirShowMinLength numero_di_caratteri
```

Impostazione predefinita

```
DirShowMinLength 15
```

DirShowSize — Indica di visualizzare la dimensione file sugli elenchi directory

Utilizzare questa direttiva per specificare se gli elenchi directory includono la dimensione di ciascun file.

Formato

```
DirShowSize {on | off}
```

Impostazione predefinita

```
DirShowSize On
```

Disable — Indica di disabilitare i metodi HTTP

Utilizzare questa direttiva per specificare i metodi HTTP che il server non accetta. Per ciascun metodo che il server deve rifiutare, inserire una direttiva Disable separata.

Nel file di configurazione predefinito, i metodi GET, HEAD, OPTIONS, POST e TRACE sono abilitati mentre tutti gli altri metodi HTTP supportati sono disabilitati. Per disabilitare un metodo attualmente abilitato, eliminarlo dalla direttiva Enable e aggiungerlo alla direttiva Disable.

Formato

```
Disable metodo
```

Nota: i moduli di configurazione e amministrazione utilizzano il metodo POST per aggiornare la configurazione del server. Se si disabilita il metodo POST, non sarà possibile utilizzare i moduli di configurazione e amministrazione.

Impostazioni predefinite

```
Disable   PUT
Disable   DELETE
Disable   CONNECT
```

DisInheritEnv — Indica di specificare le variabili di ambiente non ereditate dai programmi CGI

Utilizzare questa direttiva per specificare le variabili di ambiente che non devono essere ereditate dai programmi CGI (diverse dalle variabili di ambiente CGI specifiche per l'elaborazione CGI).

Per impostazione predefinita, le variabili di ambiente vengono ereditate dai programmi CGI. Utilizzare questa direttiva per escludere singole variabili di ambiente, in modo che non vengano ereditate.

Formato

```
DisInheritEnv variabile_ambiente
```

Esempi

```
DisInheritEnv PATH
DisInheritEnv LANG
```

In questo esempio, tutte le variabili di ambiente, tranne PATH e LANG, vengono ereditate dai programmi CGI.

Impostazione predefinita
Nessuna

DNS-Lookup — Indica di specificare se il server ricerca nomi host client

Utilizzare questa direttiva per specificare se il server ricerca i nomi host dei client richiedenti.

Formato
```
DNS-Lookup {on | off}
```

Il valore utilizzato influisce su alcuni fattori relativi al funzionamento del server:

- Le prestazioni del server. L'uso del valore `Off` migliora le prestazioni e il tempo di risposta del server, in quanto non utilizza risorse per eseguire la ricerca del nome host.
- Le informazioni che il server registra relativamente ai client quando scrive su file di log.
  `Off`—I client vengono identificati dall'indirizzo IP.
  `On`—I client vengono identificati dal nome host.
- Se utilizzare o meno nomi host su maschere indirizzo in impostazioni di protezione, file di gruppi server e file ACL (Access Control List).
  `Off`—Non è possibile utilizzare nomi host su maschere indirizzo; è necessario utilizzare indirizzi IP.
  `On`—È possibile utilizzare nomi host o maschere indirizzo ma non indirizzi IP.

Nota: per utilizzare nomi dominio nelle regole di protezione, è necessario impostare la direttiva DNS-Lookup su `On`.

Impostazione predefinita
```
DNS-Lookup   Off
```

Enable — Indica di abilitare i metodi HTTP

Utilizzare questa direttiva per specificare i metodi HTTP accettati dal server.

È possibile abilitare tutti i metodi HTTP necessari. Per ciascun metodo che il server deve accettare, inserire una direttiva Enable separata.

Formato
```
Enable metodo
```

Se non esiste alcuna direttiva per uno specifico URL, è possibile utilizzare la direttiva Enable per eseguire la programmazione personalizzata dei metodi HTTP. Il programma specificato su questa direttiva ignora l'elaborazione standard per quel metodo.
```
Enable metodo /percorso/fileDLL:nome_funzione
```

Impostazioni predefinite
```
Enable GET
Enable HEAD
Enable POST
Enable TRACE
Enable OPTIONS
```

EnableTcpNodelay — Indica di abilitare l'opzione socket TCP NODELAY

Utilizzare questa direttiva per abilitare l'opzione socket TCP NODELAY.

La direttiva EnableTcpNodelay migliora le prestazioni quando pacchetti IP di piccole dimensioni, come sincronizzazioni SSL o brevi risposte HTTP, vengono trasmessi tra Caching Proxy e il client. Per impostazione predefinita, l'opzione TCP NODELAY è abilitata per tutti i socket.

Formato

```
EnableTcpNodelay {All | HTTP | HTTPS | None}
```

Impostazione predefinita

```
EnableTcpNodelay  All
```

Error — Indica di personalizzare la fase Errore

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata che deve essere chiamata dal server durante la fase Errore. Questo codice viene eseguito per fornire una routine di errore personalizzata in caso di errore.

Formato

```
Error  maschera_richiesta /percorso/file:nome_funzione
```

maschera_richiesta
Specifica una maschera per richieste che determina ulteriormente se la funzione applicativa viene chiamata. La specifica include il protocollo, il dominio e l'host; può essere preceduta da un carattere barra (/) ed è possibile utilizzare l'asterisco (*) come carattere jolly. Ad esempio, `/front_page.html`, `http://www.ics.raleigh.ibm.com`, `/pub*`, `/*` e `*` sono tutti validi.

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

Esempio

```
Error  /index.html /ics/api/bin/icsext05.so:error_rtns
```

Impostazione predefinita

Nessuna

ErrorLog — Indica di specificare il file dove sono registrati gli errori server

Utilizzare questa direttiva per specificare il percorso e il nome file dove il server deve registrare gli errori interni.

Nota: se si modificano i valori predefiniti del server relativamente a ID utente, ID gruppo o percorsi di directory log, creare le nuove directory, quindi aggiornarne autorizzazioni e proprietà. Per fare in modo che il server scriva le informazioni su una directory log definita dall'utente, l'autorizzazione per tale directory deve essere impostata su 755 mentre l'ID del server definito dall'utente deve essere impostato su proprietario. Ad esempio, se l'ID utente del server viene modificato dal valore predefinito al valore jdoe e la

directory logs predefinita viene modificata in server_root/account, quest'ultima deve disporre dell'autorizzazione 755 ed essere di proprietà di jdoe.

Se in esecuzione, il server avvia un nuovo file di log ogni giorno a mezzanotte. In caso contrario, questo si verifica appena il server viene avviato. Quando il file viene creato, il server utilizza il nome del file specificato, a cui appone un suffisso data. Il suffisso data è nel formato *Mmmddyyyy* , dove *Mmm* rappresenta le prime tre lettere del mese, *dd* il giorno del mese e *yyyy* l'anno.

Formato

`ErrorLog` */percorso/directory_logs/nome_file*

Impostazioni predefinite

- **Sistemi Linux e UNIX:** `ErrorLog /opt/ibm/edge/cp/server_root/logs/error`
- **Sistemi Windows:** `ErrorLog` *unità*`:\Programmi\IBM\edge\cp\logs\error`

ErrorPage — Indica di specificare un messaggio personalizzato per una determinata condizione di errore

Utilizzare questa direttiva per specificare il nome di un file da inviare al client richiedente quando il server riscontra una particolare condizione di errore. Il file di configurazione ibmproxy.conf fornisce le direttive ErrorPage che associano le parole chiave relative all'errore ai file dei messaggi di errore.

Per personalizzare i messaggi di errore, è possibile modificare le direttive ErrorPage per associare le parole chiave relative all'errore a file differenti o modificare i file dei messaggi di errore forniti. Ad esempio, è possibile modificare un messaggio in modo che contenga informazioni aggiuntive sulla causa del problema e suggerisca le possibili soluzioni per correggerlo. Per le reti interne, è possibile fornire un contatto a cui gli utenti possono rivolgersi.

Le direttive ErrorPage possono essere posizionate ovunque nel file di configurazione. Quando si verifica un errore, il file viene elaborato in base alle regole di mappatura definite nel file di configurazione. Perciò, il file da inviare deve risiedere in una posizione raggiungibile attraverso le regole di mappatura, come definito dalle direttive Fail, Map, NameTrans, Pass, Redirect e Service. Come minimo, è necessaria la direttiva Pass che consente al server di trasferire il file del messaggio di errore.

Formato

`ErrorPage` *parola chiave /percorso/nomefile.html*

parola chiave
: Specifica una delle parole chiave associate a una condizione di errore. Le parole chiave sono elencate nelle direttive ErrorPage nel file ibmproxy.conf. Le parole chiave non possono essere modificate.

/percorso/nomefile.html
: Specifica il nome Web completo del file di errore, come visualizzato da un client sul Web. I file di messaggi di errore predefiniti si trovano in /HTML/errorpages/.

Esempio

```
ErrorPage scriptstart /HTML/errorpages/scriptstart.htmls
```

In questo esempio, quando si riscontra una condizione `scriptstart`, il server invia al client un file scriptstart.htmls presente nella directory /HTML/errorpages/.

Il testo HTML riportato di seguito è un esempio del possibile contenuto del file:

```
<HTML>
<HEAD>
<TITLE>Messaggio per condizione SCRIPTSTART</TITLE>
</HEAD>
<BODY>
Impossibile avviare il programma CGI.
<P>
<A HREF="mailto:admin@websvr.com">Riferire il problema</A>
all'amministratore.
</BODY>
</HTML>
```

Se la direttiva che corrisponde al suddetto percorso nel file di configurazione del server è `PASS /* /wwwhome/*`, il percorso completo a questo file di messaggio è `/wwwhome/HTML/errorpages/scriptstart.htmls`.

Personalizzazione dei messaggi di errore restituiti dal server

Ciascuna condizione di errore è identificata da una parola chiave. Per stabilire quali messaggi di errore personalizzare, esaminare i file di messaggi di errore inclusi in Caching Proxy, disponibili in /HTML/errorpages. La pagina di errore contiene il numero errore, il messaggio predefinito, una spiegazione della causa e un'azione di ripristino adatta.

Quindi, effettuare una delle seguenti operazioni per modificare un messaggio di errore:

- Modificare il file HTML o HTMLS esistente (creare prima una copia di backup) o creare un nuovo file HTML o HTMLS con testo a scelta. È possibile utilizzare un editor HTML o ASCII. È necessario utilizzare un file HTMLS se si intende adoperare inclusioni lato server.
- Se è stato creato un file di messaggi di errore con un nome differente (o in un differente percorso), modificare la direttiva ErrorPage per quella parola chiave in modo che punti al file.

Condizioni di errore, cause e messaggi predefiniti

Tutte le parole chiave relative all'errore e i file di messaggi di errore predefiniti sono elencati nel file ibmproxy.conf nella sezione della direttiva ErrorPage. I file di messaggi di errore contengono il numero del messaggio di errore, la parola chiave, il messaggio predefinito, la spiegazione e la risposta dell'utente (azione).

Impostazioni predefinite

Molte impostazioni predefinite sono contenute nel file ibmproxy.conf

Se non si modifica una direttiva ErrorPage per una condizione di errore, viene inviata la pagina di errore predefinita del server per quella condizione.

EventLog — Indica di specificare il percorso al file di log eventi

Utilizzare questa direttiva per specificare il nome file e il percorso al file di log eventi. Il log eventi cattura i messaggi informativi sulla cache.

Nota: se si modificano i valori predefiniti del server relativamente a ID utente, ID gruppo o percorsi di directory log, creare le nuove directory, quindi

aggiornarne autorizzazioni e proprietà. Per fare in modo che il server scriva le informazioni su una directory log definita dall'utente, l'autorizzazione per tale directory deve essere impostata su 755 mentre l'ID del server definito dall'utente deve essere impostato su proprietario. Ad esempio, se si modifica l'ID utente del server dal valore predefinito a jdoe e la directory logs predefinita in server_root/account, la directory server_root/account deve disporre dell'autorizzazione 755 ed essere di proprietà di jdoe.

Se in esecuzione, il server avvia un nuovo file di log ogni giorno a mezzanotte. In caso contrario, questo si verifica appena il server viene avviato. Quando il file viene creato, il server utilizza il nome del file specificato, a cui appone un suffisso data. Il suffisso data è nel formato *Mmmddyyyy* , dove *Mmm* rappresenta le prime tre lettere del mese, *dd* il giorno del mese e *yyyy* l'anno.

Formato

`EventLog` */percorso/directory_logs/nome_file*

Impostazioni predefinite

- **Sistemi Linux e UNIX:** `EventLog /opt/ibm/edge/cp/server_root/logs/event`
- **Sistemi Windows:** `EventLog` *drive*`:\Programmi\IBM\edge\cp\logs\event`

Exec — Indica di eseguire un programma CGI per eseguire la corrispondenza delle richieste

Utilizzare questa direttiva per specificare una maschera per le richieste da accettare e a cui rispondere eseguendo un programma CGI. Se una richiesta corrisponde a una maschera su una direttiva Exec, non viene confrontata con le maschere richiesta sulle direttive successive.

Formato

`Exec` *percorso_programma maschera_richiesta* [*indirizzo_IP_server* | *nome_host*]

maschera_richiesta
Specifica una maschera per le richieste che il server deve accettare e a cui deve rispondere eseguendo il programma CGI.

È necessario utilizzare un asterisco (*) come carattere jolly sia in `maschera_richiesta` che in `percorso_programma`. La parte della richiesta che corrisponde al carattere jolly `maschera_richiesta` deve iniziare con il nome del file che contiene il programma CGI.

La richiesta può anche contenere ulteriori dati trasferiti al programma CGI nella variabile di ambiente PATH_INFO. I dati aggiuntivi seguono il primo carattere barra (/) successivo al nome file del programma CGI sulla richiesta. I dati vengono trasferiti in base alle specifiche CGI.

percorso_programma
Specifica il percorso al file che contiene il programma CGI che il server esegue per la richiesta. *percorso_programma* deve contenere anche un carattere jolly. Quest'ultimo viene sostituito con il nome del file che contiene il programma CGI.

La direttiva Exec è ricorsiva e si applica a tutte le sottodirectory. Non è necessario utilizzare una direttiva Exec separata per ciascuna directory in cgi-bin e admin-bin.

[*indirizzo_IP_server* | *nome_host*]
Se si utilizzano più indirizzi IP o host virtuali, utilizzare questo parametro per specificare un indirizzo IP o un nome host. Il server utilizza la direttiva

esclusivamente per le richieste inviate al server su questo indirizzo IP o per questo host. Per un indirizzo IP, si tratta dell'indirizzo della connessione di rete del server e non dell'indirizzo del client richiedente.

È possibile specificare un indirizzo IP (ad esempio, `240.146.167.72`) o un nome host (ad esempio, `hostA.bcd.com`).

Questo parametro è opzionale. Senza questo parametro, il server utilizza la direttiva per tutte le richieste a prescindere dall'indirizzo IP su cui è stata ricevuta la richiesta o dal nome host nell'URL.

I caratteri jolly non possono essere utilizzati per specificare indirizzi IP server.

Esempi

Nell'esempio riportato di seguito, se il server riceve una richiesta `/idd/depts/plan/c92` , esegue il programma CGI in /depts/bin/plan.exe con `c92` trasferito al programma come input.

L'esempio di seguito utilizza il parametro indirizzo IP opzionale. Se il server riceve richieste che iniziano con `/cgi-bin/`, supporta la richiesta da una differente directory, in base all'indirizzo IP della connessione di rete su cui è arrivata la richiesta. Per le richieste che arrivano su 130.146.167.72, il server utilizza la directory /CGI-BIN/customerA. Per le richieste che arrivano su una qualsiasi connessione con indirizzo 0.83.100.45, il server utilizza la directory /CGI-BIN/customerB.

```
Exec    /cgi-bin/*    /CGI-BIN/customerA/*   130.129.167.72
Exec    /cgi-bin/*    /CGI-BIN/customerB/*   0.83.100.45
```

Nell'esempio riportato di seguito viene utilizzato il parametro nome host opzionale. Se il server riceve richieste che iniziano con `/cgi-bin`, supporta la richiesta da una differente directory, in base al nome host nell'URL. Per le richieste che arrivano per hostA.bcd.com, il server utilizza la directory /CGI-BIN/customerA. Per le richieste che arrivano per hostB.bcd.com, il server utilizza la directory /CGI-BIN/customerB.

```
Exec    /cgi-bin/*    /CGI-BIN/customerA/*   hostA.bcd.com
Exec    /cgi-bin/*    /CGI-BIN/customerB/*   hostB.bcd.com
```

Impostazioni predefinite

- **Sistemi Linux e UNIX**

  ```
  Exec  /cgi-bin/*
  /opt/ibm/edge/cp/server_root/cgi-bin/*
  Exec  /admin-bin/*    /opt/ibm/edge/cp/server_root/admin-bin/*
  ```

- **Sistemi Windows**

  ```
  Exec  server_root/cgi-bin/*
  Exec  server_root/admin-bin/*
  Exec  server_root/DOCS/admin-bin/*
  ```

ExportCacheImageTo — Indica di esportare la memoria cache su disco

Utilizzare questa direttiva per esportare i contenuti cache in un file di dump. Si tratta di un'operazione utile quando la cache in memoria va perduta durante il riavvio o quando la medesima cache viene distribuita a più proxy.

Formato

`ExportCacheImageTo` *`nome_file_esportazione`*

Impostazione predefinita
Nessuna

ExternalCacheManager — Indica di configurare Caching Proxy per Dynamic Caching di IBM WebSphere Application Server

Utilizzare questa direttiva per configurare Caching Proxy in modo che riconosca un prodotto IBM WebSphere Application Server (configurato con un modulo adattatore Caching Proxy) da cui possa memorizzare dinamicamente nella cache le risorse create. Caching Proxy salva le copie dei risultati JSP anch'essi memorizzati nella cache dinamica del server delle applicazioni. Caching Proxy memorizza nella cache solo il contenuto di un prodotto IBM WebSphere Application Server il cui ID gruppo corrisponde a una voce ExternalCacheManager.

Notare che, per abilitare questa funzione, è necessario aggiungere anche una direttiva Service al file di configurazione Caching Proxy. Inoltre, è necessario eseguire altre procedure di configurazione sul server delle applicazioni. Fare riferimento a Capitolo 22, "Memorizzazione nella cache di contenuto generato dinamicamente", a pagina 101 per le informazioni.

Formato
```
ExternalCacheManager ID_gestore_cache_esterno
Scadenza_massima
```

ID_gestore_cache_esterno
L'ID assegnato a IBM WebSphere Application Server che supporta il proxy. L'ID deve corrispondere all'ID impostato nell'attributo `externalCacheGroup: group id` nel file dynacache.xml sul server delle applicazioni.

Scadenza_massima
La scadenza predefinita impostata per le risorse memorizzate nella cache per conto del gestore cache esterno. Se il gestore cache esterno non invalida una risorsa memorizzata nella cache entro una scadenza prestabilita, una volta raggiunto questo valore la richiesta non sarà più valida. Questo valore può essere espresso in minuti o secondi.

Esempio
La voce riportata di seguito definisce un gestore cache esterno (IBM WebSphere Application Server) che si trova all'interno del dominio www.xyz.com e le cui risorse scadono in 20 secondi o meno.
```
ExternalCacheManager   IBM-CP-XYZ-1  20 seconds
```

Impostazione predefinita
Nessuna

Fail — Indica di rifiutare le richieste corrispondenti

Utilizzare questa direttiva per specificare una maschera per le richieste che il server non deve elaborare. Se una richiesta corrisponde a una maschera su una direttiva Fail, non viene confrontata con le maschere richiesta sulle direttive successive.

Formato
```
Fail maschera_richiesta [indirizzo_IP_server | nome_host]
```

maschera_richiesta
Specifica una maschera per le richieste che il server deve rifiutare. Se una richiesta corrisponde a una maschera, il server invia un messaggio di errore al richiedente.

Nella maschera, è possibile utilizzare un asterisco come carattere jolly. Il carattere tilde (~), subito dopo una barra (/), deve essere confrontato in modo esplicito; infatti per questa operazione non è possibile utilizzare un carattere jolly.

[*indirizzo_IP_server* | *nome_host***]**
Se si utilizzano più indirizzi IP o host virtuali, utilizzare questo parametro per specificare un indirizzo IP o un nome host. Il server utilizza la direttiva esclusivamente per le richieste inviate al server su questo indirizzo IP o per questo host. Per un indirizzo IP, si tratta dell'indirizzo della connessione di rete del server e non dell'indirizzo del client richiedente.

È possibile specificare un indirizzo IP (ad esempio, `240.146.167.72`) o un nome host (ad esempio, `hostA.bcd.com`).

Questo parametro è opzionale. Senza questo parametro, il server utilizza la direttiva per tutte le richieste a prescindere dall'indirizzo IP su cui è stata ricevuta la richiesta o dal nome host nell'URL.

Per un indirizzo IP del server non è possibile specificare un carattere jolly.

Esempi

Nell'esempio riportato di seguito, il server rifiuta le richieste che iniziano con `/usr/local/private/`.

```
Fail /usr/local/private/*
```

Nell'esempio riportato di seguito viene utilizzato il parametro dell'indirizzo IP opzionale. Il server rifiuta le richieste che iniziano con `/customerB/` se la richiesta arriva su una connessione di rete con l'indirizzo IP 240.146.167.72. Il server rifiuta le richieste che iniziano con `/customerA/` se la richiesta arriva su una connessione di rete con l'indirizzo IP 0.83.100.45.

