







Web Server: IIS e Apache

Oggi parleremo di

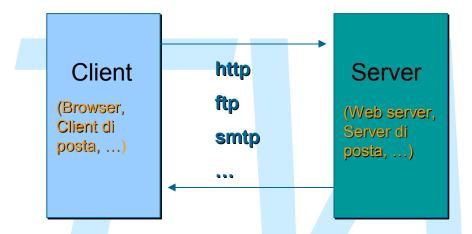
Web Server: cosa sono

Internet Information Services

Apache

Web server

Architettura client-server:



Ogni applicazione server resta in attesa di una richiesta ad una specifica porta:

- Web server: richieste HTTP su porta 80
- Server FTP: richieste su porta 21
- Server di posta: richieste SMTP su porta 25

•

Web Server: tipi di risorse (1)

Risorse statiche

- i contenuti provengono da file fisicamente presenti sul server:
 - * l'URL della richiesta viene mappato in un path locale del server che indirizza il file contenente la risorsa (documento HTML, immagine, documento CSS, ...)
 - + ad es. l'URL

http://www.nomesito.com/percorso/index.htm

viene mappato dal client in una richiesta HTTP di questo tipo:

GET /percorso/index.htm HTTP/1.1 Host: www.nomesito.com

ed il server restituisce la risorsa presente nel file indirizzato dal path /percorso/index.htm (percorso relativo alla radice del web server)

gestione veloce delle risposte

Web Server: tipi di risorse (2)

Risorse dinamiche

- i contenuti vengono generati dinamicamente da altri programmi o script richiamati dal web server:
 - in base al percorso specificato nell'URL o all'estensione del file specificato nel percorso il web server richiama un apposito programma o una libreria per la generazione della risorsa richiesta
 - + ad es. se l'URL richiesto è

 http://www.nomesito.com/index.php

il web server richiama la libreria php passandogli il documento index.php e restituisce al client la risposta che riceve

- possibilità di creare contenuti "al volo"
- minore efficienza nei tempi di risposta

Introduzione a IIS

Definizione

IIS: <u>Internet Information Services</u> è il server web di Microsoft per sistemi Windows.

Installazione

Dal pannello "Installazione componenti di Windows" accessibile da "Installazione applicazioni" del "Pannello di controllo"

Una volta installato presenta la seguente struttura :

- \systemroot\system32\inetsrv (libreria di sistema)
- Inetpub (la radice del server)
- \systemroot\help\iishelp (i file di help)
- Inetpub\wwwroot (sito web di default)

Organizzazione dei contenuti

Un sito su IIS può essere organizzato in due modi:

- Una directory di root locale (di default \Inetpub\wwwroot) e al suo interno tutte le sottodirectory
- Un insieme di Virtual Directory. Sono directory non necessariamente contenute fisicamente in IIS ma che fanno parte dell'insieme dei contenuti associati ad un sito web. Possono essere di due tipi:
 - Directory locali, ma non dipendenti dalla directory di root
 - Directory remote identificate da URL

Conviene usare le Virtual Directory?

- Pro: Flessibilità e Scalabilità
- Contro: Prestazioni ridotte

IIS request Processing

Quando IIS riceve una richiesta, determina dall'URL se riguarda un documento statico (HTML) o dinamico:

- ◆ Pagina HTML: ritorna la pagina immediatamente (lo stesso meccanismo per immagini, CSS, javascript, etc.etc.)
- ◆ File corrispondenti a determinate estensioni ISAPI: carica la DLL appropriata con cui gestire la richiesta (ad esempio le richieste di file .asp vengono dirette al file ASP.dll)
- Applicazioni CGI: viene creato un nuovo processo a cui passare tutti i parametri attraverso l'ambiente di gestione del processo

Configurare IIS

- ◆ IIS permette di costruire e configurare diversi siti sullo stesso server (solo nelle versioni Server di Windows)
- ◆ La configurazione di ciascun sito è registrata in un "metabase", che assume valori di default al momento dell'installazione.
- Ogni sito web in IIS ha associato un insieme di "classi" per gestire le proprietà del sito.
- Esistono tre livelli gerarchici di configurazione:
 - * *Master*: fissa una configurazione comune a tutti i siti web
 - * Site by site: fissa una configurazione specifica per un sito
 - + File by file: fissa una configurazione specifica per un file
- Ad ogni livello, la configurazione avviene tramite il menù Proprietà.