```
Fail    /customerB/*    240.146.167.72
Fail    /customerA/*    0.83.100.45
```

Nell'esempio riportato di seguito viene utilizzato il parametro del nome host opzionale. Il server rifiuta le richieste con `/customerB/` se la richiesta arriva per hostA.bcd.com. Il server rifiuta le richieste che iniziano con `/customerA/` se la richiesta arriva per hostB.bcd.com.

```
Fail    /customerB/*    hostA.bcd.com
Fail    /customerA/*    hostB.bcd.com
```

Impostazione predefinita

Nessuna

FIPSEnable — Indica di abilitare la crittografia approvata FIPS (Federal Information Processing Standard) per SSLV3 e TLS

Utilizzare questa direttiva per abilitare la crittografia approvata FIPS per il protocollo SSLV3 e TLS nelle connessioni SSL. Quando questa direttiva è abilitata, l'elenco delle specifiche di crittografia supportate per SSLV3 (direttiva V3CipherSpecs) viene ignorato. Inoltre, le specifiche di crittografia TLS consentite verranno impostate su 352F0AFF09FE mentre le specifiche di crittografia SSLV3 su FFFE.

Formato

```
FIPSEnable {on | off}
```

Impostazione predefinita

```
FIPSEnable  off
```

flexibleSocks — Indica di abilitare l'implementazione SOCKS flessibile

Utilizzare questa direttiva per indicare al proxy di utilizzare il file di configurazione SOCKS per determinare il tipo di connessione da creare.

Formato

```
flexibleSocks {on | off}
```

Impostazione predefinita

```
flexibleSocks on
```

FTPDirInfo — Indica di generare un messaggio descrittivo o iniziale per una directory

Utilizzare questa direttiva per abilitare i server FTP a generare un messaggio descrittivo o iniziale per una directory. Facoltativamente, è possibile visualizzare questo messaggio come parte degli elenchi FTP. La direttiva FTPDirInfo consente di controllare dove viene visualizzato il messaggio.

Formato

```
FTPDirInfo  {top | bottom | off}
```

top
Indica di visualizzare il messaggio iniziale in cima alla pagina, prima dell'elenco dei file nella directory.

bottom
Indica di visualizzare il messaggio iniziale in fondo alla pagina, dopo l'elenco dei file nella directory.

off
Indica di non visualizzare la pagina iniziale.

Impostazione predefinita

```
FTPDirInfo top
```

ftp_proxy — Indica di specificare un altro server proxy per le richieste FTP

Se il server proxy fa parte di una catena di proxy, utilizzare questa direttiva per specificare il nome di un altro proxy che il server può contattare per le richieste FTP. È necessario specificare un URL completo, contenente il carattere barra finale (/). Per informazioni sull'uso di una maschera o nome dominio opzionale, fare riferimento a "no_proxy — Indica di specificare le maschere per la connessione diretta ai domini" a pagina 232.

Formato

```
ftp_proxy URL_completo [nome_dominio_o_maschera]
```

Esempio

```
ftp_proxy http:// outer.proxy.server/
```

Impostazione predefinita

Nessuna

FTPUrlPath — Indica di specificare la modalità di interpretazione di URL FTP

Utilizzare questa direttiva per specificare se le informazioni del percorso negli URL FTP vengono interpretate come relative alla directory di lavoro dell'utente collegato o alla directory root.

Formato

```
FTPUrlPath  {relative | absolute}
```

Se la direttiva FTPUrlPath viene impostata su `absolute`, la directory di lavoro FTP dell'utente collegato deve essere inclusa nel percorso URL FTP. Se viene specificata la direttiva `FTPUrlPath Relative`, la directory di lavoro FTP dell'utente collegato deve essere omessa dal percorso URL FTP. Ad esempio, per accedere al file test1.html, contenuto nella directory di lavoro /export/home/user1 di un utente collegato, sono necessari i seguenti percorsi URL, a seconda dell'impostazione della direttiva FTPUrlPath:

- Se l'impostazione è `FTPUrlPath absolute`, il percorso URL richiesto è `ftp://ftphost/export/home/user1/test1.html`.
- Se l'impostazione è `FTPUrlPath relative`, il percorso URL richiesto è `ftp://ftphost/test1.html`.

Impostazione predefinita

Nessuna

Gc — Indica di specificare la raccolta di dati inutili

Utilizzare questa direttiva per specificare se utilizzare la raccolta di dati inutili. Se la memorizzazione nella cache è abilitata, il server utilizza il processo di raccolta di dati inutili per eliminare i file che non devono più essere conservati nella cache. I file vengono eliminati in base alla relativa data di scadenza e ad altri valori della direttiva proxy. Generalmente, se la memorizzazione nella cache è abilitata, viene utilizzata la raccolta di dati inutili. Se la raccolta di dati inutili non viene adoperata, la cache proxy viene utilizzata in modo inefficiente.

Formato

```
Gc {on | off}
```

Impostazione predefinita

```
Gc On
```

GCAdvisor — Indica di personalizzare il processo di raccolta di dati inutili

Utilizzare questa direttiva per specificare un'applicazione personalizzata che il server deve utilizzare per la raccolta di dati inutili.

Formato

`GCAdvisor` */percorso/file*`:`*nome_funzione*

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

Esempio

```
GCAdvisor /api/bin/customadvise.so:gcadv
```

GcHighWater — Indica di specificare l'inizio della raccolta di dati inutili

Utilizzare questa direttiva per specificare la percentuale della capacità cache totale che deve essere raggiunta per attivare la raccolta di dati inutili. Questa percentuale viene chiamata *livello massimo di occupazione*. Il livello massimo di occupazione viene specificato come percentuale della capacità cache totale. La raccolta di dati inutili prosegue fino a raggiungere il livello minimo di occupazione — per l'impostazione di questo valore, vedere "GcLowWater — Indica di specificare la fine della raccolta di dati inutili". La percentuale del livello massimo di occupazione è compresa tra 50 e 95.

Formato

```
GcHighWater percentuale
```

Impostazione predefinita

```
GcHighWater 90
```

GcLowWater — Indica di specificare la fine della raccolta di dati inutili

Utilizzare questa direttiva per specificare la percentuale della capacità cache totale che attiva la fine della raccolta di dati inutili. Questa percentuale è nota come *livello minimo di occupazione*. Questo viene specificato come percentuale della capacità cache totale e deve essere impostato su un valore inferiore rispetto a quello del livello massimo di occupazione; per informazioni sull'impostazione di questo valore, vedere "GcHighWater — Indica di specificare l'inizio della raccolta di dati inutili".

Formato

```
GcLowWater percentuale
```

Impostazione predefinita

```
GcLowWater 60
```

gopher_proxy — Indica di specificare un altro server proxy per le richieste Gopher

Se il server proxy fa parte di una catena di proxy, utilizzare questa direttiva per specificare il nome di un altro proxy che il server può contattare per le richieste Gopher. È necessario specificare un URL completo, contenente il carattere barra finale (/). Per informazioni sull'uso di una maschera o nome dominio opzionale, fare riferimento a "no_proxy — Indica di specificare le maschere per la connessione diretta ai domini" a pagina 232.

Formato

```
gopher_proxy full_URL[nome_dominio_o_maschera]
```

Esempio

```
gopher_proxy http://outer.proxy.server/
```

Impostazione predefinita

Nessuna

GroupId — Indica di specificare l'ID gruppo

Utilizzare questa direttiva per specificare il numero o il nome gruppo assunto dal server prima di accedere ai file.

Se la direttiva viene modificata, è necessario arrestare manualmente il server, quindi riavviarlo, per convalidare le modifiche. La modifica non ha effetto se il server viene solo riavviato. (Consultare Capitolo 5, "Avvio e arresto di Caching Proxy", a pagina 15.)

Nota: se si modificano i valori predefiniti del server relativamente a ID utente, ID gruppo o percorsi di directory log, creare le nuove directory, quindi aggiornarne autorizzazioni e proprietà. Per fare in modo che il server scriva le informazioni su una directory log definita dall'utente, l'autorizzazione per tale directory deve essere impostata su 755 mentre l'ID del server definito dall'utente deve essere impostato su proprietario. Ad esempio, se l'ID utente del server viene modificato dal valore predefinito al valore jdoe e la directory logs predefinita viene modificata in server_root/account, quest'ultima deve disporre dell'autorizzazione 755 ed essere di proprietà di jdoe.

Formato

```
GroupId { nome_gruppo | numero_gruppo}
```

Impostazioni predefinite

AIX: `GroupId nobody`

HP-UX: `GroupId other`

Linux:

Red Hat: `GroupId nobody`

SUSE: `GroupId nogroup`

Solaris: `GroupId nobody`

HeaderServerName — Indica di specificare il nome del server proxy restituito nell'intestazione HTTP

Utilizzare questa direttiva per specificare il nome del server proxy restituito nell'intestazione HTTP

Formato

```
HeaderServerName nome
```

Impostazione predefinita

Nessuna

Hostname — Indica di specificare il nome dominio completo o l'indirizzo IP del server

Utilizzare questa direttiva per specificare il nome dominio o un indirizzo IP restituito ai client dalle richieste file. Se si specifica un nome dominio, il server deve essere in grado di risolvere il nome in un indirizzo IP. Se si specifica un indirizzo IP, il DNS (Domain Name Server) non è necessario né accessibile.

Nota: quando si imposta una matrice, la direttiva Hostname deve essere configurata in modo identico su tutti i membri della matrice.

Formato

```
Hostname {nome | indirizzo IP}
```

Impostazione predefinita

Per impostazione predefinita, questa direttiva non viene specificata nel file di configurazione iniziale. Se questa direttiva non viene specificata nel file di configurazione, il valore assegnato sarà il nome host definito nel DNS (Domain Name Server).

http_proxy — Indica di specificare un altro server proxy per le richieste HTTP

Se il server proxy fa parte di una catena di proxy, utilizzare questa direttiva per specificare il nome di un altro proxy che il server può contattare per le richieste HTTP. È necessario specificare un URL completo, contenente il carattere barra finale (/). Per informazioni sull'uso di una maschera o nome dominio opzionale, fare riferimento a "no_proxy — Indica di specificare le maschere per la connessione diretta ai domini" a pagina 232.

Formato

```
http_proxy URL_completo[nome_dominio_o_maschera]
```

Esempio

```
http://outer.proxy.server/
```

Impostazione predefinita

Nessuna

HTTPSCheckRoot — Indica di filtrare le richieste HTTPS

Utilizzare questa direttiva per specificare se Caching Proxy richiama la home page precaria dell'URL e tenta di ricercarvi le etichette. Nel caso queste vengano trovate, verranno applicate alla richiesta protetta. Ad esempio, se si richiede `https://www.ibm.com/`, Caching Proxy richiama http://www.ibm.com/ e ricerca le etichette, utilizzando tutte quelle che trova per filtrare https://www.ibm.com/.

Se HTTPSCheckRoot è impostato su `off`, Caching Proxy non richiama la home page precaria né ricerca le etichette.

Formato

```
HTTPSCheckRoot {on | off}
```

Impostazione predefinita

```
HTTPSCheckRoot  on
```

ICP_Address — Indica di specificare l'indirizzo IP per le query ICP

Utilizzare questa sottodirettiva per specificare un indirizzo IP utilizzato per inviare e ricevere query ICP. La sottodirettiva deve essere contenuta nelle direttive **<MODULEBEGIN> ICP** e **<MODULEEND>**.

Formato

```
ICP_Address indirizzo_IP
```

Impostazione predefinita

Per impostazione predefinita, questa direttiva non viene specificata nel file di configurazione iniziale. Se questa direttiva non viene specificata nel file di configurazione, il valore assegnato prevede di accettare e inviare query ICP su qualsiasi interfaccia.

ICP_MaxThreads — Indica di specificare il numero massimo di thread per le query ICP

Utilizzare questa sottodirettiva per specificare il numero di thread generati, in ascolto per ricevere le query ICP. La sottodirettiva deve essere contenuta nelle direttive **<MODULEBEGIN> ICP** e **<MODULEEND>**.

Nota: Su Redhat Linux 6.2 e versioni precedenti, questo valore deve essere basso in quanto il numero massimo di thread che può essere creato per processo è esiguo. Se si specifica un numero esteso di thread che deve essere utilizzato da ICP, questo può limitare il numero dei thread disponibili adoperati per supportare le richieste.

Formato

```
ICP_MaxThreads numero_di_thread
```

Impostazione predefinita

```
ICP_MaxThreads   5
```

Occupier — Indica di specificare un membro di un cluster ICP

Se il server proxy fa parte di un cluster ICP, utilizzare questa sottodirettiva per specificare i peer ICP. La sottodirettiva deve essere contenuta nelle direttive **<MODULEBEGIN> ICP** e **<MODULEEND>**.

Quando si aggiunge un nuovo peer al cluster ICP, le informazioni peer ICP devono essere aggiunte al file di configurazione di tutti i peer esistenti. Utilizzare una riga per ciascun peer. Notare che è possibile includere l'host corrente nell'elenco peer. Nel momento in cui ICP viene inizializzato, ignora la voce dell'host corrente. In questo modo, è possibile disporre di un solo file di configurazione che può essere copiato su altre macchine peer senza doverlo modificare per rimuovere l'host corrente.

Formato

```
ICP_Peer nomehost porta_http porta_icp
```

nomehost
Il nome del peer

porta_http
La porta proxy del peer

porta_icp
La porta server ICP del peer

Esempio

La riga riportata di seguito aggiunge l'host abc.xcompany.com, con porta proxy 80 e porta ICP 3128, come peer.

```
ICP_Peer  abc.xcompany.com  80  3128
```

Impostazione predefinita

Nessuna

ICP_Port — Indica di specificare il numero di porta per le query ICP

Utilizzare questa sottodirettiva per specificare il numero di porta su cui il server ICP è in ascolto per ricevere le query ICP. La sottodirettiva deve essere contenuta nelle direttive **<MODULEBEGIN> ICP** e **<MODULEEND>**.

Formato

```
ICP_Port numero_porta
```

Impostazione predefinita

```
ICP_Port 3128
```

ICP_Timeout — Indica di specificare il tempo massimo di attesa per le query ICP

Utilizzare questa sottodirettiva per specificare il tempo massimo in cui Caching Proxy attende per ricevere le risposte alle query ICP. Il tempo è specificato in millisecondi. La sottodirettiva deve essere contenuta nelle direttive **<MODULEBEGIN> ICP** e **<MODULEEND>**.

Formato

```
ICP_Timeout  timeout_in_millisecondi
```

Impostazione predefinita

```
ICP_Timeout  2000
```

IgnoreURL — Indica di specificare gli URL non aggiornati

Utilizzare questa direttiva per specificare gli URL non caricati dall'agente cache. Questa direttiva è utile quando l'agente cache carica le pagine collegate dagli URL memorizzati nella cache. Per specificare URL o maschere URL differenti, è possibile utilizzare più occorrenze della direttiva IgnoreURL. Il valore di questa direttiva può contenere asterischi (*) come caratteri jolly, per applicare una maschera.

Formato

```
IgnoreURL URL
```

Esempi

```
IgnoreURL http://www.yahoo.com/
IgnoreURL http://*.ibm.com/*
```

Impostazione predefinita

```
IgnoreURL */cgi-bin/*
```

imbeds — Indica di specificare se viene utilizzata l'elaborazione di inclusione lato server

Utilizzare questa direttiva per specificare se si intende eseguire l'elaborazione di inclusione lato server per i file supportati dal file system, programmi CGI o entrambi. L'elaborazione di inclusione lato server viene eseguita su file con un tipo di contenuto `ext/x-ssi-html`. Facoltativamente, è possibile specificare di eseguire l'elaborazione di inclusione lato server anche per i file con un tipo di contenuto `text/html`. Per ulteriori informazioni sui tipi di contenuto, consultare "AddType — Indica di specificare il tipo dati di file con particolari suffissi" a pagina 173.

Per inserire dinamicamente le informazioni nel file che deve essere restituito, è possibile utilizzare l'elaborazione di inclusione lato server. Questo tipo di

informazioni possono contenere la data, la dimensione di un file, la data in cui il file è stato modificato l'ultima volta, variabili di ambiente di inclusione CGI o lato server o file di testo. L'elaborazione di inclusione lato server viene eseguita esclusivamente sui file creati localmente. Caching Proxy non esegue l'elaborazione di inclusione lato server su oggetti proxy o cache.

L'elaborazione di inclusione lato server fa sì che il server ricerchi comandi speciali nei file, ogni volta che questi vengono supportati. Ciò può influire sulle prestazioni del server e rallentare il tempo di risposta ai client.

Formato

```
imbeds {on | off | files | cgi | noexec}  {SSIOnly | html}
```

on L'elaborazione di inclusione lato server viene eseguita per i file del file system e dei programmi CGI.

off
L'elaborazione di inclusione lato server non viene eseguita per alcun file.

files
L'elaborazione di inclusione lato server viene eseguita solo per i file del file system.

cgi
L'elaborazione di inclusione lato server viene eseguita solo per i file restituiti da programmi CGI.

noexec

SSIOnly
L'elaborazione di inclusione lato server viene eseguita per i file con un tipo di contenuto `text/x-ssi-html`.

html
L'elaborazione di inclusione lato server viene eseguita per i file con un tipo di contenuto text/html e `text/x-ssi-html`.

Il server controlla il tipo di contenuto di ciascun file che richiama e l'output di ciascun programma CGI che elabora.

Normalmente, l'elaborazione di inclusione lato server viene eseguita solo sui file con un tipo di contenuto `text/x-ssi/html`. Tuttavia, è possibile specificare che i file con un tipo di contenuto `text/html` vengano elaborati per inclusioni lato server.

Nota: il server considera file html, .html e .htm come file `html`. Il resto viene considerato come `SSIOnly`.

Ciascun suffisso deve disporre di una direttiva AddType definita con il tipo di contenuto corretto. Se si utilizzano suffissi diversi da .htm or .html, verificare di aver definito una direttiva AddType con un tipo di contenuto `text/x-ssi/html`.

Impostazione predefinita

```
imbeds on SSIOnly
```

ImportCacheImageFrom — Indica di importare la memoria cache da un file

Utilizzare questa direttiva per importare i contenuti cache da un file di dump. Si tratta di un'operazione utile quando la cache in memoria va perduta durante il riavvio o quando la medesima cache viene distribuita a più proxy.

Formato

```
ImportCacheImageFrom nome_file_importazione
```

Impostazione predefinita

Nessuna

InheritEnv — Indica di specificare le variabili di ambiente ereditate da programmi CGI

Utilizzare questa direttiva per specificare le variabili di ambiente che devono essere ereditate dai programmi CGI (diverse dalle variabili di ambiente CGI specifiche per l'elaborazione CGI).

Se non si inserisce la direttiva InheritEnv, i programmi CGI erediteranno tutte le variabili di ambiente. Se si inserisce una direttiva InheritEnv, verranno ereditate solo le variabili di ambiente specificate sulle direttive InheritEnv insieme alle variabili di ambiente specifiche di CGI. La direttiva consente di inizializzare facoltativamente il valore delle variabili ereditate.

Formato

```
InheritEnv variabile_ambiente
```

Esempi

```
InheritEnv PATH
InheritEnv LANG=ENUS
```

In questo esempio, i programmi CGI ereditano solo le variabili di ambiente PATH e LANG e la variabile di ambiente LANG viene inizializzata con il valore ENUS.

Impostazione predefinita

Nessuna. Per impostazione predefinita, le variabili di ambiente vengono ereditate dai programmi CGI.

InputTimeout — Indica di specificare il timeout di input

Utilizzare questa direttiva per impostare il tempo consentito a un client per inviare una richiesta dopo aver stabilito un collegamento con il server. Per prima cosa, il client si collega al server, quindi invia una richiesta. Se il client non invia alcuna richiesta entro l'intervallo di tempo specificato con questa direttiva, il server chiude il collegamento. Il valore tempo può essere specificato come una qualsiasi combinazione di ore, minuti (o min) e secondi (o sec).

Formato

```
InputTimeout intervallo di tempo
```

Esempio

```
InputTimeout 3 mins 30 secs
```

Impostazione predefinita

```
InputTimeout 2 minutes
```

JunctionReplaceUrlPrefix — Indica di sostituire l'URL anziché inserire il prefisso, se si utilizza il plugin JunctionRewrite

Questa direttiva ignora l'azione predefinita del plugin JunctionRewrite e consente al proxy di correggere determinati collegamenti URL nella pagina html. Utilizzata insieme alla direttiva JunctionRewrite.

La direttiva JunctionReplaceUrlPrefix indica al plugin JunctionRewrite di sostituire l'URL *modello_url_1* con *modello_url_2*, anziché inserire un prefisso all'inizio dell'URL.

Formato

```
JunctionReplaceUrlPrefix modello_url_1 modello_url_2
```

Esempio

```
JunctionReplaceUrlPrefix /server1.internaldomain.com/*  /server1/*
```

In questo esempio, l'URL è /server1.internaldomain.com/notes.nsf mentre il prefisso è /server1. Anziché inserire il prefisso per riscrivere l'URL in/server1/server1.internaldomain.com/notes.nsf, il plugin JunctionRewrite cambia l'URL in /server1/notes.nsf.

Impostazione predefinita

Nessuna

JunctionRewrite — Indica di attivare la riscrittura dell'URL

Questa direttiva consente alla routine di riscrittura delle giunzioni in Caching Proxy di riscrivere le risposte provenienti dai server di origine per garantire che gli URL relativi al server vengano mappati sul server di origine adeguato, quando si utilizzano le giunzioni. Se si imposta **JunctionRewrite on** senza l'opzione UseCookie, anche il plugin di riscrittura delle giunzioni deve essere abilitato. Le giunzioni vengono definite dalle regole di mappatura del proxy.

Per ulteriori informazioni su JunctionRewrite, consultare "UseCookie come alternativa a JunctionRewrite" a pagina 46 e "Plugin Transmogrifier di esempio per estendere la funzionalità JunctionRewrite" a pagina 47.

Formato