Configurare IIS

Il web server può essere configurato tramite la console "Internet Information Service" accessibile da "Strumenti di amministrazione" in "Pannello di controllo" che definisce un diverso numero di sezioni principali in base alla versione di IIS installata:

- Sito Web
- Operators (non presente nella versione 5.1)
- Performance (non presente nella versione 5.1)
- Filtri ISAPI
- Home Directory
- Documenti
- Protezione directory
- Intestazioni HTTP
- Messaggi di errore personalizzati

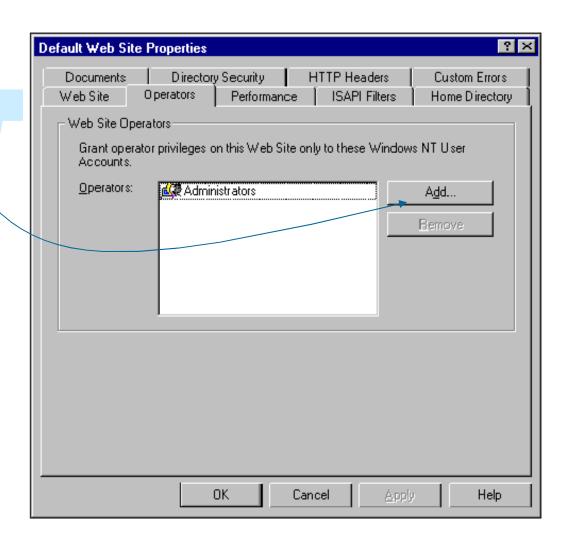
Sito Web

Proprietà - Sito Web predefinito Estensioni del server Identificazione del Sito Intestazioni HTTP Messaggi di errore personalizzati Sito Web Filtri ISAPI Home directory Protezione directory Documenti Informazioni Web. Identificazione sito Web generali Sito Web predefinito Descrizione: 127.0.0.1 Indirizzo IP: Avanzate... 80 Porta TCP: Porta SSL: Controlli sullo stato delle Connessioni connessioni Timeout connessione: 900 secondi Abilita keep-alive HTTP Consenti registrazione attività Controllo dei meccanismi Formato registro attivo: di logging del sito Proprietà... Formato di file registro esteso W3C Come creare i log Quali formati per i file di log OK Annulla Applica

Operators

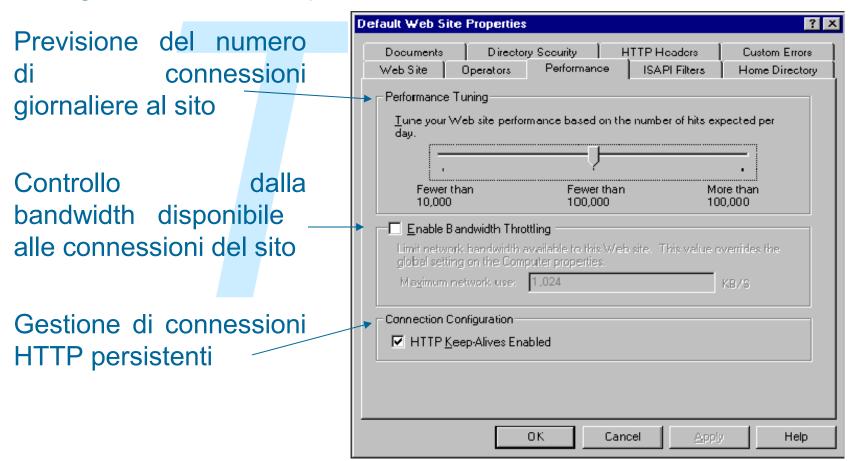
Per assegnare i privilegi di amministrazione ad utenti del sistema

Di default i privilegi sono assegnati al gruppo "Amministratori"



Performance

Consente di migliorare le prestazioni del sito Web tramite la configurazione di alcuni parametri



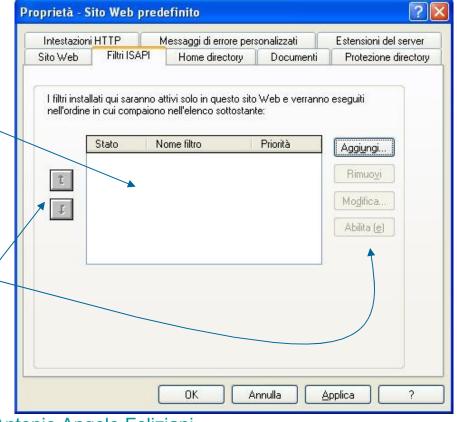
Filtri ISAPI

Permette la configurazione dei filtri ISAPI (Internet Server Application Programming Interface). I filtri ISAPI sono librerie associate a determinate estensioni dei file e attivate al momento della richiesta di file con tali estensioni

Lista dei filtri ISAPI con stato (Loaded, Unloaded, Disabled), nome e priorità (High, Medium, Low)

Tasti per aggiungere e rimuovere i filtri o modificarne lo stato

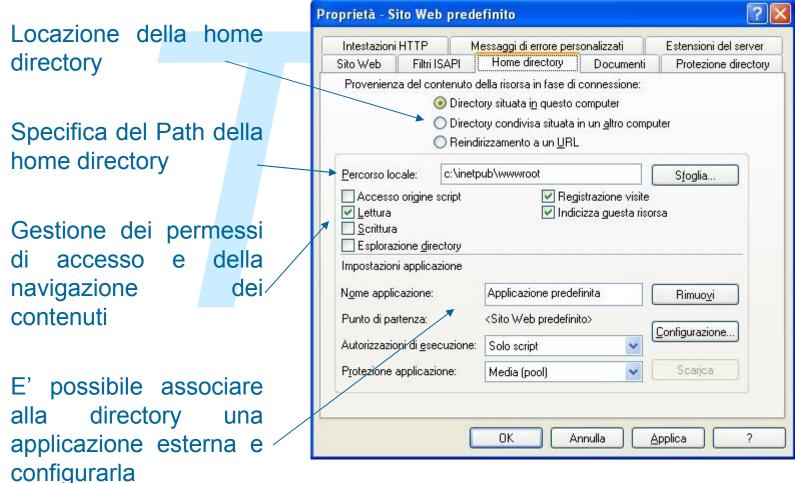
Modifica delle priorità dei filtri



Home Directory

Consente di configurare le caratteristiche della directory principale

del sito

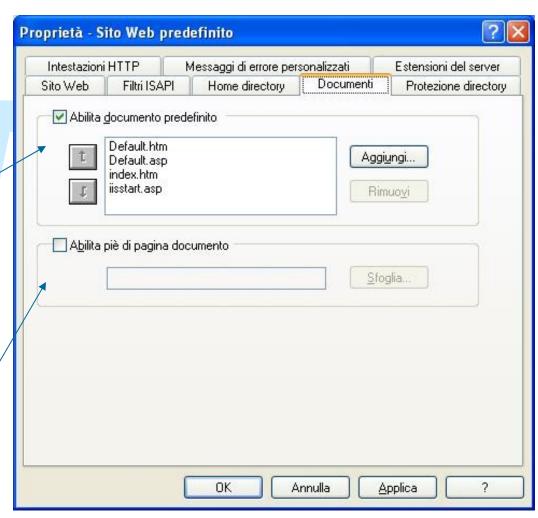


Documenti

Consente di specificare i documenti di default:

Definisce i documenti di default, cioè i documenti inviati al client quando l'URL specifica una directory