```
JunctionRewrite {on | on UseCookie | off}
```

Impostazione predefinita

```
JunctionRewrite off
```

JunctionRewriteSetCookiePath — Indica di riscrivere l'opzione di percorso nell'intestazione Set-Cookie, quando si utilizza il plugin JunctionRewrite

La direttiva consente al proxy di riscrivere l'opzione di percorso nell'intestazione Set-Cookie quando il nome cookie viene confrontato. Se la risposta richiede una giunzione e il prefisso di questa è definito, il prefisso verrà inserito prima di ciascun percorso. Può essere utilizzata con il plugin JunctionRewrite o con al direttiva RewriteSetCookieDomain.

Formato

```
JunctionRewriteSetCookiePath nome1-cookie nome2-cookie...
```

nome-cookie
Un nome cookie nell'intestazione Set-Cookie.

Impostazione predefinita

Nessuna

JunctionSkipUrlPrefix — Indica di ignorare la riscrittura degli URL che già contengono il prefisso, quando si utilizza il plugin JunctionRewrite

Questa direttiva non tiene conto dell'azione predefinita del plugin JunctionRewrite, ignorando la riscrittura dell'URL in caso di corrispondenza del modello URL. Funziona insieme al plugin JunctionRewrite, offrendo un modo per correggere alcuni collegamenti URL nella pagina html. Normalmente, la direttiva viene utilizzata per ignorare gli URL che già includono un prefisso.

Formato

```
JunctionSkipUrlPrefix modello_url
```

Esempio

```
JunctionSkipUrlPrefix  /server1/*
```

In questo esempio, l'URL è /server1/notes.nsf e il prefisso giunzione è /server1/. Anziché riscrivere l'URL in /server1/server1/notes.nsf, il plugin JunctionRewrite ignora la riscrittura dell'URL che rimane invariato, ossia /server1/notes.nsf.

Impostazione predefinita

Nessuna

KeepExpired — Indica di specificare la restituzione della copia scaduta della risorsa, se questa è stata aggiornata sul proxy

Utilizzare questa direttiva per evitare di sovraccaricare i server di backend con richieste mentre l'oggetto cache è in fase di riconvalida.

Quando un oggetto cache deve essere riconvalidato con il contenuto sul server di backend, le richieste per la medesima risorsa verranno delegate al server di backend. A volte, il server di backend si interrompe a causa di un numero considerevole di richieste identiche. Abilitando questa direttiva, è possibile evitare questa situazione. Quando la direttiva è abilitata, viene restituita una copia scaduta o obsoleta della risorsa, se questa è in fase di aggiornamento sul proxy.

Formato

```
KeepExpired {on | off}
```

Impostazione predefinita

```
KeepExpired off
```

KeyRing — Indica di specificare il percorso file al database di chiavi

Utilizzare questa direttiva per specificare il percorso file al database di chiavi utilizzato dal server per le richieste SSL. I file di chiavi vengono generati per mezzo del programma di utilità gestore chiavi iKeyman.

Nota: le direttive SSL non sono supportate su SUSE Linux.

Formato

```
KeyRing nomefile
```

Esempi
Windows: `KeyRing c:\Programmi\IBM\edge\cp\\key.kdb`

Linux e UNIX: `KeyRing /etc/key.kdb`

Impostazione predefinita
Nessuna

KeyRingStash — Indica di specificare il percorso al file password del database di chiavi

Utilizzare questa direttiva per specificare il percorso al file password del database di chiavi. Il file password viene generato per mezzo del programma di utilità gestore chiavi iKeyman, quando si crea un file database di chiavi.

Nota: le direttive SSL non sono supportate su SUSE Linux.

Formato
`KeyRingStash` *`percorso_file`*

Esempi
Windows: `KeyRingStash c:\Programmi\IBM\edge\cp\key.sth`

Linux e UNIX: `KeyRingStash /etc/key.sth`

Impostazione predefinita
Nessuna

LimitRequestBody — Indica di specificare la dimensione corpo massima nelle richieste PUT o POST

Utilizzare questa direttiva per controllare la dimensione corpo massima nelle richieste PUT o POST. Le direttive LimitRequest vengono utilizzate per proteggere il proxy da eventuali attacchi.

Il valore può essere specificato in kilobyte (K), megabyte (M) o gigabyte (G).

Formato
`LimitRequestBody` *`dimensione_corpo_max`* `{K | M | G}`

Impostazione predefinita
`LimitRequestBody 10 M`

LimitRequestFields — Indica di specificare il numero massimo di intestazioni nelle richieste client

Utilizzare questa direttiva per specificare il numero massimo di intestazioni che possono essere inviate nelle richieste client. Le direttive LimitRequest vengono utilizzate per proteggere il proxy da eventuali attacchi.

Formato
`LimitRequestFields` *`numero_intestazioni`*

Impostazione predefinita
`LimitRequestFields 32`

LimitRequestFieldSize — Indica di specificare la lunghezza massima dell'intestazione e della riga della richiesta

Utilizzare questa direttiva per specificare la lunghezza massima della riga della richiesta e di ciascuna intestazione in una richiesta. Le direttive LimitRequest vengono utilizzate per proteggere il proxy da eventuali attacchi.

Il valore può essere specificato in byte (B) o kilobyte (K).

Formato

```
LimitRequestFieldSize lunghezza_intestazione_max {B | K}
```

Impostazione predefinita

```
LimitRequestFieldSize 4096 B
```

ListenBacklog — Indica di specificare il numero di connessioni client backlog di ascolto che il server può supportare

Utilizzare questa direttiva per specificare il numero di connessioni client backlog di ascolto che il server può supportare prima di inviare ai client messaggi che indicano che la connessione è stata rifiutata. Questo numero dipende dal numero di richieste che il server può elaborare in pochi secondi. Non impostare questo numero su un valore superiore al numero che il server può tollerare prima che si verifichi il timeout dei client e la connessione si interrompa.

Nota: se il valore di ListenBacklog è superiore al valore SOMAXCONN supportato da TCP/IP, verrà utilizzato il valore SOMAXCONN.

Formato

```
ListenBacklog numero_di_richieste
```

Impostazione predefinita

```
ListenBacklog 128
```

LoadInlineImages — Indica di controllare l'aggiornamento di immagini incorporate

Utilizzare questa direttiva per specificare se le immagini in linea vengono richiamate dall'agente cache. Se LoadInlineImages è impostata su `on`, le immagini incorporate in una pagina che deve essere memorizzata nella cache verranno anch'esse memorizzate. Se impostata su `off`, le immagini incorporate non verranno memorizzate nella cache.

Formato

```
LoadInlineImages {on | off}
```

Impostazione predefinita

```
LoadInlineImages on
```

LoadTopCached — Indica di specificare il numero delle pagine più utilizzate da aggiornare

Utilizzare questa direttiva per indicare all'agente cache di accedere al log accessi cache della sera precedente e di caricare gli URL più richiesti.

Quando si imposta un valore per la direttiva LoadTopCached, è necessario impostare la direttiva Caching su `On` e un valore per la direttiva CacheAccessLog.

Formato

`LoadTopCached` *`numero_di_pagine`*

Impostazione predefinita

```
LoadTopCached 100
```

LoadURL — Indica di specificare gli URL da aggiornare

Utilizzare questa direttiva per specificare gli URL che l'agente cache deve caricare nella cache. Nel file di configurazione, è possibile includere più direttive LoadURL ma non è possibile utilizzare caratteri jolly.

Formato

`LoadURL` *`url`*

Esempio

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

Impostazione predefinita

Nessuna

Log — Indica di personalizzare la fase Log

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata che deve essere richiamata dal server durante la fase Log. Questo codice consente di eseguire registrazioni e altre elaborazioni dopo la chiusura della connessione.

Formato

`Log` *`maschera_richiesta`*
`/percorso/file``:`*`nome_funzione`*

`maschera_richiesta`
Specifica una maschera per richieste che determina ulteriormente se la funzione applicativa viene chiamata. La specifica include il protocollo, il dominio e l'host; può essere preceduta da un carattere barra (/) ed è possibile utilizzare l'asterisco (*) come carattere jolly. Ad esempio, `/front_page.html`, `http://www.ics.raleigh.ibm.com`, `/pub*`, `/*` e `*` sono tutti validi.

`/percorso/file`
Specifica il nome file completo del programma compilato e include l'estensione.

`nome_funzione`
Specifica il nome della funzione applicativa all'interno del programma. È necessario specificare i nomi delle funzioni open, write e close.

Esempio

```
Log /index.html /api/bin/icsextpgm.so:log_url
```

Impostazione predefinita

Nessuna

LogArchive — Indica di specificare il funzionamento dell'archiviazione log

Utilizzare questa direttiva per specificare il funzionamento della routine di archiviazione. Questa direttiva influisce su tutti i log con impostazioni globali. Specifica se i log vengono compressi o eliminati oppure se non sono sottoposti ad alcuna operazione.

Se si specifica `Compress`, utilizzare le direttive CompressAge e CompressDeleteAge per specificare quando i log sono compressi o eliminati. Utilizzare la direttiva CompressCommand per specificare il comando e i relativi parametri da utilizzare.

Se si specifica `Purge`, utilizzare le direttive PurgeAge e PurgeSize per specificare il momento in cui i log vengono eliminati.

Formato

```
LogArchive {Compress | Purge | none}
```

Compress
Specifica che la routine di archiviazione comprime i log.

Purge
Specifica che la routine di archiviazione elimina i log.

none
Specifica che la routine di archiviazione non esegue nulla.

Impostazione predefinita

```
LogArchive Purge
```

Direttive correlate

- "CompressAge — Indica di specificare quando comprimere i log" a pagina 190
- "CompressDeleteAge — Indica di specificare quando eliminare i log" a pagina 192
- "CompressCommand — Indica di specificare il comando di compressione e i parametri" a pagina 191
- "Midnight — Indica di specificare il plugin dell'API utilizzato per archiviare i log" a pagina 229
- "PurgeAge — Indica di specificare la durata di un log" a pagina 252
- "PurgeSize — Indica di specificare il limite della dimensione dell'archivio log" a pagina 253

LogFileFormat — Indica di specificare il formato del log accessi

Utilizzare questa direttiva per specificare il formato dei file di log accessi.

Formato

```
LogFileFormat  {common | combined}
```

Per impostazione predefinita, i log vengono visualizzati nel formato di log comune NCSA. Specificare `combined` per visualizzare i log nel formato combinato NCSA. Questo formato aggiunge i campi per URL di riferimento, Agente utente e Cookie (se presenti nella richiesta).

Impostazione predefinita

```
LogFileFormat  common
```

LogToGUI (solo Windows) — Indica di visualizzare le voci di log nella finestra server

Solo sistemi Windows. Quando il proxy viene eseguito dalla riga comandi, utilizzare questa direttiva per inviare l'output al log accessi. Per ottimizzare le prestazioni, per impostazione predefinita, questa direttiva è impostata su `off` (disabilitata).

Nota: questa direttiva non ha effetto durante l'esecuzione del proxy come servizio.

Formato

```
LogToGUI  {on | off}
```

Impostazione predefinita

```
LogToGUI off
```

LogToSyslog — Indica di specificare l'invio delle informazioni di accesso al log di sistema (solo Linux e UNIX)

Solo sistemi Linux e UNIX. Utilizzare questa direttiva per specificare se il server registra le richieste di accesso e gli errori nel log di sistema oltre che nei file di log relativi agli accessi e agli errori.

Formato

```
LogToSyslog {on | off}
```

Il file di log di sistema deve essere presente sul server per poter specificare di scrivervi le informazioni del log errori. Si può scegliere se registrare le informazioni di accesso, di errore o entrambe.

Per inviare solo le informazioni di errore sul log di sistema, aggiungere la seguente riga al file /etc/syslog.conf:

```
user.err file_output_syslog_per_informazioni_errore
```

Per inviare solo le informazioni di accesso sul log di sistema, aggiungere la seguente riga al file /etc/syslog.conf:

```
user.info file_info_syslog_per_informazioni_accesso
```

Per inviare le informazioni di errore e di accesso al log di sistema, aggiungere la seguente riga al file/etc/syslog.conf:

Specificare *file_output_syslog* e *file_info_syslog* nei seguenti formati:

- **AIX:** `/var/adm/nome_file_syslog`
- **HP-UX:** `/var/adm/syslog/syslog.log`
- **Linux:** `/var/adm/messages`
- **Solaris:** `/var/adm/messages`

Dopo aver creato il file di log di sistema, è possibile riavviarlo con il seguente comando:

```
kill -HUP 'cat /etc/syslog.pid'
```

Impostazione predefinita

```
LogToSyslog Off
```

Map — Indica di modificare le richieste corrispondenti con una nuova stringa richiesta

Utilizzare questa direttiva per specificare una maschera per le richieste da modificare con una nuova stringa richiesta. Una volta che il server ha modificato la richiesta, acquisisce la nuova stringa e la confronta con le maschere richiesta sulle direttive successive.

Formato

`Map` *`maschera_richiesta nuova_richiesta`* [*`indirizzo_IP_server`* | *`nome_host`*]

`maschera_richiesta`
Specifica una maschera per le richieste che il server modifica, quindi continua a confrontare la nuova stringa richiesta con altre maschere.

Nella maschera, è possibile utilizzare un asterisco (*) come carattere jolly. Il carattere tilde (~), subito dopo una barra (/), deve essere confrontato in modo esplicito; infatti per questa operazione non è possibile utilizzare un carattere jolly.

`nuova_richiesta`
Specifica la nuova stringa richiesta con cui il server continua a confrontare i modelli richiesta sulle direttive successive. La stringa specificata con *`nuova_richiesta`* può contenere un carattere jolly se *`maschera_richiesta`* ne ha uno. La parte della richiesta che corrisponde al carattere jolly *`maschera_richiesta`* viene inserita al posto del carattere jolly in *`nuova_richiesta`*.

[*`indirizzo_IP_server`* | *`nome_host`*]
Se si utilizzano più indirizzi IP o host virtuali, utilizzare questo parametro per specificare un indirizzo IP o un nome host. Il server utilizza la direttiva esclusivamente per le richieste inviate al server su questo indirizzo IP o per questo host. Per un indirizzo IP, si tratta dell'indirizzo della connessione di rete del server e non dell'indirizzo del client richiedente.

È possibile specificare un indirizzo IP (ad esempio, `240.146.167.72`) o un nome host (ad esempio, `hostA.raleigh.ibm.com`).

Questo parametro è opzionale. Senza questo parametro, il server utilizza la direttiva per tutte le richieste a prescindere dall'indirizzo IP su cui è stata ricevuta la richiesta o dal nome host nell'URL.

Per un indirizzo IP del server non è possibile specificare un carattere jolly.

Esempi

- Nell'esempio riportato di seguito, il server acquisisce ogni richiesta che inizia con `/stuff/` e modifica la parte `/stuff/` della richiesta con `/good/stuff/`. Anche tutto quello che segue `/stuff/` sulla richiesta originale viene incluso nella nuova stringa richiesta. Perciò, `/stuff/whatsup/` viene modificato in `/good/stuff/whatsup/`. Il server acquisisce la nuova stringa richiesta e continua a confrontarla con le maschere richiesta sulle direttive successive.

  ```
  Map  /stuff/*   /good/stuff/*
  ```

- Nell'esempio riportato di seguito viene utilizzato il parametro dell'indirizzo IP opzionale. Se il server riceve richieste che iniziano con `/stuff/`, modifica la richiesta con una stringa richiesta differente, in base all'indirizzo IP della connessione di rete su cui è arrivata la richiesta. Per le richieste che arrivano su 240.146.167.72, il server modifica la parte `/stuff/` della richiesta in `/customerA/good/stuff/`. Per le richieste che arrivano su una qualsiasi

connessione con un indirizzo 0.83.100.45, il server modifica la parte /stuff/ della richiesta in /customerB/good/stuff/.

```
Map   /stuff/*   /customerA/good/stuff/*   240.146.167.72
Map   /stuff/*   /customerB/good/stuff/*   0.83.104.45
```

- Nell'esempio riportato di seguito viene utilizzato il parametro del nome host opzionale. Se il server riceve richieste che iniziano con /stuff/, le modifica con una stringa richiesta differente, in base al nome host nell'URL. Per le richieste che arrivano per hostA, il server modifica la parte /stuff/ della richiesta in /customerA/good/stuff//. Per le richieste che arrivano per hostB, il server modifica la parte /stuff/ della richiesta in /customerB/good/stuff/.

```
Map   /stuff/*   /customerA/good/stuff/*   hostA.bcd.com
Map   /stuff/*   /customerB/good/stuff/*   hostB.bcd.com
```

Impostazione predefinita

Nessuna

MaxActiveThreads — Indica di specificare il numero massimo di thread attivi

Utilizzare questa direttiva per impostare il numero massimo di thread attivi contemporaneamente. Quando viene raggiunto il numero massimo, il server trattiene le nuove richieste fino al completamento di un'altra richiesta, che libera i thread. Generalmente, più la macchina è potente, più il numero impostato per questa direttiva sarà elevato. Se una macchina inizia a impiegare troppo tempo su attività generali, quali lo swapping della memoria, ridurre questo valore.

Formato

```
MaxActiveThreads numero_di_thread
```

Impostazione predefinita

```
MaxActiveThreads 100
```

MaxContentLengthBuffer — Indica di specificare la dimensione del buffer per dati dinamici

Utilizzare questa direttiva per impostare la dimensione del buffer per i dati dinamici generati dal server. I dati dinamici provengono da programmi CGI, inclusioni lato server e programmi API.

Il valore può essere specificato in byte (B), kilobyte (K), megabyte (M) o gigabyte (G). La presenza di uno spazio tra il numero e il valore (B, K, M, G) è irrilevante.

Formato

```
MaxContentLengthBuffer dimensione
```

Impostazione predefinita

```
MaxContentLengthBuffer 100 K
```

MaxLogFileSize — Indica di specificare la dimensione massima per ciascun file di log

Utilizzare questa direttiva per specificare la dimensione massima di ciascun file di log. Ciascun file di log non può superare la dimensione definita da questa direttiva. Quando un file di log raggiunge la dimensione massima definita, il file di log corrente viene chiuso e ne viene creato uno nuovo con lo stesso nome, a cui viene aggiunto il valore intero incrementale successivo.

Note:

1. Caching Proxy è un'applicazione a 32 bit che apre i propri file di log con una funzione a 32 bit. A causa di questa limitazione, *non* specificare una direttiva MaxLogFileSize superiore a 2 GB. Se il file di log supera la dimensione di 2 GB, Caching Proxy può bloccarsi se tenta di scrivere nel file di log mentre sta ancora elaborando attivamente le richieste.
2. Su piattaforme Linux e UNIX, i file di log non vengono creati se le autorizzazioni della directory su cui risiedono i file di log non includono autorizzazioni di scrittura almeno per il gruppo su cui è in esecuzione il daemon ibmproxy. In altre parole, le posizioni dei file di log per registrare le direttive nel file ibmproxy.conf devono disporre di autorizzazioni di scrittura almeno per il gruppo definito dalla direttiva GroupId nel file ibmproxy.conf. Può trattarsi di un problema solo se la posizione predefinita dei file di log è stata modificata o se la direttiva UserId o GroupId predefinita è stata modificata nel file ibmproxy.conf.

La dimensione massima può essere specificata in una delle seguenti unità: byte (B), kilobyte (K), megabyte (M) e gigabyte (G).

Formato

```
MaxLogFileSize dimensione massima {B | K | M | G}
```

Impostazione predefinita

```
MaxLogfileSize 128 M
```

MaxPersistRequest — Indica di specificare il numero massimo di richieste da ricevere su una connessione permanente

Utilizzare questa direttiva per specificare il numero massimo di richieste che il server riceve su una connessione permanente. Quando si determina questo numero, considerare la quantità delle immagini presenti nelle pagine. Ciascuna immagine deve disporre di una richiesta separata.

Formato

```
MaxPersistRequest numero
```

Impostazione predefinita

```
MaxPersistRequest 5
```

MaxQueueDepth — Indica di specificare il numero massimo di URL da accodare

Utilizzare questa direttiva per specificare il livello massimo della coda dell'agente cache che contiene le richieste di richiamo pagine in attesa. Se si dispone di un sistema di grandi dimensioni con una notevole quantità di memoria, è possibile definire una coda di richieste di richiamo pagine più grande senza utilizzare tutta la memoria disponibile.

La coda di URL da memorizzare nella cache viene determinata all'avvio di ogni esecuzione dell'agente cache. Se si indica all'agente cache di seguire i collegamenti ipertestuali ad altri URL, questi non verranno conteggiati nel livello della coda cache. Quando si raggiunge il valore specificato nella direttiva MaxURLs, l'agente cache si arresta, anche in presenza di altri URL nella coda.

Formato

```
MaxQueueDepth livello_massimo
```

Impostazione predefinita

```
MaxQueueDepth 250
```

MaxRuntime — Indica di specificare il tempo massimo di esecuzione di un agente cache

Utilizzare questa direttiva per specificare il tempo massimo che l'agente cache ha a disposizione per richiamare gli URL durante una specifica esecuzione. Un valore pari a `0` indica che l'agente cache sarà in esecuzione fino al completamento.

Formato