Specifica un "footer" da inserire in ogni pagina automaticamente



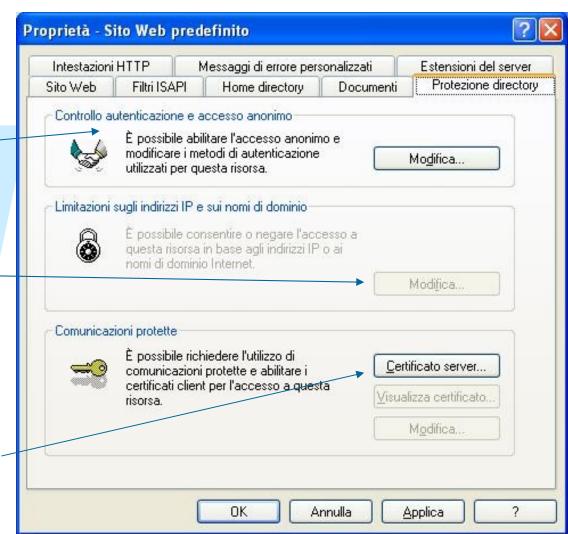
Protezione directory

Configurazione dell'accesso anonimo e dei metodi di autenticazione

Gestione delle politiche di accesso (solo per versioni Server di Windows)

- granted access
- denied access

Creazione della richiesta per ricevere un certificato digitale SSL



Anonymous Access and Authentication Control

Esistono tre meccanismi di autenticazione e controllo sugli accessi al server:

Allow Anonymous Access: consente l'accesso al server a utenti non riconosciuti (anonymous user), creando una connessione anonima e assegnando loro un account anonimo. L'account usato è un account valido per il sistema.

Basic Authentication: esegue un riconoscimento dell'utente che vuole accedere al server tramite la richiesta di login e password trasmessi in chiaro sulla connessione.

Windows NT Challenge/Response: meccanismo di autenticazione basato sullo scambio non in chiaro di login e password che richiede l'uso di Microsoft Internet Explorer versione 2.0 o successiva

Cosa è un certificato?

- I certificati sono una forma di identificazione digitale che consente ai Web server e ai client l'autenticazione prima di stabilire una connessione
- Sono parte del protocollo SSL per l'utilizzo di connessioni sicure: per sfruttare connessioni SSL un Web server deve ottenere ed installare un certificato
- I certificati contengono chiavi utilizzate per criptare le connessioni
- Possono essere rilasciati da organizzazioni per la certificazione che garantiscono sulle informazioni contenute nel certificato

Gestione dei certificati in IIS

Per installare una connessione SSL su un sito, si deve creare un certificato che garantisca l'identità del sito. IlS mette a disposizione una procedura per la creazione della richiesta di certificato

- Si lancia il tool di IIS che richiede l'inserimento delle informazioni da includere nel certificato.
- questo tool genera un codice criptato che rappresenta la richiesta da inoltrare ad un ente certificatore per ottenere il certificato vero e proprio.
- ottenuta questa richiesta, ci si collega ad un sito che fornisce i certificati (es: www.instantssl.com)
- si spedisce via form (o via mail) la richiesta criptata
- si riceve per posta il certificato vero e proprio
- In seguito IIS permette di installare il certificato ricevuto, di modificarlo, cambiarlo ecc. e abilitare la connessione SSL

Utilizzo dei certificati

Una visione ad alto livello di SSL:

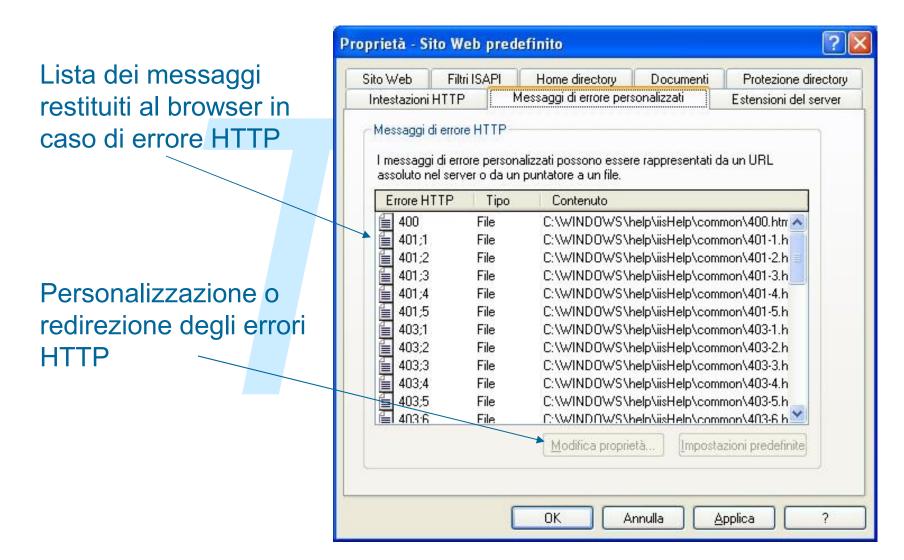
- Il browser cerca di stabilire una connessione sicura (le pagine si richiamano con https://)
- Il server invia il suo certificato con la chiave pubblica
- Il browser genera una chiave di sessione e la cifra utilizzando la chiave pubblica del server e gliela invia
- Utilizzando la sua chiave privata il server decodifica la chiave di sessione e il canale è così stabilito.
- Server e browser comunicano usando la chiave di sessione

Intestazioni HTTP

Consente di creare specifici header HTTP da spedire al browser

Proprietà - Sito Web predefinito Gestione della Filtri ISAPI Home directory Documenti Sito Web Protezione directory scadenza delle pagine Intestazioni HTTP Messaggi di errore personalizzati Estensioni del server Abilita scadenza contenuto Scadenza contenuto: Immediata Creazione di "HTTP Dopo: Scadenza venerdi 17 marzo 2006 Header" personalizzati Intestazioni HTTP personalizzate Aggi<u>u</u>ngi. Modifica. Classificazione via PICS dei contenuti del sito Classificazioni del contenuto L'impostazione delle classificazioni consente agli Modifica classificazioni. utenti di identificare il tipo di contenuto disponibile nel sito. Gestione dei tipi MIME Mapping MIME Per configurare ulteriori tipi MIME inviati dal servizio Web al browser nell'intestazione HTTP, (Multipurpose Internet Tipi di file... scegliere il pulsante Tipi di file. Mail Extension) OK Annulla Applica

Messaggi di errore personalizzati



Apache HTTP Server

- Apache HTTP Server è il web server HTTP della Apache Software Foundation
- Sviluppato e aggiornato per sistemi operativi come UNIX e Windows
- Open-source
- Apache è dal 1996 il web server più diffuso in Internet (nel 2005 usato dal 70% dei siti web)

Compilazione e installazione per sistemi Unix-like

```
Download $ lynx http://httpd.apache.org/download.cgi
Extract
        $ gzip -d httpd-NN.tar.gz
         $ tar xvf httpd-NN.tar
         $ cd httpd-NN
Configure $ ./configure --prefix=PREFIX
Compile $ make
Install $ make install
Customize $ vi PREFIX/conf/httpd.conf
Test
         $ PREFIX/bin/apachectl -k start
```

Starting Apache

In Unix Apache è un programma **httpd** eseguito in background come demone che gestisce le richieste.

httpd può essere eseguito lanciando lo script apachectl, che configura alcune variabili di ambiente dipendenti dal sistema operativo.