```
MaxRuntime {0 | tempo_massimo}
```

Esempio

```
MaxRuntime 2 hours 10 minutes
```

Impostazione predefinita

```
MaxRuntime 2 hours
```

MaxSocketPerServer — Indica di specificare il numero massimo di socket aperti per server

Utilizzare questa direttiva per impostare il numero massimo di socket aperti da mantenere per qualsiasi server di origine. Utilizzare questa direttiva solo se la direttiva ServerConnPool è impostata su `on`.

Formato

```
MaxSocketPerServer num
```

Esempio

```
MaxSocketPerServer 10
```

Impostazione predefinita

```
MaxSocketPerServer 5
```

MaxUrls — Indica di specificare il numero massimo di URL da aggiornare

Utilizzare questa direttiva per specificare il numero massimo di URL richiamati dall'agente cache durante una specifica esecuzione. Un valore pari a `0` indica che non ci sono limiti. Quando si utilizza la modalità automatica dell'agente cache, le direttive LoadURL e LoadTopCached hanno la precedenza su MaxURLs.

Formato

```
MaxURLs numero_massimo
```

Impostazione predefinita

```
MaxURLs 2000
```

Member — Indica di specificare un membro di una matrice

Utilizzare questa direttiva per specificare i membri delle matrici condivisi dai server mediante la funzione RCA (Remote Cache Access).

Nota: durante l'impostazione di una matrice, configurare la direttiva Hostname in modo identico su tutti i membri della matrice.

Formato

```
Member nome {
sottodirettiva
sottodirettiva
.
.
}
```

Sono incluse le seguenti sottodirettive:

RCAAddr
Questa sottodirettiva obbligatoria identifica l'indirizzo IP o il nome host per la comunicazione RCA.

RCAPort
Questa sottodirettiva obbligatoria identifica la porta per le comunicazioni RCA. Il numero di porta deve essere maggiore di 1024 e minore di 65535.

CacheSize {*n* bytes | *n* Kbytes | *n* Mbytes | *n* Gbytes}
Questa sottodirettiva obbligatoria identifica la dimensione della cache di questo membro, che deve essere un valore positivo.

[Timeout *n* milliseconds | *n* seconds | *n* hours | *n* days | *n* months | *n* years | forever]
Identifica il tempo di attesa di questo membro. *n* deve essere un valore intero positivo. `Timeout` è opzionale; il valore predefinito è `1000 millisecondi`. I valori di timeout sono generalmente espressi in secondi o millisecondi.

[BindSpecific {on | off}]
Consente le comunicazioni su una sottorete privata, offrendo una misura di sicurezza. `BindSpecific` è opzionale; il valore predefinito è `On`.

[ReuseAddr {on | off}]
Consente di riunire velocemente una matrice; se impostata su `On`, altri processi si approprieranno della porta causando un funzionamento indefinito. `ReuseAddr` è opzionale; il valore predefinito è `Off`.

Esempio

```
Member bittersweet.chocolate.ibm.com {
  RCAAddr      127.0.0.1
  RCAPort      6294
  CacheSize    25G
  Timeout      500 milliseconds
  BindSpecific On
  ReuseAddr    Off
  }
```

Impostazione predefinita

Nessuna

Midnight — Indica di specificare il plugin dell'API utilizzato per archiviare i log

Utilizzare questa direttiva per specificare il plugin dell'applicazione in esecuzione a mezzanotte per archiviare i log. Questa direttiva viene inizializzata durante l'installazione. Se questa direttiva non è inclusa nel file di configurazione, l'archiviazione non viene eseguita.

Formato

```
Midnight /percorso/file:nome_funzione
```

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

Impostazioni predefinite

- **Linux e UNIX:** `Midnight /usr/lib/archive.so:begin`
- **Windows:** `Midnight C:\Programmi\IBM\edge\cp\\bin\archive.dll:begin`

NameTrans — Indica di personalizzare la fase Conversione nome

Utilizzare questa direttiva per specificare una funzione applicativa personalizzate richiamata dal server durante la fase Conversione nome. Questo codice fornisce il meccanismo per convertire il percorso virtuale nella richiesta nel percorso fisico sul server, mappando gli URL su specifici oggetti.

Nota: non si tratta di una regola di mappatura terminale. L'URL trasformato deve ancora corrispondere a una delle direttive della regola di mappatura terminale, come Exec, Fail, Map, Pass, Redirect e Service.

Formato

```
NameTrans maschera_richiesta /percorso/file:nome_funzione
  [indirizzo_IP_server | nome_host]
```

maschera_richiesta
Specifica una maschera per richieste che determina ulteriormente se la funzione applicativa viene chiamata. La specifica include il protocollo, il dominio e l'host; può essere preceduta da un carattere barra (/) ed è possibile utilizzare l'asterisco (*) come carattere jolly. Ad esempio, `/front_page.html`, `http://www.ics.raleigh.ibm.com`, `/pub*`, `/*` e `*` sono tutti validi.

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

[*indirizzo_IP_server* | *nome_host***]**
Se si utilizzano più indirizzi IP o host virtuali, determina se la funzione applicativa viene richiamata solo per le richieste inviate a uno specifico indirizzo IP o per un determinato host.

Per un indirizzo IP del server non Þ possibile specificare un carattere jolly.

Nota: la direttiva deve essere specificata su una riga, anche se in questo caso è mostrata su due righe per facilitarne la lettura.

Esempio

```
NameTrans /index.html /api/bin/icsextpgm.so:trans_url
```

Impostazione predefinita

Nessuna

NoBG — Indica di eseguire il processo Caching Proxy in primo piano

Su piattaforme Linux e UNIX, utilizzare questa direttiva per impedire che il processo server Caching Proxy venga eseguito automaticamente in background. Per impostazione predefinita, la direttiva, impostata su off, ha il seguente formato:

```
NoBG [on | off]
```

Nota: L'opzione **-nobg** del comando **ibmproxy** non è valida sui sistemi Windows.

Esempio

```
NoBG on
```

Impostazione predefinita

```
NoBG off
```

NoCaching — Indica di specificare di non memorizzare nella cache i file con URL corrispondenti a una maschera

Utilizzare questa direttiva per specificare che il server non memorizza nella cache i file con URL che corrispondono alla maschera specificata. È possibile includere più occorrenze di questa direttiva nel file di configurazione. Includere una direttiva separata per ciascuna maschera. La maschera URL deve contenere il protocollo.

Se la direttiva CacheOnly o NoCaching non è impostata, qualsiasi URL può essere memorizzato nella cache.

Formato

```
NoCaching modello_URL
```

Esempio

```
NoCaching http://joke/*
```

Impostazione predefinita

Nessuna

NoLog — Indica di eliminare le voci di log per host o domini specifici che corrispondono a una maschera

Utilizzare questa direttiva per specificare che le richieste di accesso effettuate da host o domini specifici che corrispondono a una maschera prescelta non verranno registrate. Ad esempio, non si desidera registrare le richieste di accesso di host locali.

È possibile includere più occorrenze di questa direttiva nel file di configurazione. Inoltre, è possibile inserire più maschere sulla stessa direttiva, purché vengano separate da uno o più spazi. È possibile utilizzare nomi host o indirizzi IP sulle maschere.

Nota: per utilizzare le maschere nomi host, è necessario impostare la direttiva DNS-Lookup su `On`. Se la direttiva DNS-Lookup è impostata su `Off` (il valore predefinito), è possibile utilizzare solo maschere indirizzi IP.

Formato

```
NoLog  {nome_host | indirizzo_IP}  [...]
```

Esempio

```
NoLog 128.0.*  *.edu  localhost.*
```

Impostazione predefinita

Nessuna

no_proxy — Indica di specificare le maschere per la connessione diretta ai domini

Se si utilizza la direttiva http_proxy, ftp_proxy o gopher_proxy per le catene di proxy, è possibile utilizzare questa direttiva per specificare i domini a cui il server si collega direttamente anziché passare per un proxy.

Specificare un valore come una stringa di nomi dominio o maschere nomi dominio. Separare ciascuna voce nella stringa con una virgola (,). *Non* utilizzare spazi nella stringa.

Le maschere in questa direttiva vengono inserite in modo differente rispetto ad altre direttive. Inoltre, *non è possibile* utilizzare caratteri jolly (*). È *possibile* specificare una maschera includendo solo l'ultima parte di un nome dominio. Il server si collega direttamente a qualsiasi dominio che termina con una stringa corrispondente alle maschere specificate. Questa direttiva si applica solo a catene di proxy ed è equivalente a una riga `@/=` diretta nel file di configurazione SOCKS.

Formato

```
no_proxy  nome_dominio_o_maschera[,...]
```

Esempio

```
no_proxy   www.someco.com,.raleigh.ibm.com,.some.host.org:8080
```

In questo esempio, il server non passa attraverso un proxy per le seguenti richieste:

- Qualsiasi richiesta ai domini che terminano con www.someco.com
- Qualsiasi richiesta ai domini che terminano con .raleigh.ibm.com, come blugrass.raleigh.ibm.com o keystone.raleigh.ibm.com
- Qualsiasi richiesta alla porta 8080 di domini che terminano con .some.host.org, come myname.some.host.org:8080. (Non sono incluse le richieste ad altre porte, come myname.some.host.org, che utilizzano la porta predefinita 80.)

Impostazione predefinita

Nessuna

NoProxyHeader — Indica di specificare le intestazioni client da bloccare

Utilizzare questa direttiva per specificare le intestazioni URL client da bloccare. Le intestazioni HTTP inviate da un client, comprese le intestazioni obbligatorie, possono essere bloccate. Fare attenzione mentre si bloccano le intestazioni. Tra le intestazioni comuni sono incluse:

- `Pragma:`— Normalmente utilizzata per comunicare a browser e server con cache di utilizzare il file del server originale per ogni richiesta del file.
- `Referer:`— URL del file da cui si ottiene Request-URI.

Consultare la specifica del protocollo HTTP, per i dettagli su queste e altre informazioni. È possibile utilizzare questa direttiva più volte.

Formato

```
NoProxyHeader intestazione
```

Esempio

```
NoProxyHeader Referer:
```

Impostazione predefinita

Nessuna

NumClients — Indica di specificare il numero di thread agente cache da utilizzare

Utilizzare questa direttiva per specificare il numero di thread utilizzati dall'agente cache per richiamare le pagine nella coda. Basare il numero di thread sulla velocità della rete interna e del collegamento a Internet. L'intervallo di valori consentito è compreso tra 1 e 100.

Nota: se si utilizzano più di sei thread, la velocità delle richieste sui server di contenuti potrebbe essere eccessiva.

Formato

```
NumClients numero
```

Impostazione predefinita

```
NumClients 4
```

ObjectType — Indica di personalizzare la fase Tipo di oggetto

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata richiamata dal server durante la fase Tipo di oggetto. Questo codice individua gli oggetti richiesti nel file system e ne specifica il tipo MIME.

Formato

```
ObjectType maschera_richiesta /percorso/file:nome_funzione
```

maschera_richiesta
: Specifica una maschera per richieste che determina ulteriormente se la funzione applicativa viene chiamata. La specifica include il protocollo, il dominio e l'host; può essere preceduta da un carattere barra (/) ed è possibile utilizzare l'asterisco (*) come carattere jolly. Ad esempio, `/front_page.html`, `http://www.ics.raleigh.ibm.com`, `/pub*`, `/*` e `*` sono tutti validi.

/percorso/file
: Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
: Specifica il nome della funzione applicativa all'interno del programma.

Esempio

```
ObjectType /index.html /api/bin/icsextpgm.so:obj_type
```

Impostazione predefinita

Nessuna

OutputTimeout — Indica di specificare il timeout dell'output

Utilizzare questa direttiva per impostare il tempo massimo consentito al server per inviare l'output a un client. Il limite di tempo è valido per le richieste di file locali

e per le richieste per cui il server funge da proxy. Questo limite non è valido per le richieste che avviano un programma CGI locale.

Se il server non invia la risposta completa entro il limite di tempo specificato su questa direttiva, interrompe il collegamento. Il valore tempo può essere specificato come una qualsiasi combinazione di ore, minuti (o min) e secondi (o sec).

Formato

```
OutputTimeout tempo
```

Impostazione predefinita

```
OutputTimeout 30 minutes
```

PacFilePath — Indica di specificare la directory contenente i file PAC

Utilizzare questa direttiva per specificare la directory contenente i file di auto-configurazione proxy generati utilizzando il modulo file PAC di configurazione remoto.

Formato

```
PacFilePath percorso_directory
```

Impostazioni predefinite

- **Windows:** `PacFilePath c:\Programmi\IBM\edge\cp\\HTML\pacfiles`
- **Linux e UNIX:** `PacFilePath /opt/ibm/edge/cp/server_root/pub/pacfiles`

Pass — Indica di specificare la maschera per accettare le richieste

Utilizzare questa direttiva per specificare una maschera per le richieste che si intende accettare e a cui si desidera rispondere con un file dal server. Se una richiesta corrisponde a una maschera su una direttiva Pass, non viene confrontata con le maschere richiesta sulle direttive successive.

Formato

```
Pass  maschera_richiesta [percorso_file [indirizzo_IP_server | nome_host]]
```

maschera_richiesta
Specifica una maschera per le richieste che il server deve accettare e a cui deve rispondere con un file.

Nella maschera, è possibile utilizzare un asterisco (*) come carattere jolly. Il carattere tilde (~), subito dopo una barra (/), deve essere confrontato in modo esplicito; infatti per questa operazione non è possibile utilizzare un carattere jolly.

[*percorso_file***]**
Specifica il percorso del file che il server deve restituire. Il *percorso_file* può contenere un carattere jolly, se presente in *maschera_richiesta*. La parte della richiesta che corrisponde al carattere jolly *maschera_richiesta* viene inserita al posto del carattere jolly in *percorso_file*.

Questo parametro è opzionale. Se non si specifica un percorso, la richiesta stessa viene utilizzata come percorso.

[*indirizzo_IP_server* | *nome_host***]**
Se si utilizzano più indirizzi IP o host virtuali, utilizzare questo parametro per specificare un indirizzo IP o un nome host. Il server utilizza la direttiva

esclusivamente per le richieste inviate al server su questo indirizzo IP o per questo host. Per un indirizzo IP, si tratta dell'indirizzo della connessione di rete del server e non dell'indirizzo del client richiedente.

È possibile specificare un indirizzo IP (ad esempio, `240.146.167.72`) o un nome host (ad esempio, `hostA.raleigh.ibm.com`).

Questo parametro è opzionale. Senza questo parametro, il server utilizza la direttiva per tutte le richieste a prescindere dall'indirizzo IP su cui è stata ricevuta la richiesta o dal nome host nell'URL.

Per un indirizzo IP del server non è possibile specificare un carattere jolly.

Esempi

- Negli esempi riportati di seguito, il server risponde a una richiesta che inizia con `/updates/parts/` con un file dal percorso in elenco, a seconda del sistema operativo. Anche tutto ciò che segue `/updates/parts/` viene utilizzato per specificare il file.

  Sistemi Linux e UNIX: `Pass /updates/parts/* /opt/ibm/edge/cp/server_root/pub/*`

  Sistemi Windows: `Pass /updates/parts/* c:\Programmi\IBM\edge\cp\pub\*`

- Nell'esempio riportato di seguito, il server risponde a una richiesta che inizia con `/gooddoc/` con un file della directory /gooddoc. Quindi il server risponde alla richiesta `/gooddoc/volume1/issue2/newsletter4.html` con il documento nel file /gooddoc/volume1/issue2/newsletter4.html.

  ```
  Pass /gooddoc/*
  ```

- Nell'esempio riportato di seguito viene utilizzato il parametro dell'indirizzo IP opzionale. Se il server riceve richieste che iniziano con `/parts/`, restituisce un file da una directory differente, in base all'indirizzo IP della connessione di rete su cui è arrivata la richiesta. Per le richieste che arrivano su 240.146.167.72, il server restituisce un file da /customerA/catalog/. Per le richieste che arrivano su una connessione con indirizzo 0.83.100.45, il server restituisce un file da /customerB/catalog/.

  ```
  Pass   /parts/*   /customerA/catalog/*   240.146.167.72
  Pass   /parts/*   /customerB/catalog/*   0.83.100.45
  ```

- Nell'esempio riportato di seguito viene utilizzato il parametro del nome host opzionale. Se il server riceve richieste che iniziano con `/parts/`, restituisce un file da una directory differente, in base al nome host nell'URL. Per le richieste che arrivano per hostA, il server restituisce un file da /customerA/catalog/. Per le richieste che arrivano per hostB, il server resttuisce un file da /customerB/catalog/.

  Sistemi 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/*
  ```

  Sistemi Solaris, HP-UX e 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/*
  ```

Impostazioni predefinite

Sistemi AIX

```
Pass    /Admin/*    /usr/lpp/internet/server_root/Admin/*
Pass    /Docs/*     /usr/lpp/internet/server_root/Docs/*
Pass    /errorpages/*  /usr/lpp/internet/server_root/pub/errporpages/*
Pass    /*          /usr/lpp/internet/server_root/pub/*
```

Sistemi HP-UX, Linux e 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/*
```

Sistemi Windows

```
Pass    /icons/*    C:\Programmi\IBM\edge\cp\icons\*
Pass    /Admin/*    C:\Programmi\IBM\edge\cp\Admin\*
Pass    /Docs/*     C:\Programmi\IBM\edge\cp\Docs\*
Pass    /erropages/*  C:\Programmi\IBM\edge\cp\pub\errorpages\*
Pass    /*          C:\Programmi\IBM\edge\cp\pub\*
```

PersistTimeout — Indica di specificare il tempo di attesa del client prima di inviare un'altra richiesta

Utilizzare questa direttiva per specificare l'intervallo di tempo che il server attende tra le risposte del client prima di annullare una connessione permanente. Il tempo può essere specificato utilizzando un qualsiasi incremento valido ma normalmente viene espresso in secondi o minuti.

Il server utilizza una direttiva timeout differente, InputTimeout, per determinare il tempo di attesa per l'invio della prima richiesta da parte del client, dopo aver stabilito la connessione. Per ulteriori informazioni sul timeout di input, consultare "InputTimeout — Indica di specificare il timeout di input" a pagina 217.

Dopo l'invio della prima risposta, il server utilizza il valore impostato per la direttiva PersistTimeout per determinare il tempo di attesa tra una richiesta e l'altra, prima di annullare la connessione permanente.

Formato

```
PersistTimeout  tempo
```

Impostazione predefinita

```
PersistTimeout 4 seconds
```

PICSDBLookup — Indica di personalizzare la fase Richiamo etichetta PICS

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata che il server adopera per richiamare le etichette PICS di un determinato URL. La funzione consente di creare automaticamente un'etichetta PICS per il file richiesto o ricercarne una in un file o database alternativo.

Formato

```
PICSDBLookup  /percorso/file:nome_funzione
```

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

Esempio

```
PICSDBLookup  /api/bin/icsext05.so:get_pics
```

Impostazione predefinita

Nessuna

PidFile (solo Linux e UNIX) — Indica di specificare il file in cui memorizzare l'ID processo di Caching Proxy

Solo Linux e UNIX. Utilizzare questa direttiva per specificare la posizione del file che contiene l'ID processo di Caching Proxy. All'avvio del processo server, l'ID processo (PID) viene registrato in un file. Se più istanze del server sono in esecuzione su un unico sistema, ciascuna istanza deve disporre della propria direttiva PidFile.

Formato

```
PidFile percorso_a_info_file_pid
```

Esempio

```
PidFile /usr/pidinfo
```

Impostazioni predefinite

- Se viene specificata una direttiva ServerRoot: `PidFile server_root /ibmproxy-pid`
- Se non viene specificata alcuna direttiva ServerRoot: `PidFile /tmp/ibmproxy-pid`

Direttive del modulo plugin

Le direttive riportate di seguito sono state aggiunte al file Caching Proxy ibmproxy.conf per abilitare nuove funzioni e plugin. La maggior parte di queste direttive non può essere modificata con i moduli di configurazione e amministrazione. Utilizzare un editor di testo standard, quale vi o emacs, per modificarle manualmente. Ulteriori informazioni su ciascuna di queste direttive sono disponibili nel presente capitolo, in ordine alfabetico.

- "ExternalCacheManager — Indica di configurare Caching Proxy per Dynamic Caching di IBM WebSphere Application Server" a pagina 207
- "ICP_Address — Indica di specificare l'indirizzo IP per le query ICP" a pagina 213
- "ICP_Port — Indica di specificare il numero di porta per le query ICP" a pagina 215
- "ICP_Timeout — Indica di specificare il tempo massimo di attesa per le query ICP" a pagina 215
- "Occupier — Indica di specificare un membro di un cluster ICP" a pagina 214
- "ICP_MaxThreads — Indica di specificare il numero massimo di thread per le query ICP" a pagina 214
- "SignificantURLTerminator — Indica di specificare un codice di interruzione per le richieste URL" a pagina 263
- "SSLCertificate — Indica di specificare le etichette chiave per i certificati" a pagina 264
- "SSLOnly — Indica di disabilitare i thread per le richieste HTTP" a pagina 266

Nel file ibmproxy.conf, inserire le direttive utilizzate per configurare i moduli plugin di Caching Proxy nel seguente formato:

```
<MODULEBEGIN> nome plugin
sottodirettiva1
sottodirettiva2

<MODULEEND>
```

Ciascun programma plugin analizza il file ibmproxy.conf e legge solo il proprio blocco di direttive. Il programma di analisi di Caching Proxy trascura tutto ciò che è compreso tra <MODULEBEGIN> e <MODULEEND>.