(può essere lanciato all'avvio del sistema aggiungendo una chiamata allo script apachectl ai file di startup (tipicamente rc.local))

Lo script apachectl permette il controllo del ciclo di vita del web server. E' possibile specificare quattro operazioni:

Start: avvia il server

Stop: blocca l'esecuzione

Restart: ri-avvia il server

Graceful restart: ri-avvia dopo aver terminato i processi-figlio

httpd legge il file di configurazione httpd.conf

Compilazione, installazione e configurazione per sistemi Windows

Download:

http://httpd.apache.org/download.cgi

Installazione:

- pacchetto auto-installante
- compilazione da sorgenti

Configurazione parametri di Apache: modificare del file http.conf con un editor testuale

Esecuzione:

- come servizio di Windows apache -k install -n "ServiceName" -f "c:\path_to_conf\my.conf"
- da console apache

Modularità di Apache

Apache è un server modulare: le sue funzionalità sono rese disponibili tramite dei moduli che possono essere aggiunti o disattivati nel server sfruttando il modulo mod_so

Le funzionalità di base sono incluse nel core Server

Nel processo di configurazione si possono scegliere i moduli da aggiungere al server

I moduli possono essere :

- Compilati staticamente nel web server
- Aggiunti dinamicamente nel file httpd.conf sfruttando il supporto DSO (Dynamic Shared Object)

Esempi: mod_auth (autenticazione utenti usando file di testo), mod_cgi (esecuzione di moduli cgi), mod_ISAPI (estensione ISAPi per Apache sotto Windows), mod rewrite (riscrittura degli URL), mod dav (WEBDAV)

Multi – Processing Modules (MPMs)

Apache è stato progettato per essere flessibile su ogni tipo di piattaforma e con "ogni" configurazione d'ambiente

E' possibile aggiungere moduli MPM, per la gestione di operazioni quali il binding, accept delle richieste, gestione dei processi / threads, connessioni.

Un modulo MPM è compilato nel server e permette :

- ◆ a sistemi operativi differenti di fornire moduli appropriati per ottenere maggiore efficienza
- agli amministratori, in base alle esigenza del proprio web server, di applicare politiche diverse

Solo un modulo MPM per volta può essere caricato nel server

Esempi MPM: mpm_winnt, prefork, mpmt_os2

File di configurazione

Apache viene configurato tramite delle direttive riportate nel file di testo httpd.conf

La configurazione è aggiornata solo al riavvio del server

La gestione dei tipi MIME è gestita nel file mime.types

Le direttive si applicano all'intero server, a meno di specificare lo scope, se consentito, in cui sono valide (es. usando <Directory> per definire la directory in cui applicarla)

Il file di configurazione principale è *httpd.conf*, ma se ne possono creare di nuovi, per ogni sito o ogni directory. Si usano i file *.htaccess*, le cui direttive vengono applicate solo al sotto albero in cui il file *.htaccess* è presente.

Uso delle direttive nei file di configurazione

Le direttive nei file di configurazione possono essere applicate all'intero server, a directory, a file, host o URL

Possono essere valutate solo all'avvio del server (es. < If Module > oppure ad ogni richiesta ricevuta

Possono riguardare la struttura del filesystem (es. <Directory>) oppure la struttura del sito (Es. location)

Alcune direttive consentono l'uso di espressioni regolari secondo la sintassi Perl (es. DirectoryMatch):

```
<Directory /home/Rossi/public_cgi/>
Options ExecCGI
</Directory>
```

Autenticazione

Richiede innanzitutto la creazione di un file delle password (htpasswd-c /usr/locl/apache/passwd/password) utente.

Utilizzando il modulo mod_auth_dbm le utenze possono anche essere gestite tramite un database

Esempio di configurazione degli accessi:

```
AuthType Basic
AuthName "Restricted Area"
AuthUserFile /usr/locl/apahce/passwd/password
require valid-user
```

L'abilitazione all'accesso può essere anche assegnato in base all'host-name o all'host-address della macchina che richiede il documento

```
allow from 205.252.46.165 deny from 205.252.46.165
```

Autenticazione

AuthType Basic

Seleziona il metodo di autenticazione utilizzato

Basic è implementato dal modolo mod_auth

Digest è implementato dal modulo mod_auth_digest

AuthName "Restricted Area"

identifica un nome per l'area a cui accedere per consentire il riutilizzo delle password al client

AuthUserFile /usr/locl/apache/passwd/password il file contenente le password

Require valid-user

specifica il nome dell'utente abilitato all'accesso. Si possono anche creare dei gruppi per consentire l'accesso a più utenti.