I moduli plugin di Caching Proxy e alcune nuove funzioni richiedono di aggiungere le direttive API al file ibmproxy.conf. Dal momento che il server proxy interagisce con i moduli plugin nell'ordine in cui sono elencati, prestare attenzione quando si ordinano le direttive all'interno del file di configurazione proxy. Le direttive prototipo (sotto forma di commenti) sono state aggiunte alla sezione API del file ibmproxy.conf. L'ordine di queste direttive API è significativo. Quando di aggiungono direttive API per abilitare nuove funzioni e moduli plugin, l'ordine delle direttive viene illustrato nella sezione dei prototipi del file di configurazione. In alternativa, rimuovere il commento e modificare le direttive API, se necessario, per includere il supporto a ogni funzione o plugin prescelto. Aggiungere moduli plugin creati dall'utente dopo quelli forniti dal prodotto.

Port — Indica di specificare la porta su cui il server è in ascolto per ricevere richieste

Utilizzare questa direttiva per specificare il numero di porta su cui il server è in ascolto per ricevere richieste. Il numero di porta standard per HTTP è 80. Le porte con numero inferiore a 1024 sono riservate ad altre applicazioni TCP/IP e non devono essere utilizzate. Le porte comuni utilizzate per i server Web proxy sono la numero 8080 e 8008.

Quando viene utilizzata una porta diversa dalla 80, i client devono includere un numero di porta specifico sulle richieste al server. Il numero di porta è preceduto da un carattere due punti (:) e collocato dopo il nome host dell'URL. Ad esempio, dal browser, l'URL `http://www.turfco.com:8008/` richiede la pagina iniziale predefinita da un host denominato www.turfco.com, in ascolto sulla porta 8008.

Per non tenere conto di questa impostazione durante l'avvio del server, è possibile utilizzare l'opzione **-p** sul comando **ibmproxy**.

Formato

```
Port numero
```

Se la direttiva viene modificata, è necessario arrestare manualmente il server, quindi riavviarlo, per convalidare le modifiche. Il server non riconosce la modifica se viene solamente riavviato. (Consultare Capitolo 5, "Avvio e arresto di Caching Proxy", a pagina 15.)

Impostazione predefinita

```
Porta 80
```

PostAuth — Indica di personalizzare la fase PostAuth

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata richiamata dal server durante la fase PostAuth. Questo codice viene eseguito indipendentemente dai codici di ritorno delle fasi precedenti o di altri handler PostAuth e consente di deallocare le risorse assegnate per elaborare la richiesta.

Formato

```
PostAuth  /percorso/file:nome_funzione
```

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

Esempio

```
AuthExit  /ics/api/bin/icsext05.so:post_exit
```

Impostazione predefinita

Nessuna

PostExit — Consente di personalizzare la fase PostExit

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata richiamata dal server durante la fase PostExit. Questo codice viene eseguito indipendentemente dai codici di ritorno delle fasi precedenti o di altri handler PostExit e consente di deallocare le risorse assegnate per elaborare la richiesta.

Formato

```
PostExit  /percorso/file:nome_funzione
```

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

Esempio

```
PostExit  /ics/api/bin/icsext05.so:post_exit
```

Impostazione predefinita

Nessuna

PreExit — Indica di personalizzare la fase PreExit

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata richiamata dal server durante la fase PreExit. Questo codice viene eseguito in seguito alla lettura di una richiesta client ma prima di qualsiasi altra elaborazione. Durante questa fase, è possibile richiamare il modulo GoServe.

Formato

```
PreExit /percorso/file:nome_funzione
```

/percorso/file
Specifica il percorso completo al file DLL compilato, compresa l'estensione.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

Esempio

```
PreExit  /ics/api/bin/icsext05.so:pre_exit
```

Impostazione predefinita

Nessuna

Protect — Indica di attivare un'impostazione di protezione predefinita per le richieste che corrispondono a una maschera

Utilizzare questa direttiva per attivare le regole dell'impostazione di protezione per le richieste che corrispondono a una maschera.

Nota: per far funzionare correttamente la protezione, le direttive DefProt e Protect devono essere posizionate prima di qualsiasi direttiva Pass, Exec o Proxy nel file di configurazione.

Un'impostazione di protezione viene definita con sottodirettive di protezione. Il formato della direttiva Protect varia a seconda che si desideri puntare a un'etichetta o a un file contenente le sottodirettive di protezione oppure includere queste ultime in linea come parte della direttiva Protect.

Formato

Questo parametro può assumere i seguenti formati:

- La direttiva Protect può essere specificata come percorso completo o nome file di un file separato contenente le sottodirettive di protezione. Può essere inoltre specificata da un nome etichetta di impostazione protezione che corrisponde a un nome definito in precedenza su una direttiva Protection; quest'ultima contiene le sottodirettive di protezione. Utilizzare il seguente formato:

  ```
  Protect maschera_richiesta [file_impostazione | etichetta[
       [FOR indirizzo_IP_server | nome_host]
  ```

  Nota: la direttiva deve essere specificata su una riga, anche se in questo caso è mostrata su due righe.

- È possibile specificare le attuali sottodirettive di protezione in linea sulla direttiva Protect. Le sottodirettive vanno racchiuse tra parentesi ({}). Il carattere parentesi sinistra deve essere l'ultimo carattere sulla stessa riga della direttiva Protect. Ciascuna sottodirettiva deve proseguire sulla propria riga. Il carattere parentesi destra deve trovarsi sulla propria riga, di seguito alla riga dell'ultima sottodirettiva. Tra le parentesi non sono consentite righe di commenti. Per includere sottodirettive di protezione in linea, come parte della direttiva Protect, il formato è il seguente:

  ```
  Protect maschera_richiesta [FOR indirizzo_IP_server | nome_host]
      sottodirettiva  valore
      sottodirettiva  valore
      .
      .
      .
    }
  ```

Vengono utilizzati i parametri riportati di seguito:

maschera_richiesta
: Specifica una maschera per le richieste per cui si attiva la protezione. Il server confronta le richieste client in entrata con la maschera e, in caso di corrispondenza, attiva la protezione.

[*file_impostazione* | *etichetta***]**
: Se si punta a un'etichetta o a un file contenente le sottodirettive di protezione, questo parametro specifica l'impostazione di protezione da attivare per le richieste che corrispondono a *maschera_richiesta*.

  Questo parametro è opzionale. Se omesso, l'impostazione di protezione viene definita dalla direttiva DefProt più aggiornata contenente una maschera corrispondente.

[FOR *indirizzo_IP_server* | *nome_host*]

Se si utilizzano più indirizzi IP o host virtuali, utilizzare questo parametro per specificare un indirizzo IP o un nome host. Il server utilizza la direttiva esclusivamente per le richieste inviate al server su questo indirizzo IP o per questo host. Per un indirizzo IP, si tratta dell'indirizzo della connessione di rete del server e non dell'indirizzo del client richiedente. Se un indirizzo IP è protetto, verranno protetti anche l'indirizzo IP e il nome host completo. Tuttavia, se il server viene richiamato dalla rete utilizzando un nome diverso dal nome host completo, ad esempio, mediante una voce in un file nome host, non verrà protetto.

Esempio:

```
Protect http://x.x.x.x  PROT-ADMIN
```

In un browser Web:

- http://x.x.x.x è protetto
- http://hostname.example.com è protetto
- http://hostname non è protetto

Esempio:

```
Protect http://hostname.example.com  PROT-ADMIN
```

In un browser Web:

- http://x.x.x.x non è protetto
- http://hostname.example.com è protetto
- http://hostname non è protetto

È possibile specificare un indirizzo IP (ad esempio, `FOR 240.146.167.72`) o un nome host (ad esempio, `FOR hostA.bcd.com`).

I caratteri jolly non possono essere utilizzati per specificare indirizzi IP server.

Questo parametro è opzionale. Senza questo parametro, il server utilizza la direttiva per tutte le richieste a prescindere dall'indirizzo IP su cui è stata ricevuta la richiesta o dal nome host nell'URL.

Nota: il parametro [*indirizzo_IP_server* | *nome_host*] viene utilizzato con il parametro [*file_impostazione* | *etichetta*] o con il parametro *valore sottodirettiva*.

- Per utilizzare [*indirizzo_IP_server* | *nome_host*] con [*file_impostazione* | *etichetta*], è necessario inserire `FOR`, o altre stringhe di caratteri (senza spazi), tra il parametro [*file_impostazione* | *etichetta*] e i parametri [*indirizzo_IP_server* | *nome_host*].
- Per utilizzare [*indirizzo_IP_server* | *nome_host*] con i parametri *valore sottodirettiva*, *non* inserire `FOR` prima di *indirizzo_IP* o *nome_host*.

valore sottodirettiva

Per includere sottodirettive di protezione come parte della direttiva Protect, utilizzare questo parametro. Per le descrizioni delle sottodirettive di protezione, consultare quanto segue:

- "AuthType — Indica di specificare il tipo di autenticazione" a pagina 245
- "DeleteMask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a eliminare i file" a pagina 245

- "GetMask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a richiamare i file" a pagina 245
- "GroupFile — Indica di specificare la posizione del file gruppo associato" a pagina 245
- "Mask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a eseguire richieste HTTP" a pagina 246
- "PasswdFile — Indica di specificare la posizione del file di password associato" a pagina 246
- "PostMask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a inviare i file" a pagina 246
- "PutMask — Indica di specificare i nomi degli utenti, i gruppi e gli indirizzi autorizzati a inserire file" a pagina 246
- "ServerID — Indica di specificare un nome da associare al file di password" a pagina 247

Esempi

- Nell'esempio riportato di seguito, il server attiva la protezione come di seguito:
  - Le richieste che iniziano con `/secret/scoop/` attivano la protezione. L'impostazione di protezione viene definita nel file di impostazione della protezione /server/protect/setup1.acc. Dal momento che la direttiva Protect non specifica un'impostazione di protezione, viene utilizzata l'impostazione di protezione sulla direttiva DefProt già corrispondente.
  - Le richieste che iniziano con `/secret/business/` attivano la protezione. L'impostazione di protezione viene definita sulla direttiva Protection che presenta un'etichetta `BUS-PROT`.
  - Le richieste che iniziano con `/topsecret/` attivano la protezione. L'impostazione di protezione viene inclusa direttamente sulla direttiva Protect.

  Questi esempi utilizzano indirizzi IP. Se il server riceve richieste che iniziano con `/secret/` o `/topsecret/`, attiva un'impostazione di protezione differente per la richiesta, in base all'indirizzo IP della connessione di rete su cui è arrivata la richiesta.
  - Per le richieste `/secret/` in entrata su 0.67.106.79, il server attiva l'impostazione di protezione definita su una direttiva Protection con un'etichetta `CustomerA-PROT`. Per le richieste `/topsecret/ requests` in entrata su 0.67.106.79, il server attiva l'impostazione di protezione definita in linea sulla direttiva Protect per `/topsecret/`.
  - Per le richieste `/secret/` in entrata su 0.83.100.45, il server attiva l'impostazione di protezione definita su una direttiva Protection con un'etichetta `CustomerB-PROT`. Per le richieste `/topsecret/` in entrata su 0.83.100.45, il server attiva l'impostazione di protezione definita in linea sulla direttiva Protect per `/topsecret/`.

```
Protection BUS-PROT {
   UserID    busybody
   GroupID   webgroup
   AuthType Basic
   ServerID restricted
   PasswdFile  /docs/WWW/restrict.pwd
   GroupFile   /docs/WWW/restrict.grp
   GetMask authors
   PutMask authors
}
DefProt  /secret/*  /server/protect/setup1.acc
Protect  /secret/scoop/*
Protect  /secret/business/*   BUS-PROT
```

```
Protect  /topsecret/*  {
   AuthType Basic
   ServerID restricted
   PasswdFile /docs/WWW/restrict.pwd
   GroupFile  /docs/WWW/restrict.grp
   GetMask topbrass
   PutMask topbrass
}
Pass   /secret/scoop/*       /WWW/restricted/*
Pass   /secret/business/*    /WWW/confidential/*
Pass   /topsecret/*          /WWW/topsecret/*

Protect   /secret/*   CustomerA-PROT   FOR  0.67.106.79
Protect   /secret/*   CustomerB-PROT   FOR  0.83.100.45
Protect  /topsecret/*   0.67.106.79  {
   AuthType Basic
   ServerID restricted
   PasswdFile /docs/WWW/customer-A.pwd
   GroupFile  /docs/WWW/customer-A.grp
   GetMask A-brass
   PutMask A-brass
}
Protect  /topsecret/*   0.83.100.45   {
   AuthType Basic
   ServerID restricted
   PasswdFile /docs/WWW/customer-B.pwd
   GroupFile  /docs/WWW/customer-B.grp
   GetMask B-brass
   PutMask B-brass
}
```

- Negli esempi riportati di seguito, vengono utilizzati host virtuali. Se il server riceve richieste che iniziano con `/secret/` o `/topsecret/`, attiva una differente impostazione di protezione per la richiesta, in base al nome host nell'URL.
  - Per le richieste `/secret/` in entrata per hostA.bcd.com, il server attiva l'impostazione di protezione definita su una direttiva Protection con un'etichetta `CustomerA-PROT`. Per le richieste `/topsecret/` in entrata su hostA.bcd.com, il server attiva l'impostazione di protezione definita in linea sulla direttiva Protect per `/topsecret/`.
  - Per le richieste `/secret/` in entrata per hostB.bcd.com, il server attiva l'impostazione di protezione definita su una direttiva Protection con un'etichetta `CustomerB-PROT`. Per le richieste `/topsecret/` in entrata per hostB.bcd.com, il server attiva l'impostazione di protezione definita in linea sulla direttiva Protect per `/topsecret/`.
  - Per le richieste inviate tramite proxy, il server attiva l'impostazione di protezione definita su una direttiva Protection con un'etichetta `proxy-prot`. Ad esempio:

    ```
    Protect http://host1/* proxy-prot

    Protect   /secret/*   CustomerA-PROT   FOR  hostA.bcd.com
    Protect   /secret/*   CustomerB-PROT   FOR  hostB.bcd.com
    Protect  /topsecret/*   hostA.bcd.com  {
       AuthType Basic
       ServerID restricted
       PasswdFile /docs/WWW/customer-A.pwd
       GroupFile  /docs/WWW/customer-A.grp
       GetMask A-brass
       PutMask A-brass
    }
    Protect  /topsecret/*   hostB.bcd.com {
       AuthType Basic
       ServerID restricted
       PasswdFile /docs/WWW/customer-B.pwd
    ```

```
GroupFile  /docs/WWW/customer-B.grp
GetMask B-brass
PutMask B-brass
}
```

Impostazione predefinita

Per impostazione predefinita, la protezione per i moduli di configurazione e amministrazione viene fornita da una direttiva Protect con una maschera richiesta `/admin-bin/* .`

Protection — Indica di definire un'impostazione di protezione denominata nel file di configurazione

Utilizzare questa direttiva per definire un'impostazione di protezione nel file di configurazione. Assegnare un nome all'impostazione di protezione e definire il tipo di protezione utilizzando le sottodirettive di protezione.

Note:

1. Nel file di configurazione, inserire le direttive Protection davanti alle direttive DefProt o Protect che puntano a esse.
2. Per utilizzare i nomi dominio nelle regole di protezione, impostare la direttiva DNS-Lookup su `on`.

Formato

```
Protection nome_etichetta  {
    sottodirettiva  valore
    sottodirettiva  valore
    .
    .
    .
  }
```

nome_etichetta
: Specifica il nome da associare a questa impostazione di protezione. Il nome può essere utilizzato da direttive DefProt e Protect successive per puntare a questa impostazione di protezione.

valore sottodirettiva
: Le sottodirettive sono racchiuse tra parentesi ({ }). Il carattere parentesi sinistra deve essere l'ultimo carattere sulla stessa riga di *nome_etichetta*. Ciascuna sottodirettiva deve proseguire sulla propria riga. Il carattere parentesi destra deve trovarsi sulla propria riga, di seguito alla riga dell'ultima sottodirettiva. Tra le parentesi non sono consentite righe di commenti.

  Per le descrizioni delle sottodirettive di protezione, consultare "Sottodirettive di protezione — Indica di specificare in che modo proteggere una serie di risorse" a pagina 245.

Esempio

```
Protection NAME-ME   {
   AuthType Basic
   ServerID restricted
   PasswdFile  /WWW/password.pwd
   GroupFile   /WWW/group.grp
   GetMask groupname
   PutMask groupname
}
```

Impostazione predefinita

```
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
}
```

Sottodirettive di protezione — Indica di specificare in che modo proteggere una serie di risorse

Di seguito sono riportate le descrizioni delle sottodirettive di protezione che possono essere utilizzate in un'impostazione di protezione. Le sottodirettive sono in ordine alfabetico.

Le impostazioni di protezione possono trovarsi in file separati o essere incluse nel file di configurazione, come parte delle direttive DefProt, Protect o Protection.

AuthType — Indica di specificare il tipo di autenticazione

Utilizzare questa sottodirettiva di protezione quando si limita l'accesso in base a nomi utente e password. Specificare il tipo di autenticazione da utilizzare quando il client invia una password al server. Con l'autenticazione di base (`AuthType Basic`), le password vengono inviate al server sotto forma di testo normale. Le password sono codificate ma non crittografate.

Impostazione predefinita:

```
AuthType Basic
```

DeleteMask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a eliminare i file

Utilizzare questa sottodirettiva Protection per specificare nomi utente, gruppi e maschere indirizzi autorizzati a eseguire richieste DELETE su una directory protetta.

Esempio:

```
DeleteMask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*
```

GetMask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a richiamare i file

Utilizzare questa sottodirettiva Protection per specificare nomi utente, gruppi e maschere indirizzi autorizzati a eseguire richieste GET su una directory protetta.

Esempio:

```
GetMask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*
```

Impostazione predefinita:

```
GetMask  All@(*)
```

GroupFile — Indica di specificare la posizione del file gruppo associato

Utilizzare questa sottodirettiva Protection per specificare il percorso e il nome del file gruppo server utilizzato dall'impostazione di protezione. I gruppi definiti nel file gruppo server possono quindi essere utilizzati da:

- Qualsiasi sottodirettiva Mask appartenente all'impostazione di protezione. (Le sottodirettive Mask sono DeleteMask, GetMask, Mask, PostMask e PutMask.)
- Qualsiasi file ACL su una directory protetta dall'impostazione di protezione.

Esempio:

```
GroupFile /docs/etc/WWW/restrict.group
```

Mask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a eseguire richieste HTTP

Utilizzare questa sottodirettiva per specificare nomi utente, gruppi e maschere indirizzo autorizzati a eseguire richieste HTTP non contemplate da altre sottodirettive Mask.

Esempi:

```
Mask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*
```

Nota: quando si utilizza la direttiva Mask, è importante notare che Mask distingue tra caratteri maiuscoli e minuscoli. Di seguito è riportato un esempio di protezione Mask specificata su un ID utente:

```
MASK WEBADM,webadm
```

PasswdFile — Indica di specificare la posizione del file di password associato

Utilizzare questa sottodirettiva di protezione quando si limita l'accesso in base a nomi utente e password. Specificare il percorso e il nome del file di password che deve essere utilizzato da questa impostazione di protezione.

Dal momento che alcuni browser memorizzano nella cache gli ID utente e le password per domini di sicurezza (ServerID) in un host, seguire le istruzioni qui riportate mentre si specificano file di password e ServerID:

- Per le impostazioni di protezione che utilizzano lo stesso file di password, utilizzare il medesimo ServerID.
- Per impostazioni di protezione che utilizzano file di password differenti, utilizzare diversi ServerID.

Esempio:

```
PasswdFile /docs/etc/WWW/restrict.password
```

Nota: se il percorso o il nome del file di password contiene spazi incorporati, il percorso e il nome file devono essere racchiusi tra virgolette ("".)

```
PasswdFile "c:\test this\admin.pwd"
```

PostMask — Indica di specificare i nomi utente, i gruppi e gli indirizzi autorizzati a inviare i file

Per un server protetto, utilizzare questa sottodirettiva Protection per specificare utenti, gruppi e maschere indirizzo autorizzati a eseguire richieste POST su una directory protetta.

Esempio:

```
PostMask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*
```

PutMask — Indica di specificare i nomi degli utenti, i gruppi e gli indirizzi autorizzati a inserire file

Utilizzare questa sottodirettiva Protection per specificare utenti, gruppi e maschere indirizzi autorizzati a eseguire richieste PUT su una directory protetta.

Esempio:

```
PutMask authors,(niceguy,goodie)@45.96.3.1,128.0.*.*
```

ServerID — Indica di specificare un nome da associare al file di password

Utilizzare questa sottodirettiva di protezione quando si limita l'accesso in base a nomi utente e password. Specificare un nome da associare al file di password da utilizzare. Il nome non deve essere necessariamente quello di una macchina reale.

Il nome viene utilizzato come identificativo per il richiedente. Dal momento che impostazioni di protezione differenti possono utilizzare diversi file di password, se si associa un nome all'impostazione di protezione, il client potrà stabilire più facilmente quale password inviare. La maggior parte dei client visualizza questo nome quando viene richiesto un nome utente e una password.

Dal momento che alcuni browser memorizzano nella cache ID utente e password per dominio di sicurezza (ServerID) in un host, seguire le istruzioni qui riportate mentre si specificano file di password e ServerID:

- Per le impostazioni di protezione che utilizzano lo stesso file di password, utilizzare il medesimo ServerID.
- Per impostazioni di protezione che utilizzano file di password differenti, utilizzare diversi ServerID.

Esempio:

```
ServerID restricted
```

Proxy — Indica di specificare i protocolli proxy o il proxy inverso

Utilizzare questa direttiva per indicare i protocolli che Caching Proxy deve elaborare e per mappare una richiesta su un server. I protocolli validi sono `http`, `ftp` e `gopher`.

L'opzione del parametro UseSession per la direttiva Proxy aiuta a mantenere un canale permanente sul lato server, se le richieste dei client vengono inoltrate allo stesso server e dallo stesso canale TCP lato client. UseSession non tiene conto della direttiva ServerConnPool, il che consente alle richieste di differenti client di condividere una connessione permanente al server di back-end.

L'opzione del parametro JunctionPrefix per la direttiva Proxy viene utilizzata insieme al plugin di riscrittura giunzione. Per ulteriori informazioni, consultare "Abilitazione della riscrittura delle giunzioni (facoltativa)" a pagina 44 e "Definizione della giunzione con l'opzione JunctionPrefix (metodo consigliato)" a pagina 44.

Formato

```
Proxy maschera_richiesta percorso_server_destinazione [[ip]:porta]
      [UseSession] [JunctionPrefix:prefisso_url]
```

Questa direttiva trasferisce la richiesta a un server remoto. Ad esempio, la seguente direttiva consente di inoltrare tutte le richieste all'URL designato:

```
Proxy /*   http://proxy.server.name/*
```

Per un server proxy inverso protetto, utilizzare la seguente direttiva:

```
Proxy /*  https://proxy.server.name/*
```

Se si desidera ridurre le limitazioni sul server proxy, rimuovere il commento dalle seguenti direttive nel file di configurazione. (Tuttavia, queste direttive possono introdurre un problema di sicurezza quando il proxy è configurato come proxy inverso.)

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

Di seguito è riportato un esempio dell'opzione UseSession per la direttiva Proxy:

```
Proxy  /abc/*   http://server1/default/abc/*  :80  UseSession
```

Quando la richiesta client in entrata arriva dalla porta 80 e se l'URL sulla richiesta client corrisponde al modello /abc/*, l'URL viene mappato su http://server1/default/abc/* .

Di seguito è riportato il formato dell'opzione JunctionPrefix per la direttiva Proxy:

```
Proxy schema_url1 schema_url2 JunctionPrefix:prefisso_url
```

Per ulteriori informazioni sull'uso dell'opzione del parametro JunctionPrefix, consultare "Abilitazione della riscrittura delle giunzioni (facoltativa)" a pagina 44 e "Definizione della giunzione con l'opzione JunctionPrefix (metodo consigliato)" a pagina 44.

Impostazioni predefinite

Nessuna.

ProxyAccessLog — Indica di denominare il percorso al file di log accessi proxy

Utilizzare questa direttiva per specificare il percorso e il nome del file dove il server deve registrare le statistiche di accesso per le richieste proxy. Per impostazione predefinita, il server scrive una voce in questo log ogni volta che funge da proxy per una richiesta client. Se non si desidera registrare le richieste di determinati client, è possibile utilizzare la direttiva NoLog.

Il server avvia un nuovo file di log ogni giorno a mezzanotte, se in esecuzione. In caso contrario, questo si verifica appena il server viene avviato. Quando il file viene creato, il server utilizza il nome del file specificato, a cui appone un suffisso data o un'estensione. Il suffisso data o estensione è nel formato *Mmmddyyyy*, dove *Mmm* si riferisce alle prime tre lettere del mese, *dd* al giorno e *yyyy* all'anno.

È opportuno eliminare i file di log meno recenti in quanto occupano una significativa quantità di spazio sul disco rigido.

Formato

```
ProxyAccessLog percorso/file
```

Impostazioni predefinite

- **Sistemi Linux e UNIX:** `ProxyAccessLog /opt/ibm/edge/cp/server_root/logs/proxy`
- **Sistemi Windows:** `ProxyAccessLog unità:\Programmi\IBM\edge\cp\logs\proxy`

ProxyAdvisor — Indica di personalizzare il supporto per le richieste proxy

Utilizzare questa direttiva per specificare un'applicazione personalizzata che il server deve richiamare durante la fase Proxy Advisor. Questo codice supporta la richiesta.

Formato

`ProxyAdvisor /percorso/file:nome_funzione`

/percorso/file
Specifica il nome file completo del programma compilato.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

Esempio:

```
ProxyAdvisor /api/bin/customadvise.so:proxyadv
```

Impostazione predefinita

Nessuna

ProxyForwardLabels — Indica di specificare il filtro PICS

Utilizzare la direttiva ProxyForwardLabels per specificare il filtro PICS sul server proxy e sul client o su due proxy in una gerarchia.

Se ProxyForwardLabels è impostata su `on`, il server proxy genera intestazioni HTTP `PICS-Label:` per tutte le etichette PICS individuate, comprese etichette del server di origine, banche di etichette, cache etichette di Caching Proxy e plugin per la fornitura di etichette.

Se ProxyForwardLabels è impostata su `Off`, le intestazioni HTTP `PICS-Label:` non vengono generate.

Formato

`ProxyForwardLabels {on | off}`

Impostazione predefinita

`ProxyForwardLabels Off`

ProxyFrom — Indica di specificare un client con un'intestazione From:

Utilizzare questa direttiva per generare un'intestazione `From:`. Normalmente, questa viene utilizzata per fornire un indirizzo e-mail dell'amministratore proxy.

Formato

`ProxyFrom indirizzo_e-mail`

Esempio

L'impostazione `ProxyFrom webmaster@proxy.ibm.com` modifica l'intestazione nel modo seguente:

Intestazione originale	**Intestazione modificata**
`Indirizzo: http://www.ibm.com/`	`Indirizzo: http://www.ibm.com/`
`Ultima modifica: martedì 5 Nov 1997 10:05:39 GMT`	`Ultima modifica: martedì 5 Nov 1997 10:05:39 GMT`

Intestazione originale	Intestazione modificata
`Pragma: no-cache`	**`From: webmaster@proxy.ibm.com`** `Pragma: no-cache`

Impostazione predefinita
Nessuna

ProxyIgnoreNoCache — Indica di ignorare una richiesta di caricamento

Utilizzare questa direttiva per specificare la reazione del server quando gli utenti selezionano con il mouse il pulsante **Ricarica** sul browser. Se la direttiva ProxyIgnoreNoCache è impostata su `on`, durante i periodi di carico elevato, il server non richiede la pagina dal server di destinazione ma fornisce la copia del file memorizzata nella cache, se disponibile. In pratica, il server ignora l'intestazione `Pragma: no-cache` inviata dal browser.

Formato
```
ProxyIgnoreNoCache  {on | off}
```

Impostazione predefinita
```
ProxyIgnoreNoCache off
```

ProxyPersistence — Indica di autorizzare connessioni permanenti

Utilizzare questa direttiva per specificare se mantenere una connessione permanente con il client. Una connessione permanente riduce il tempo di attesa degli utenti e il carico CPU sul server proxy ma richiede un numero superiore di risorse. Una connessione permanente richiede più thread, quindi più memoria sul server proxy.

Le connessioni permanenti non devono essere utilizzate su un'impostazione server proxy a struttura, se uno dei proxy non è conforme a HTTP 1.1.

Formato
```
ProxyPersistence {on | off}
```

Impostazione predefinita
```
ProxyPersistence on
```

ProxySendClientAddress — Indica di generare un'intestazione IP Address: del client

Utilizzare questa direttiva per specificare se il proxy inoltra l'indirizzo IP del client al server di destinazione.

Formato
```
ProxySendClientAddress  {IP_client: | OFF}
```

Esempio
La direttiva `ProxySendClientAddress` *`IP-client`*`:` modifica l'intestazione nel modo seguente:

Intestazione originale	Intestazione modificata
`Indirizzo: http://www.ibm.com/`	`Indirizzo: http://www.ibm.com`

Intestazione originale
```
Ultima modifica: martedì 5 Nov 1997
10:05:39 GMT
Pragma: no-cache
```

Intestazione modificata
```
Ultima modifica: martedì 5 Nov 1997
10:05:39 GMT
Client-IP: 0.67.199.5
Pragma: no-cache
```

Impostazione predefinita
Nessuna

ProxyUserAgent — Indica di modificare la stringa agente utente

Utilizzare questa direttiva per specificare una stringa `Agente utente` che sostituisca la stringa inviata dal client. In questo modo, è possibile mantenere l'anonimato mentre si visitano i siti Web. Tuttavia, alcuni siti presentano delle pagine personalizzate basate sulla stringa `Agente utente`. L'uso della direttiva ProxyUserAgent impedisce di visualizzare alcune pagine personalizzate.

Formato
```
ProxyUserAgent nome_prodotto/versione
```

Esempio
La direttiva `ProxyUserAgent Caching Proxy/6.0` modifica l'intestazione nel modo seguente:

Intestazione originale
```
Indirizzo: http://www.ibm.com/
Ultima modifica: martedì 5 Nov 1997
10:05:39 GMT
Agente utente: Mozilla/ 2.02 OS2
Pragma: no-cache
```

Intestazione modificata
```
Indirizzo: http://www.ibm.com
Ultima modifica: martedì 5 Nov 1997
10:05:39 GMT
Agente utente: Caching Proxy/6.0
Pragma: no-cache
```

Impostazione predefinita
Nessuna

ProxyVia — Indica di specificare il formato dell'intestazione HTTP

Utilizzare questa direttiva per controllare il formato dell'intestazione HTTP. Per questa direttiva, sono possibili quattro valori. Se ProxyVia è impostata su `Full`, Caching Proxy aggiunge un'intestazione Via nella richiesta o nella risposta; se un'intestazione Via si trova già nel flusso, Caching Proxy aggiunge le informazioni host alla fine. Se impostata su `Set`, Caching Proxy imposta l'intestazione Via sulle informazioni host; se un'intestazione Via già si trova nel flusso, Caching Proxy la elimina. Se impostata su `Pass`, Caching Proxy inoltra le informazioni dell'intestazione così come sono. Se impostata su `Block`, Caching Proxy non inoltra intestazioni Via.

Formato
```
ProxyVia {Full | Set | Pass | Block}
```

Esempio
```
ProxyVia Pass
```

Impostazione predefinita

```
ProxyVia Full
```

ProxyWAS — Indica di specificare di inviare le richieste a WebSphere Application Server

La direttiva di mappatura ProxyWAS funziona come la direttiva Proxy con la sola differenza che indica a Caching Proxy di dirigere le richieste corrispondenti a WebSphere Application Server. Per gli esempi su questa direttiva, consultare "Proxy — Indica di specificare i protocolli proxy o il proxy inverso" a pagina 247.

Formato

```
ProxyWAS maschera_richiesta percorso_server_destinazione [UseSession]
        [JunctionPrefix:prefisso_url]
```

Impostazione predefinita

Nessuna

PureProxy — Indica di disattivare un proxy dedicato

Utilizzare questa direttiva per specificare se il server funge da server proxy o da proxy e server di contenuti. Si consiglia di utilizzare Caching Proxy solo come proxy.

Formato

```
PureProxy {on | off}
```

Impostazione predefinita

```
PureProxy on
```

PurgeAge — Indica di specificare la durata di un log

Utilizzare questa direttiva per specificare la durata di un log, espressa in giorni, prima che il log venga eliminato. Se PurgeAge è impostata su `0`, il log non viene eliminato.

Nota: il plugin non elimina il log del giorno corrente o precedente.

Formato

```
PurgeAge numero
```

Impostazione predefinita

```
PurgeAge 7
```

Direttive correlate

- "CompressAge — Indica di specificare quando comprimere i log" a pagina 190
- "CompressDeleteAge — Indica di specificare quando eliminare i log" a pagina 192
- "CompressCommand — Indica di specificare il comando di compressione e i parametri" a pagina 191
- "Midnight — Indica di specificare il plugin dell'API utilizzato per archiviare i log" a pagina 229
- "LogArchive — Indica di specificare il funzionamento dell'archiviazione log" a pagina 223
- "PurgeSize — Indica di specificare il limite della dimensione dell'archivio log" a pagina 253

PurgeSize — Indica di specificare il limite della dimensione dell'archivio log

Utilizzare questa direttiva per specificare la dimensione, in megabyte, che i file di log possono raggiungere prima che l'archivio log venga svuotato. Se la direttiva PurgeSize è impostata su `0`, non esiste alcun limite relativo alla dimensione, quindi i file non verranno eliminati.

L'impostazione di PurgeSize si riferisce a *tutti* i log di un determinato tipo. Ad esempio, se si stanno registrando errori (ossia, se una voce ErrorLog è stata creata nel file di configurazione) e PurgeSize è pari a 10 MB, Caching Proxy calcola le dimensioni di tutti i log errori, le somma ed elimina i log finché la dimensione totale non rientra al di sotto dei 10 MB.

Nota: il plugin non elimina il log del giorno corrente o precedente. Quando i file di log vengono eliminati, quelli meno recenti vengono rimossi per primi, finché la dimensione di ciascun file di log di un determinato tipo non torna a essere minore o uguale al valore definito da PurgeSize (in megabyte).

Formato

```
PurgeSize numero_di_MB
```

Impostazione predefinita

```
PurgeSize 0
```

Direttive correlate

- "CompressAge — Indica di specificare quando comprimere i log" a pagina 190
- "CompressDeleteAge — Indica di specificare quando eliminare i log" a pagina 192
- "CompressCommand — Indica di specificare il comando di compressione e i parametri" a pagina 191
- "LogArchive — Indica di specificare il funzionamento dell'archiviazione log" a pagina 223
- "Midnight — Indica di specificare il plugin dell'API utilizzato per archiviare i log" a pagina 229
- "PurgeAge — Indica di specificare la durata di un log" a pagina 252

RCAConfigFile — Indica di specificare un alias per ConfigFile

Utilizzare questa direttiva per specificare il nome e il percorso del file di configurazione RCA (Remote Cache Access).

Nota: il file di configurazione RCA è stato unito al file ibmproxy.conf. Per questioni di compatibilità con le versioni precedenti, RCAConfigFile è supportato come alias di ConfigFile.

Formato

```
RCAConfigFile /etc/nome_file
```

Esempio

```
RCAConfigFile /etc/user2rca.conf
```

Impostazione predefinita

```
RCAConfigFile /etc/rca.conf
```

RCAThreads — Indica di specificare il numero di thread per porta

Utilizzare questa direttiva per specificare il numero di thread attivi su una porta RCA.

Formato

```
RCAThreads numero_di_thread
```

Esempio

```
RCAThreads 50
```

Impostazione predefinita

```
MaxActiveThreads x [(ArraySize -1) / (2 x ArraySize -1)]
```

ReadTimeout — Indica di specificare il limite di tempo di una connessione

Utilizzare questa direttiva per specificare il limite di tempo consentito senza attività di rete prima che una connessione venga annullata.

Formato

```
ReadTimeout tempo
```

Impostazione predefinita

```
ReadTimeout 5 minutes
```

Redirect — Indica di specificare una maschera per le richieste inviate a un altro server

Utilizzare questa direttiva per specificare una maschera per le richieste che si intende accettare e inviare a un altro server. Se una richiesta corrisponde a una maschera su una direttiva Redirect, la richiesta non viene confrontata con le maschere su altre direttive nel file di configurazione.

Formato

```
Redirect maschera_richiesta URL  [indirizzo_IP_server | nome_host]
```

maschera_richiesta
: Specifica una maschera per le richieste che il server deve inviare a un altro server.

  Nella maschera, è possibile utilizzare un asterisco (*) come carattere jolly. Il carattere tilde (~), subito dopo una barra (/), deve essere confrontato in modo esplicito; infatti per questa operazione non è possibile utilizzare un carattere jolly.

URL
: Specifica la richiesta URL che il server invia a un altro server. La risposta a questa richiesta viene indirizzata al richiedente originale, senza indicare che non proviene dal proprio server.

  L'*URL* deve contenere la specifica di un protocollo e il nome del server a cui viene inviata la richiesta. Può inoltre contenere un percorso o nome file. Se *maschera_richiesta* adopera un carattere jolly, anche il percorso o il nome file sull'*URL* può utilizzare un carattere jolly. La parte della richiesta originale che corrisponde al carattere jolly su *maschera_richiesta* viene inserita al posto del carattere jolly sull'*URL*.

[*indirizzo_IP_server* | *nome_host*]

Se si utilizzano più indirizzi IP o host virtuali, utilizzare questo parametro per specificare un indirizzo IP o un nome host. Il server utilizza la direttiva esclusivamente per le richieste inviate al server su questo indirizzo IP o per questo host. Per un indirizzo IP, si tratta dell'indirizzo della connessione di rete del server e non dell'indirizzo del client richiedente.

È possibile specificare un indirizzo IP (ad esempio, `240.146.167.72`) o un nome host (ad esempio, `hostA.bcd.com`).

Questo parametro è opzionale. Senza questo parametro, il server utilizza la direttiva per tutte le richieste a prescindere dall'indirizzo IP su cui è stata ricevuta la richiesta o dal nome host nell'URL.

Per un indirizzo IP del server non è possibile specificare un carattere jolly.

Esempi

- Nell'esempio riportato di seguito, il server invia le richieste che iniziano con `/chief/stuff/` alla directory wahoo del www.other.org server.

```
Redirect  /chief/stuff/*   http://www.other.org/wahoo/*
```

- Nell'esempio riportato di seguito viene utilizzato il parametro dell'indirizzo IP opzionale. Se il server riceve richieste che iniziano con `/stuff/`, reindirizza la richiesta a server differenti, in base all'indirizzo IP della connessione di rete su cui è arrivata la richiesta. Per le richieste in entrata su 240.146.167.72, il server invia la richiesta alla directory wahoo del server www.chief.org. Per le richieste in entrata su una connessione con un indirizzo 0.83.100.45, il server invia la richiesta alla directory pound del server 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
```

- Nell'esempio riportato di seguito viene utilizzato il parametro dell'indirizzo IP opzionale. Se il server riceve richieste che iniziano con `/stuff/`, reindirizza la richiesta a server differenti, in base al nome host nell'URL. Per le richieste in entrata per hostA, il server invia la richiesta alla directory wahoo del server www.chief.org. Per le richieste in entrata per hostB, il server invia la richiesta alla directory pound del server www.dawg.com.

```
Redirect  /stuff/*   http://www.chief.org/wahoo/*   hostA.bcd.com
Redirect  /stuff/*   http://www.dawg.com/pound/*    hostB.bcd.com
```

Impostazione predefinita

Nessuna

RegisterCacheIdTransformer — Indica di memorizzare più di una variante di una risorsa, in base all'intestazione Cookie

Utilizzare questa direttiva per consentire a Caching Proxy di memorizzare nella cache più di una variante di una risorsa (URI) in base all'intestazione Cookie.

Nota: se i cookie sono disabilitati sui browser client, i client possono accedere agli stessi oggetti memorizzati nella cache.

Per ulteriori informazioni, vedere "SupportVaryHeader — Indica di memorizzare nella cache più di una variante di una risorsa, in base all'intestazione HTTP Vary" a pagina 268.

Formato

```
RegisterCacheIdTransformer Cookie nome-cookie
```

Il *nome-cookie* è il nome nell'intestazione Cookie nella richiesta del client.

Esempio

```
RegisterCacheIdTransformer Cookie Usergroup
```

Per un esempio sull'uso di questa direttiva insieme a SupportVaryHeader, consultare "SupportVaryHeader — Indica di memorizzare nella cache più di una variante di una risorsa, in base all'intestazione HTTP Vary" a pagina 268.

Impostazione predefinita

Nessuna

ReversePass — Indica di intercettare automaticamente le richieste reindirizzate

La direttiva di mappatura ReversePass esamina il flusso di risposte del server per individuare le richieste riscritte come risultato del reindirizzamento automatico. Normalmente, quando un server restituisce un codice HTTP nella classe 3*xx* (ad esempio, 301, Spostato in modo permanente, o 303, Visualizza altro), il server invia un messaggio con una risposta che indica al client richiedente di indirizzare le future richieste all'URL e all'indirizzo IP corretti. Nel caso di impostazione di un proxy inverso, un messaggio di reindirizzamento dal server di origine può far sì che i browser client ignorino il server proxy per le richieste successive. Per evitare che i client contattino direttamente il server di origine, utilizzare la direttiva ReversePass per intercettare le richieste eseguite in modo specifico al server di origine.

A differenza di altre direttive di mappatura, che elaborano il flusso di richieste, ReversePass confronta la relativa maschera con il flusso di risposte. Il flusso di risposte è la risposta che il server proxy ottiene dal server di origine e invia al client.

Formato

```
ReversePass URL_riscritto URL_proxy [host:porta]
```

L'opzione *host*:*porta* consente al proxy di applicare una regola ReversePass differente, in base al nome host e alla porta del server di backend.

Esempi

- La seguente istruzione di esempio impedisce di inviare richieste dirette al server di origine:

  ```
  ReversePass  http://backend.company.com:9080/*  http://edge.company.com/*
  ```

  La porta 9080 è la porta predefinita di Application Service at the Edge. Questo tipo di richiesta può essere generato se il server delle applicazioni di origine restituisce un codice 3*xx* al client.
- La seguente istruzione di esempio memorizza nella cache le richieste reindirizzate da un codice 301 dell'applicazione Edge: server.

  ```
  ReversePass
  http://edge.company.com:9080/*  http://edge.company.com/*
  ```

Nota: il contenuto del modello *URL_proxy*, fino al carattere jolly (*), deve corrispondere esattamente al contenuto che il server di back-end invia nell'intestazione dell'indirizzo altrimenti la direttiva non riesce.

Impostazione predefinita
Nessuna

RewriteSetCookieDomain — Indica di specificare un modello del dominio da riscrivere

Utilizzare questa direttiva per specificare il modello del dominio da riscrivere. La direttiva trasforma il dominio da *modello1_dominio* a *modello2_dominio*.

Formato
```
RewriteSetCookieDomain modello1_dominio modello2_dominio
```

Esempio
```
RewriteSetCookieDomain .internal.com .external.com
```

Impostazione predefinita
Nessuna

Direttive correlate
- "JunctionRewriteSetCookiePath — Indica di riscrivere l'opzione di percorso nell'intestazione Set-Cookie, quando si utilizza il plugin JunctionRewrite" a pagina 218

RTSPEnable — Indica di abilitare il reindirizzamento RTSP

La direttiva abilita o disabilita il reindirizzamento RTSP. Le opzioni sono `on` o `off`.

Formato
```
RTSPEnable {on | off}
```

Esempio
```
RTSPEnable  on
```

Impostazione predefinita
Nessuna

rtsp_proxy_server - Indica di specificare i server per il reindirizzamento

Questa direttiva viene utilizzata per specificare i server proxy RTSP che ricevono le richieste reindirizzate. Per differenti tipi di flussi è possibile specificare server diversi. Il formato di questa direttiva è il seguente:

```
rtsp_proxy_server indirizzo dns server[:porta] serie predefinita [elenco di tipi mime]
```

Esempio
```
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
```

Impostazione predefinita
Nessuna

rtsp_proxy_threshold — Indica di specificare il numero di richieste prima di reindirizzarle alla cache

Questa direttiva specifica il numero di richieste ricevute prima che una richiesta RTSP venga reindirizzata a un server proxy anziché a un server di origine. I proxy RealNetworks memorizzano nella cache i flussi sulla prima richiesta e, inizialmente, si riscontra un raddoppio della larghezza di banda per la ricezione del flusso. Specificando una soglia superiore a uno, le richieste eseguite una sola volta non verranno memorizzate nella cache. Il formato di questa direttiva è il seguente:

```
rtsp_proxy_threshold numero_di_occorrenze
```

Esempio

```
rtsp_proxy_threshold 5
```

Impostazione predefinita

Nessuna

rtsp_url_list_size — Indica di specificare il numero di URL nella memoria proxy

Questa direttiva specifica il numero di URL univoci conservati in memoria per il reindirizzamento. Il proxy fa riferimento a questo elenco per determinare se è già stato riscontrato uno specifico URL. Un elenco di dimensioni superiori aumenta la capacità del server proxy di inviare una richiesta successiva allo stesso server proxy che ha ricevuto la richiesta precedente, ma ciascuna voce in elenco utilizza circa 16 byte di memoria.

Formato

```
rtsp_url_list_size dimensione_elenco
```

Esempio

```
rtsp_url_list_size 8192
```

Impostazione predefinita

Nessuna

ScriptTimeout – Indica di specificare l'impostazione di timeout per gli script

Utilizzare questa direttiva per impostare il tempo concesso per chiudere un programma CGI avviato dal server. Scaduto il tempo, il server chiude il programma. Su piattaforme Linux e UNIX, questo avviene con il segnale KILL.

Specificare un valore tempo utilizzando una qualsiasi combinazione di ore, minuti (o min) e secondi (o sec).

Formato

```
ScriptTimeout timeout
```

Impostazione predefinita

```
ScriptTimeout 5 minutes
```

SendHTTP10Outbound — Indica di specificare la versione del protocollo per le richieste inviate tramite proxy

Utilizzare questa direttiva per specificare che le richieste inviate da Caching Proxy a un server downstream devono utilizzare il protocollo HTTP versione 1.0. (Un server *downstream* è un altro server proxy in una catena di proxy o un server di origine che elabora la richiesta.)

Se viene utilizzata questa direttiva, Caching Proxy identifica HTTP 1.0 come protocollo nella riga richieste. Al server downstream vengono inviate esclusivamente la funzionalità specifica di HTTP 1.0 e determinate funzioni di HTTP 1.1, come le intestazioni Cache-Control, supportate dalla maggior parte dei server HTTP 1.0. Utilizzare questa direttiva se si dispone di un server downstream che non gestisce correttamente le richieste HTTP 1.1.

Se la direttiva SendHTTP10Outbound *non* viene specificata, Caching Proxy identifica HTTP 1.1 come il protocollo della riga richieste. Nella richiesta, è possibile utilizzare anche la funzionalità HTTP 1.1, come le connessioni permanenti.

Formato

`SendHTTP10Outbound` *`modello_url`*

Esempi

Questa direttiva può essere specificata più di una volta, ad esempio:

```
SendHTTP10Outbound http://www.hosta.com/*
SendHTTP10Outbound http://www.hostb.com/*
```

Per motivi di compatibilità con le versioni precedenti, la suddetta sintassi di SendHTTP10Outbound viene gestita come segue:

- `SendHTTP10Outbound on` viene considerata come se si fosse specificato `SendHTTP10Outbound * .`
- `SendHTTP10Outbound off` viene ignorata.

Nota: se viene specificato sia `SendHTTP10Outbound off` che `SendHTTP10Outbound` *`modello_url`*, `SendHTTP10Outbound off` viene ignorata ma compare un messaggio di avvertenza.

Impostazione predefinita

Nessuna

SendRevProxyName — Indica di specificare il nome host di Caching Proxy nell'intestazione HOST

Se funge da proxy inverso, Caching Proxy riceve le richieste HTTP da un client e le invia al server di origine. Per impostazione predefinita, Caching Proxy scrive il nome host del server di origine nell'intestazione HOST della richiesta che invia al server di origine. Al contrario, se la direttiva SendRevProxyName è impostata su yes, Caching Proxy scrive il proprio nome host nell'intestazione HOST. Questa direttiva può essere utilizzata per attivare una configurazione speciale per i server di back-end, in cui la richiesta inviata al server di origine sembra sempre provenire dal server proxy, anche nel caso in cui la richiesta viene reindirizzata da un server di back-end all'altro.

Questa direttiva si distingue dalla direttiva di mappatura ReversePass nel modo seguente: la direttiva ReversePass intercetta le richieste con una determinata

sintassi e ne sostituisce il contenuto con quello specificato. La direttiva SendRevProxyName può essere impostata solo per sostituire il nome host Caching Proxy al nome host del server di origine. Non è utile per configurare Application Service at the Edge.

Formato

```
SendRevProxyName  {yes | no}
```

ServerConnGCRun — Indica di specificare l'intervallo in cui eseguire il thread di raccolta di dati inutili

Questa direttiva imposta l'intervallo in cui il thread di raccolta di dati inutili controlla le connessioni server in timeout (impostata con la direttiva ServerConnTimeout). Utilizzare questa direttiva solo se la direttiva ServerConnPool è impostata su on.

Formato

```
ServerConnGCRun intervallo_tempo
```

Esempio

```
ServerConnGCRun 2 minutes
```

Impostazione predefinita

```
ServerConnGCRun 2 minutes
```

ServerConnPool — Indica di specificare il lotto connessioni ai server di origine

Questa direttiva consente al proxy di raggruppare le proprie connessioni in uscita ai server di origine. Se impostata su on è possibile migliorare le prestazioni e sfruttare al massimo i server di origine che autorizzano alle connessioni permanenti. Con la direttiva ServerConnTimeout, è inoltre possibile specificare per quanto tempo una connessione può rimanere inutilizzata.

Nota: questa direttiva può essere sfruttata al meglio in un ambiente controllato; infatti, può diminuire le prestazioni nel caso di un proxy di inoltro o di server di origine non conformi a HTTP 1.1.

Formato

```
ServerConnPool {on | off}
```

Impostazione predefinita

```
ServerConnPool off
```

ServerConnTimeout — Indica di specificare il tempo di inattività massimo

Utilizzare questa direttiva per limitare il tempo concesso senza attività di rete prima che la connessione venga annullata. Utilizzare questa direttiva solo se la direttiva ServerConnPool è impostata su on.

Formato

```
ServerConnTimeout spec-tempo
```

Esempio

```
ServerConnTimeout 30 seconds
```

Impostazione predefinita

```
ServerConnTimeout 10 seconds
```

ServerInit — Indica di personalizzare la fase Inizializzazione del server

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata richiamata dal server durante le routine di inizializzazione. Questo codice viene eseguito prima della lettura di qualsiasi richiesta client e ogni volta che il server viene riavviato.

Se si utilizzano i moduli GoServe nelle fasi PreExit o Service, è necessario chiamare qui il modulo `gosclone`.

Formato

```
ServerInit /percorso/file:nome_funzione
[stringa_inizializzazione]
```

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

stringa_inizializzazione
Opzionale; specifica una stringa di testo da trasferire alla funzione applicativa.

Esempio

```
ServerInit   /ics/api/bin/icsext05.so:svr_init
```

Impostazione predefinita

Nessuna

ServerRoot — Indica di specificare la directory dove è installato il programma server

Utilizzare questa direttiva per specificare la directory dove è installato il programma server (l'attuale directory di lavoro del server). Le direttive di registrazione utilizzano questa directory di lavoro come root predefinita quando si utilizzano nomi percorso relativi.

Su sistemi Windows, la directory viene identificata durante l'installazione.

Formato

```
ServerRoot  percorso_directory
```

Impostazioni predefinite

- **Sistemi Linux e UNIX:** `ServerRoot /opt/ibm/edge/cp/server_root/`
- **Sistemi Windows:** `C:\Programmi\IBM\edge\cp\bin\`

Nota: è possibile modificare l'impostazione predefinita ma ciò non influisce sulla modalità di elaborazione delle richieste da parte del server.

Nota: le regole PASS e EXEC possono essere indipendenti da questa directory.

ServerTerm — Indica di personalizzare la fase Chiusura del server

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata richiamata dal server durante la fase Chiusura del server. Questo codice viene eseguito quando si verifica una chiusura regolare e ogni volta che il server viene riavviato. In questo modo, è possibile rendere disponibili le risorse assegnate da una funzione applicativa PreExit.

Formato

```
ServerTerm  /percorso/file:nome_funzione
```

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

Esempio

```
ServerTerm  /ics/api/bin/icsext05.so:shut_down
```

Impostazione predefinita

Nessuna

Service — Indica di personalizzare la fase Servizio

Utilizzare questa direttiva per specificare una funzione applicativa personalizzate richiamata dal server durante la fase Servizio. Questo codice supporta le richieste client. Ad esempio, consente di inviare il file o di eseguire il programma CGI.

Non sono disponibili impostazioni predefinite per questa direttiva. Se la richiesta corrisponde a una regola relativa al servizio (ossia, se viene eseguita una funzione applicativa specificata su una direttiva Service) ma la funzione restituisce HTTP_NOACTION, il server genera un errore e la richiesta non riesce.

Formato

```
Service maschera_richiesta/percorso/file:nome_funzione
[indirizzo_IP_server | nome_host]
```

maschera_richiesta
Specifica una maschera per richieste che determina ulteriormente se la funzione applicativa viene chiamata. La specifica include il protocollo, il dominio e l'host; può essere preceduta da un carattere barra (/) ed è possibile utilizzare l'asterisco (*) come carattere jolly. Ad esempio, `/front_page.html`, `http://www.ics.raleigh.ibm.com`, `/pub*`, `/*` e `*` sono tutti validi.

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome della funzione applicativa all'interno del programma.

[*indirizzo_IP_server* | *nome_host***]**
Se si utilizzano più indirizzi IP o host virtuali, questo parametro determina se la funzione applicativa viene richiamata solo per le richieste inviate a uno specifico indirizzo IP o per un determinato host.

Per un indirizzo IP del server non è possibile specificare un carattere jolly.

Esempi

```
Service  /index.html /ics/api/bin/icsext05.so:serve_req
Service  /cgi-bin/hexcalc* /ics/api/calculator:HEXcalc*
```

Nota: se si desidera eseguire la conversione del percorso completo, compresa la *stringa_query*, è necessario specificare un asterisco (*) sia in *maschera_richiesta* che in *percorso*/*file:nome_funzione*, come illustrato nel secondo esempio.

Impostazione predefinita

Nessuna

SignificantURLTerminator — Indica di specificare un codice di interruzione per le richieste URL

Utilizzare questa direttiva per specificare un codice di interruzione per le richieste URL. Se si utilizza un codice di interruzione in una richiesta, Caching Proxy valuta solo i caratteri che precedono questo codice quando elabora la richiesta e stabilisce se il risultato è già memorizzato nella cache. Quando viene definito più di un codice di interruzione, Caching Proxy confronta gli URL in entrata con i codici di interruzione nell'ordine in cui questi si trovano nel file ibmproxy.conf.

Formato

```
SignificantURLTerminator stringa_fine
```

Esempio

```
SignificantURLTerminator  &.
```

In questo esempio, le due richieste che seguono sono considerate identiche.

```
http://www.exampleURL.com/tx.asp?id=0200&.;x=004;y=001
http://www.exampleURL.com/tx.asp?id=0200&.;x=127;y=034
```

Impostazione predefinita

Nessuna

SMTPServer (solo Windows)— Indica di impostare un server SMTP per la routine Sendmail

Utilizzare questa direttiva per impostare il server SMTP utilizzato dalla routine sendmail interna in Caching Proxy per Windows. Per questa routine, è necessario impostare anche le due direttive riportate di seguito: "WebMasterEMail — Indica di impostare un indirizzo e-mail per ricevere report di server selezionati" a pagina 273 e "WebMasterSocksServer (solo Windows)— Indica di impostare un server Socks per la routine sendmail" a pagina 273.

Formato

```
SMTPServer nome host o indirizzo IP del server SMTP
```

Esempio

```
SMTPServer mybox.com
```

Impostazione predefinita

```
Nessuna
```

SNMP — Indica di abilitare o disabilitare il supporto SNMP

Utilizzare questa direttiva per abilitare o disabilitare il supporto SNMP.

Formato

```
SNMP   {on | off}
```

Impostazione predefinita

```
SNMP off
```

SNMPCommunity — Indica di fornire una password di sicurezza per SNMP

Utilizzare questa direttiva per definire la password tra l'agente secondario DPI (Distributed Protocol Interface) del server Web e l'agente SNMP. Il nome della comunità SNMP autorizza un utente a visualizzare le variabili relative alle prestazioni monitorate da SNMP per una comunità di server prescelta. L'amministratore di sistema definisce le variabili da cui i server possono essere visualizzati quando viene specificata una password. Se si modifica il nome della comunità SNMP, assicurarsi di aver modificato anche il nome della comunità specificato nel file /etc/snmpd.conf.

Formato

```
SNMPCommunity nome
```

Impostazione predefinita

```
SNMPCommunity public
```

SSLCaching — Indica di abilitare la memorizzazione nella cache di una richiesta protetta

Utilizzare questa direttiva per memorizzare nella cache il contenuto su una richiesta protetta quando si utilizza un proxy inverso. Questa direttiva configura la memorizzazione nella cache di tutte le connessioni al server proxy, sia le connessioni client che quelle con un server di contenuti di back-end.

Nota: le direttive SSL non sono supportate su SUSE Linux.

Formato

```
SSLCaching {on | off}
```

Impostazione predefinita

```
SSLCaching off
```

SSLCertificate — Indica di specificare le etichette chiave per i certificati

Utilizzare questa direttiva per specificare le etichette chiave che consentono al proxy di determinare quale certificato inviare al client, quando Caching Proxy funge da unico proxy inverso per più domini che offrono i propri certificati SSL, e di indicare al server proxy se richiamare o meno un certificato PKI lato client per l'autenticazione client.

Formato

```
SSLCertificate serverIP/hostname CertificateLabel
     [NoClientAuth | ClientAuthRequired]
```

serverIP/hostname
: È possibile specificare un indirizzo IP (ad esempio, 204.146.167.72) o un nome host (ad esempio, hostA.raleigh.ibm.com) per il server a cui è indirizzata la richiesta SSL.

CertificateLabel
Il nome del certificato che deve essere utilizzato se l'autenticazione client è necessaria per le richieste SSL destinate all'indirizzo IP o al nome host designato.

[NoClientAuth | ClientAuthRequired]
Le istruzioni per il server proxy che indicano se richiamare o meno un certificato PKI lato client.

Esempi

```
SSLCertificate  www.abc.com      ABCCert
SSLCertificate  204.146.167.72   intABCCert
SSLCertificate  www.xyz.com      XYZCert
SSLCertificate  www.xyz.com      XYZCert      ClientAuthRequired
```

Impostazione predefinita

Nessuna

SSLCryptoCard — Indica di specificare la scheda crittografica installata

Utilizzare questa direttiva per indicare al server proxy la presenza di una scheda crittografica installata e per specificarla.

Formato

```
SSLCryptoCard {rainbowcs | ciphernfast} {on | off}
```

Esempio

```
SSLCryptoCard rainbowcs on
```

Impostazione predefinita

Nessuna

SSLEnable — Indica di specificare l'ascolto sulla porta 443 per la ricezione di richieste protette

Utilizzare questa direttiva per specificare che Caching Proxy è in ascolto sulla porta 443 per ricevere richieste protette.

Nota: le direttive SSL non sono supportate su SUSE Linux.

Formato

```
SSLEnable {on | off}
```

Impostazione predefinita

```
SSLEnable off
```

SSLForwardPort — Indica di specificare la porta destinata agli aggiornamenti SSL HTTP

Utilizzare questa direttiva per specificare la porta destinata alle richieste HTTP trasformate in richieste HTTPS da Caching Proxy mediante l'implementazione di SSL. Specificare una porta diversa dalla porta principale HTTP 80 o SSL 443.

Formato

```
SSLForwardPort numero porta
```

Esempio
```
SSLForwardPort 8888
```

Impostazione predefinita
Nessuna

SSLOnly — Indica di disabilitare i thread per le richieste HTTP

Utilizzare questa direttiva per disabilitare i thread listener per le richieste HTTP standard (normalmente le porte 80 e 8080) quando SSL (normalmente la porta 443) è abilitato.

Formato
```
SSLOnly    {on | off}
```

Impostazione predefinita
```
SSLOnly   off
```

SSLPort — Indica di specificare una porta di ascolto HTTPS diversa da quella predefinita

Utilizzare questa direttiva per specificare la porta di ascolto HTTPS diversa dalla porta HTTPS 443 predefinita di ibmproxy.

Nota: ibmproxy supporta una porta HTTPS per ciascuna istanza, quindi è preferibile NON utilizzare questa direttiva per specificare più porte HTTPS. Per supportare porte HTTPS multiple, avviare più istanze ibmproxy con file `ibmproxy.conf` differenti.

Formato
`SSLPort` *`valore porta`*

Dove *valore porta* è un numero intero maggiore di 0. Inoltre, *valore porta* deve essere consentito dal sistema operativo e non deve essere utilizzato da altre applicazioni.

Esempio
```
SSLPort 8443
```

Impostazione predefinita
443

SSLTunneling — Indica di abilitare l'operazione di tunnel SSL

Utilizzare questa direttiva per consentire l'operazione di tunnel SSL su qualsiasi porta sull'host di destinazione. Impostando questa direttiva su on, è possibile eseguire l'operazione di tunnel SSL su qualsiasi porta sul server di destinazione. Se si imposta su off, l'operazione di tunnel SSL è consentita esclusivamente su determinate porte specificate nelle regole Proxy. Se non sono disponibili regole Proxy per operazioni di tunnel SSL, e la direttiva SSLTunneling è impostata su `off`, allora tale operazione non è consentita. Se la direttiva SSLTunneling è impostata su `on`, è necessario abilitare anche il metodo CONNECT, mediante la direttiva Enable.

Quando Caching Proxy viene utilizzato come proxy inverso, la disabilitazione di questa direttiva (impostazione predefinita) consente di proteggere i punti deboli del tunnel SSL da attacchi.

Nota: utilizzare la direttiva Proxy per abilitare l'operazione di tunnel SSL per una porta specifica sull'host di destinazione.

Formato

```
SSLTunneling {on | off}
```

Impostazione predefinita

```
SSLTunneling off
```

SSLVersion — Indica di specificare la versione di SSL

Utilizzare questa direttiva per specificare la versione di SSL da utilizzare: V2, V3 o tutte le versioni. Impostare questa direttiva su `V2` se si utilizzano server che non sono in grado di supportare la versione 3 di SSL.

Nota: le direttive SSL non sono supportate su SUSE Linux.

Formato

```
SSLVersion  {SSLV2 | SSLV3 | all}
```

Impostazione predefinita

```
SSLVersion SSLV3
```

SSLV2Timeout — Indica di specificare il tempo di attesa prima della scadenza di una sessione SSLV2

Utilizzare questa direttiva per specificare, in secondi, il tempo in cui una sessione SSL della versione 2 rimane in attesa senza eseguire attività prima della scadenza della sessione.

Nota: le direttive SSL non sono supportate su SUSE Linux.

Formato

`SSLV2Timeout` *secondi*

dove *secondi* rappresenta un valore compreso tra `0` e `100`.

Impostazione predefinita

```
SSLV2Timeout 100
```

SSLV3Timeout — Indica di specificare il tempo di attesa prima della scadenza di una sessione SSLV3

Utilizzare questa direttiva per specificare, in secondi, il tempo in cui una sessione SSL della versione 3 rimane in attesa senza eseguire attività prima della scadenza.

Nota: le direttive SSL non sono supportate su SUSE Linux.

Formato

`SSLV3Timeout` *secondi*

dove *secondi* rappresenta un valore compreso tra 1 e 86400 secondi (ossia, un giorno).

Impostazione predefinita

```
SSLV3Timeout 100
```

SuffixCaseSense — Indica di specificare se le definizioni di suffisso distinguono tra caratteri maiuscoli e minuscoli

Utilizzare questa direttiva per specificare se si desidera che il server distingua tra caratteri maiuscoli e minuscoli quando i suffissi file vengono confrontati con modelli di suffissi sulle direttive AddClient, AddCharSet, AddType, AddEncoding e AddLanguage. Per impostazione predefinita, il server non distingue tra caratteri maiuscoli e minuscoli.

Formato

```
SuffixCaseSense  {on | Off}
```

Impostazione predefinita

```
SuffixCaseSense  Off
```

SupportVaryHeader — Indica di memorizzare nella cache più di una variante di una risorsa, in base all'intestazione HTTP Vary

Utilizzare questa direttiva per fare in modo che Caching Proxy memorizzi nella cache più di una variante di una risorsa (URI), in base all'intestazione HTTP Vary.

Quando la direttiva SupportVaryHeader è abilitata, il proxy crea un ID cache basato sull'URI e sui valori dell'intestazione selezionata nella richiesta client.

I nomi delle intestazioni selezionate vengono specificati nell'intestazione Vary inviata in una precedente risposta del server. Se il server modifica la serie di nomi intestazione selezionati per una risorsa, tutti gli oggetti precedenti memorizzati nella cache per la risorsa verranno eliminati dalla cache del proxy.

Questa direttiva può essere utilizzata con la direttiva RegisterCacheIdTransformer ("RegisterCacheIdTransformer — Indica di memorizzare più di una variante di una risorsa, in base all'intestazione Cookie" a pagina 255).

Quando si utilizzano entrambe le direttive, il proxy crea un trasformatore ID cache interno basato sull'intestazione Vary dell'intestazione richiesta del server e del client. In questo modo, il proxy può generare identificativi cache univoci per diverse coppie richiesta/risposta, anche se gli URI richiesti sono gli stessi.

Gli oggetti dello stesso URI memorizzati nella cache hanno una propria durata predefinita, a seconda delle intestazioni Expire e Cache-Control nelle impostazioni relative a richieste/risposte o in altre impostazioni di configurazione. Se viene utilizzato il plugin Dynacache, tutte le presentazioni multiple associate allo stesso URI non sono più valide nella cache del proxy.

Formato

```
SupportVaryHeader {on | off}
```

Esempio

In questo esempio, le seguenti direttive sono abilitate e configurate in ibmproxy.conf, come di seguito:

```
SupportVaryHeader on
RegisterCacheIdTransformer Cookie UserGroup
```

Il client Guest accede al server proxy con

```
URI [<code>] http://www.dot.com/group.jpg [</code>]
```

e la seguente richiesta/risposta:

```
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
.......
```

Quindi, il client Admin accede al server proxy con lo stesso URI

```
http://www.dot.com/group.jpg
```

e la seguente richiesta/risposta:

```
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
.......
```

Come risultato, se le risposte sono memorizzabili, il server proxy genere due differenti ID cache:

```
1. CacheID(URI, "Guest", "en_US")
2. CacheID(URI, "Admin", "fr_FR")
```

Il server proxy memorizza nella cache due diverse varianti della risposta inviata dal server. In seguito, quando un client richiede la risorsa (.../group.jpg), con una combinazione di valori di preferenza lingua e gruppo utente, il server proxy richiama e supporta la variante appropriata della risorsa dalla cache.

Impostazione predefinita

```
SupportVaryHeader off
```

TLSV1Enable — Indica di abilitare il protocollo TLS (Transport Layer Secure)

Utilizzare questa direttiva per abilitare il protocollo TLS versione 1 nelle connessioni SSL. Dopo aver attivato questa direttiva, la connessione SSL controlla innanzitutto il protocollo TLS, quindi il protocollo SSLv3, infine il protocollo SSLv2.

Nota: questa direttiva funziona con Internet Explorer e altri browser ma non con Netscape. (È preferibile non utilizzare il browser Netscape con Caching Proxy.)

Formato

```
TLSV1Enable {on | off}
```

Esempio

```
TLSV1Enable on
```

Impostazione della configurazione iniziale

Nessuna

Transmogrifier — Indica di personalizzare la fase Manipolazione dei dati

Utilizzare questa direttiva per specificare una funzione applicativa personalizzata che il server richiama durante la fase Manipolazione dei dati. Questo codice fornisce tre funzioni applicative:

- Una funzione *open* per eseguire l'inizializzazione prima di elaborare i dati
- Una funzione *write* per elaborare i dati
- Una funzione *close* per eseguire eventuali attività di ripulitura
- Una funzione *error* per notificare i problemi che si sono verificati

È possibile avere più direttive Transmogrifier attive per ciascuna istanza del server.

Formato

```
Transmogrifier /percorso/file:nome_funzione:nome_funzione:nome_funzione
```

/percorso/file
Specifica il nome file completo del programma compilato e include l'estensione.

nome_funzione
Specifica il nome assegnato alla funzione applicativa all'interno del programma. È necessario specificare i nomi delle funzioni open, write e close.

Esempio

```
Transmogrifier /ics/bin/icsext05.so:open_data:write_data:close_data
```

Impostazione predefinita

Nessuna

TransmogrifiedWarning — Indica di inviare un messaggio di avvertenza al client

Utilizzare questa direttiva per inviare un messaggio al client per informarlo che i dati:

Formato

```
transmogrifiedwaning {yes|no}
```

Impostazione predefinita

Yes

TransparentProxy — Indica di abilitare il proxy trasparente su Linux o AIX

Solo Linux e AIX. Utilizzare questa direttiva per specificare se il server può essere eseguito come server proxy trasparente.

Nota: quando la direttiva TransparentProxy è impostata su `On`, la direttiva BindSpecific viene ignorata e assume il valore `Off`. Dal momento che la maggior parte del traffico HTTP utilizza la porta 80, si consiglia di configurarla tra le altre.

Formato

```
TransparentProxy  {on | off}
Porta 80
```

Impostazione predefinita

```
TransparentProxy  Off
```

Nota: dopo aver avviato il proxy trasparente, se si intende arrestare il server Caching Proxy, è necessario emettere anche il seguente comando come root:

```
ibmproxy -unload
```

Sui sistemi Linux, questo comando elimina le regole Firewall di reindirizzamento mentre sui sistemi AIX, scarica l'estensione kernel del proxy trasparente. Se non si emette questo comando in seguito all'arresto del server, la macchina accetterà richieste di cui non è destinataria.

UpdateProxy — Indica di specificare la destinazione cache

Utilizzare questa direttiva per specificare il server proxy aggiornato dall'agente cache. La direttiva è obbligatoria se l'agente cache deve aggiornare un server proxy diverso da quello locale su cui l'agente cache è in esecuzione. Facoltativamente, è possibile specificare la porta.

Nota: su piattaforme Linux e UNIX, questa direttiva è obbligatoria per poter utilizzare l'agente cache. Se per il proxy si utilizza solo una macchina, specificare il nome host.

Sebbene l'agente cache possa aggiornare la cache su un altro server, non può richiamare il log accessi cache da quella macchina. Perciò, se la direttiva UpdateProxy specifica un host diverso dall'host locale, la direttiva LoadTopCached viene ignorata.

Formato

```
UpdateProxy nome_host_completo_del_server_proxy
```

Esempio

```
UpdateProxy proxy15.ibm.com:1080
```

Impostazione predefinita

Nessuna

UserId — Indica di specificare l'ID utente predefinito

Utilizzare questa direttiva per specificare il numero o il nome utente assunto dal server prima di accedere ai file.

Se la direttiva viene modificata, è necessario arrestare manualmente il server, quindi riavviarlo, per convalidare le modifiche. Il server non riconosce la modifica se viene solamente riavviato. (Consultare Capitolo 5, "Avvio e arresto di Caching Proxy", a pagina 15.)

Nota: se si modificano i valori predefiniti del server relativamente a ID utente, ID gruppo o percorsi di directory log, creare le nuove directory, quindi aggiornarne autorizzazioni e proprietà. Per fare in modo che il server scriva le informazioni su una directory log definita dall'utente, l'autorizzazione per tale directory deve essere impostata su 755 mentre l'ID del server definito dall'utente deve essere impostato su proprietario. Ad esempio, se si modifica l'ID utente del server dal valore predefinito a jdoe e la directory logs predefinita in server_root/account, la directory server_root/account deve disporre dell'autorizzazione 755 ed essere di proprietà di jdoe.

Formato

```
UserId  {nome_ID | numero}
```

Impostazione predefinita

AIX, Linux, Solaris: `UserId nobody`

HP-UX: `UserId www`

V2CipherSpecs — Indica di elencare le specifiche di codifica supportate per SSL versione 2

Questa direttiva elenca la specifica di codifica disponibile per SSL versione 2.

Nota: le direttive SSL non sono supportate su SUSE Linux.

Formato

```
V2CipherSpecs specifica
```

I valori accettabili prevedono qualsiasi combinazione di quanto segue. Il valore None può essere utilizzato due volte.

- `1` — RC4 US
- `2` — RC4 Export
- `3` — RC2 US
- `4` — RC2 Export
- `6` — DES 56-bit
- `7` — Triple DES US
- `NULL` — Vengono utilizzate le specifiche di codifica predefinite

Esempi

- Per gli Stati Uniti: `V2CipherSpecs '137624'`
- Per l'estero: `V2 Cipherspecs '246'`

Impostazione predefinita

None (SSL è disabilitato per impostazione predefinita.)

V3CipherSpecs — Indica di elencare le specifiche di codifica supportate per SSL versione 3

Questa direttiva elenca le specifiche di codifica disponibili per SSL versione 3.

Nota: le direttive SSL non sono supportate su SUSE Linux.

Se la direttiva FIPSenable è impostata su ″on″, la direttiva V3CipherSpecs verrà ignorata. Per ulteriori informazioni, vedere “FIPSEnable — Indica di abilitare la crittografia approvata FIPS (Federal Information Processing Standard) per SSLV3 e TLS” a pagina 208.

Formato

```
V3CipherSpecs specifica
```

Tra i valori possibili sono inclusi:

- `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 — Vengono utilizzate le specifiche di codifica predefinite.

Esempi

- Per gli Stati Uniti: `V3CipherSpecs '0A09060564620403020100'`
- Per l'estero: `V3Cipherspecs '0906646203020100'`

Impostazione predefinita

None (SSL è disabilitato per impostazione predefinita.)

WebMasterEMail — Indica di impostare un indirizzo e-mail per ricevere report di server selezionati

Utilizzare questa direttiva per impostare un indirizzo e-mail su cui ricevere report Caching Proxyselezionati, ad esempio, una notifica 30 giorni prima della scadenza di un certificato SSL. Su sistemi Linux e UNIX, deve essere in esecuzione un processo sendmail. Per sistemi Windows, il processo sendmail è incorporato in Caching Proxy, per evitare la necessità di un server di posta esterno; tuttavia, è necessario impostare due ulteriori direttive: "WebMasterSocksServer (solo Windows)— Indica di impostare un server Socks per la routine sendmail" e "SMTPServer (solo Windows)— Indica di impostare un server SMTP per la routine Sendmail" a pagina 263.

Nota: questo indirizzo e-mail viene utilizzato anche come password FTP anonima.

Formato

`WebMasterEMail` *`webmastermailaddress`*

Esempio

```
WebMasterEmail webmaster@computer.com
```

Impostazione predefinita

```
WebMasterEmail webmaster
```

WebMasterSocksServer (solo Windows)— Indica di impostare un server Socks per la routine sendmail

Utilizzare questa direttiva per impostare il server Socks utilizzato dalla routine sendmail interna in Caching Proxy per Windows. Per questa routine, è necessario impostare anche le due direttive riportate di seguito: "WebMasterEMail — Indica di impostare un indirizzo e-mail per ricevere report di server selezionati" e "SMTPServer (solo Windows)— Indica di impostare un server SMTP per la routine Sendmail" a pagina 263.

Formato

`WebMasterSocksServer` *`nome host o indirizzo IP del server Socks`*

Esempio

```
WebMasterSocksServer socks.mybox.com
```

Impostazione predefinita

```
Nessuna
```

Welcome — Indica di specificare i nomi dei file di benvenuto

Utilizzare questa direttiva per specificare il nome di un file di benvenuto che il server ricerca per rispondere alle richieste che non contengono uno specifico nome file. È possibile creare un elenco di file di benvenuto inserendo più occorrenze di questa direttiva nel file di configurazione.

Per le richieste che non contengono un nome file o un nome directory, il server ricerca sempre, nella directory root dei file, un file corrispondente a un nome specificato su una direttiva Welcome. In caso di corrispondenza, il file viene restituito al richiedente.

Per richieste contenenti un nome directory ma non un nome file, la direttiva AlwaysWelcome controlla se il server ricerca nella directory un file di benvenuto da restituire. Per impostazione predefinita, AlwaysWelcome è impostata su `On`. In altre parole, il server ricerca sempre nella directory richiesta un file corrispondente a un nome specificato sulla direttiva Welcome. In caso di corrispondenza, il file viene restituito al richiedente.

Se il server riscontra più di una corrispondenza tra i file di una directory e i nomi file sulle direttive Welcome, l'ordine delle direttive Welcome determina quale file verrà restituito. Il server utilizza la direttiva Welcome più vicina all'inizio del file di configurazione.

Formato

```
Welcome nome_file [indirizzo_IP_server |
nome_host]
```

nome_file
Specifica il nome di un file che si intende definire come file di benvenuto.

[*indirizzo_IP_server* **|** *nome_host***]**
Se si utilizzano più indirizzi IP o host virtuali, utilizzare questo parametro per specificare un indirizzo IP o un nome host. Il server utilizza la direttiva esclusivamente per le richieste inviate al server su questo indirizzo IP o per questo host. Per un indirizzo IP, si tratta dell'indirizzo della connessione di rete del server e non dell'indirizzo del client richiedente.

È possibile specificare un indirizzo IP (ad esempio, `240.146.167.72`), o un nome host (ad esempio, `hostA.bcd.com`).

Questo parametro è opzionale. Senza questo parametro, il server utilizza la direttiva per tutte le richieste a prescindere dall'indirizzo IP su cui è stata ricevuta la richiesta o dal nome host negli URL.

Per un indirizzo IP del server non è possibile specificare un carattere jolly.

Esempi

- L'esempio riportato di seguito definisce due pagine iniziali e presuppone che la direttiva AlwaysWelcome sia impostata sul valore predefinito `On`. Per le richieste che non contengono un nome file, il server tenta di restituire un file di benvenuto dalla directory specificata sulla richiesta (o dalla directory root dei file, se la richiesta non specifica un nome file o una directory). Il server ricerca

innanzitutto un file denominato letsgo.html. Se non è presente alcun file con questo nome nella directory, il server ricerca un file denominato Welcome.html.

```
Welcome letsgo.html
Welcome Welcome.html
```

- Nell'esempio riportato di seguito, il server ricerca file di benvenuto differenti, in base all'indirizzo IP della connessione di rete su cui è stata ricevuta la richiesta. Per le richieste in entrata su 0.67.106.79, il server ricerca i file di benvenuto denominati CustomerA.html. Per le richieste in entrata su 0.83.100.45, il server ricerca file di benvenuto denominati CustomerB.html. Se la richiesta arriva su un indirizzo IP differente, il server ricerca l'indirizzo predefinito.

  ```
  Welcome CustomerA.html  0.67.106.79
  Welcome CustomerB.html  0.83.100.45
  ```

- Nell'esempio riportato di seguito, il server ricerca file di benvenuto differenti, in base al nome host nell'URL. Per le richieste in entrata per hostA, il server ricerca file di benvenuto denominati CustomerA.html. Per le richieste in entrata per hostB, il server ricerca file di benvenuto denominati CustomerB.html. Se la richiesta è indirizzata a un host differente, il server ricerca il nome host predefinito.

  ```
  Welcome CustomerA.html  hostA.bcd.com
  Welcome CustomerB.html  hostB.bcd.com
  ```

Impostazioni predefinite

Queste impostazioni predefinite si trovano nell'ordine utilizzato dalla configurazione predefinita:

```
Welcome Welcome.html
Welcome welcome.html
Welcome index.html
Welcome Frntpage.html
```

Informazioni particolari

Terza edizione (Giugno 2005)

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti d'America.

IBM non può offrire in altri paesi i prodotti, i servizi o le funzioni descritti in questo documento. Per le informazioni sui prodotti ed i servizi disponibili al momento nella propria area, rivolgersi al rivenditore IBM locale. Qualunque riferimento relativo a prodotti, programmi o servizi IBM non implica che solo quei prodotti, programmi o servizi IBM possano essere utilizzati. In sostituzione a quelli forniti da IBM, possono essere usati prodotti, programmi o servizi funzionalmente equivalenti che non comportino violazione dei diritti di proprietà intellettuale o di altri diritti dell'IBM. È tuttavia responsabilità dell'utente valutare e verificare la funzionalità di tali prodotti, programmi e servizi non IBM.

IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nel presente documento. La fornitura di questa pubblicazione non implica la concessione di alcuna licenza su di essi. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

IBM Corporation
Attn.: G71A/503
P.O. box 12195
3039 Cornwallis Rd.
Research Triangle Park, N.C. 27709-2195
Deutchland

Per domande sulle licenze relative a informazioni DBCS, contattare IBM Intellectual Property Department nel proprio paese oppure scrivere a:

IBM World Trade Asia Corporation Licensing
2-31
Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

Il seguente paragrafo non è valido per il Regno Unito o per tutti i paesi le cui leggi nazionali siano in contrasto con le disposizioni in esso contenute:

INTERNATIONAL BUSINESS MACHINES CORPORATION FORNISCE QUESTA PUBBLICAZIONE NELLO STATO IN CUI SI TROVA SENZA ALCUNA GARANZIA, ESPLICITA O IMPLICITA, IVI INCLUSE EVENTUALI GARANZIE DI COMMERCIABILITÀ' ED IDONEITÀ AD UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni, quindi, la presente dichiarazione potrebbe non essere a voi applicabile.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le informazioni incluse in questo documento non vengono modificate su base periodica; tali modifiche verranno incorporate nelle nuove edizioni della pubblicazione. IBM si riserva il diritto di apportare miglioramenti e/o modifiche ai prodotti o ai programmi descritti nel manuale in qualsiasi momento e senza preavviso.

Tutti i riferimenti a siti Web non dell'IBM contenuti in questo documento sono forniti solo per consultazione. I materiali contenuti in tali siti Web non fanno parte della documentazione per questo prodotto IBM e il loro utilizzo è a discrezione dell'utente.

IBM può utilizzare o distribuire qualsiasi informazione fornita dall'utente nel modo più appropriato senza incorrere in alcuna obbligazione.

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire: (i) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi a:

IBM Corporation
ATTN: Software Licensing
11 Stanwix Street
Pittsburgh, PA 15222-9183
Deutchland

Queste informazioni possono essere rese disponibili secondo condizioni contrattuali appropriate, compreso, in alcuni casi, l'addebito di un canone.

Il programma su licenza descritto in queste informazioni e tutto il materiale su licenza ad esso relativo sono forniti da IBM nel rispetto delle condizioni previste dall'accordo IBM International Program License Agreement o da accordi equivalenti.

Tutti i dati relativi alle prestazioni contenuti in questa pubblicazione sono stati determinati in ambiente controllato. Pertanto, i risultati ottenuti in ambienti operativi diversi possono variare in modo considerevole. Alcune misure potrebbero essere state fatte su sistemi di livelli di sviluppo per cui non si garantisce che queste saranno uguali su tutti i sistemi disponibili. Inoltre, alcune misure potrebbero essere state ricavate mediante estrapolazione. I risultati possono quindi variare. Gli utenti di questa pubblicazione devono verificare che i dati siano applicabili al loro specifico ambiente.

Le informazioni relative a prodotti non IBM sono state ottenute dai fornitori di tali prodotti. IBM non ha verificato tali prodotti e, pertanto, non può garantirne l'accuratezza delle prestazioni o la compatibilità. Eventuali commenti relativi alle prestazioni dei prodotti non IBM devono essere indirizzati ai fornitori di tali prodotti.

Tutte le dichiarazioni riguardanti la futura direzione o le intenzioni dell'IBM sono soggette a sostituzione o al ritiro senza preavviso e rappresentano unicamente scopi e obiettivi della IBM stessa.

Queste informazioni contengono esempi di dati e report utilizzati quotidianamente nelle operazioni aziendali. Per meglio illustrarli, tali esempi contengono nomi di persone, società, marchi e prodotti. Tutti i nomi contenuti nel manuale sono fittizi e ogni riferimento a nomi ed indirizzi reali è puramente casuale.

Se si stanno visualizzando queste informazioni in formato elettronico, le illustrazioni a colori e le foto potrebbero non essere visualizzate.

Marchi

I seguenti termini sono marchi di IBM Corporation, negli Stati Uniti, in altri paesi o in entrambi:

- AIX
- IBM
- Netfinity
- RS/6000
- SecureWay
- Tivoli
- ViaVoice
- WebSphere

Java e tutti i marchi basati su Java sono di Sun Microsystems, Inc. negli Stati Uniti, in altri paesi o in entrambi.

Microsoft, Windows, Windows NT e il logo Windows sono marchi di Microsoft Corporation negli Stati Uniti, in altri paesi o in entrambi.

Intel, Intel Inside (loghi), MMX and Pentium sono marchi di Intel Corporation negli Stati Uniti, in altri paesi o in entrambi.

UNIX è un marchio registrato di The Open Group negli Stati Uniti e in altri paesi.

Linux è un marchio di Linus Torvalds, negli Stati Uniti, in altri paesi o in entrambi.

Nomi di altri prodotti, società o servizi possono essere marchi di altre società.

Stampato in Italia

GC13-3366-01

Spine information:

WebSphere Application Server **Caching Proxy Administration Guide** Versione 6.0.2 GC13-3366-01