SSL con APACHE

La Apache Software Foundation non include nel progetto Apache Httpd il modulo per il supporto di SSL

Esistono due progetti open source che si propongono di garantire il supporto di SSL: mod_ssl e Apache-SSL, ed entrambi gestiscono le connessioni sicure appoggiandosi alle librerie del progetto OpenSSL

Esistono altre implementazioni commerciali di moduli SSL per Apache: "Covalent Raven SSL Module For Apache", la distribuzione IBM di Apache "IBM Http Server".

Direttive per l'uso di SSL

SSLSessionCache: imposta il tipo di memorizzazione della cache

SSLEngine è la direttiva che abilita o disabilita le connessioni SSL

SSLProtocol controlla la versione del protocollo che verrà usata durante le transazioni sicure. Es. SSLProtocol All -SSLv2

SSLCertificateFile e SSLCertificateKeyFile contengono banalmente il path ai file certificato e chiave del server

SSLRequireSSL: usata nelle sezioni "<directory>" consente di rendere accessibili alcune aree del nostro server solo attraverso connessioni sicure

SSLCipherSuite permette di configurare gli algoritmi crittografici che il client può usare quando viene stabilita la connessione

Variabili d'ambiente

Apache utilizza variabili d'ambiente per gestire operazione come il log o il controllo degli accessi e per comunicare con programmi esterni come script CGI

Le direttive SetEnv, SetEnvlf permettono di definire le variabili d'ambiente, specificando eventualmente determinate condizioni

Le variabili possono essere utilizzate all'interno delle direttive per regolare operazioni del server

Utilizzo di script CGI con Apache

Il CGI (Common Gateway Interface) fornisce al server un meccanismo per interagire con programmi esterni nella creazione dei contenuti attraverso l'uso di programmi (script) CGI.

Ci sono due metodi per configurare Apache nell'utilizzo di CGI.

 Definire una directory che contiene gli script, i quali devono avere i diritti di esecuzione

```
ScriptAlias /cgi-bin /usr/local/apache/cgi-bin
```

 Dichiarare il permesso di eseguire gli script all'interno di determinate directory

```
<Directory /usr/local/apache/htdocs/somedir>
Options +ExecCGI
</Directory>
```

Inoltre è possibile specificare l'estensione dei file da eseguire via CGI AddHandler cgi-script cgi pl

Gestione degli utenti

E' possibile definire per ogni utente del sistema una directory nella quale rendere disponibili sul web i propri documenti:

```
UserDir /var/www/*/public_html
```

Si possono inoltre selezionare gli utenti che possono usare tale funzionalità

Per abilitare gli utenti all'uso di script CGI personali:

```
<Directory /home/*/cgi-bin/>
Options ExecCGI
SetHandler cgi-script
</Directory>
```

URL Rewriting

Apache fornisce con il modulo mod_rewrite una tecnica per manipolare gli URL in modo tale da consentirne elaborazione interna o ridirezione

Il modulo deve essere esplicitamente attivato nel server (il modulo simile mod alias è già attivato ma è meno potente) e:

- Usa espressioni regolari
- Permette di specificare un numero illimitato di regole di riscrittura e di condizioni per la riscrittura
- Può essere usato anche su variabili d'ambiente, header HTTP e time stamp
- Sia usa sia nel contesto del web-server (httpd.conf) che nelle directory (.htaccess), ma con differenti prestazioni.

URL Rewriting: esempi

Ridirezionare le richieste ad uno script

```
RewriteEngine on
RewriteRule ^/(.*)\.html$ /script.php
```

Cambiare la struttura delle directory

```
RewriteEngine on RewriteRule ^{-}([a-zA-z0-9]+)/(.+) /home/$1/public_html/$2
```

Modificare i contenuti in base all'ora del giorno

```
RewriteEngine on

RewriteCond %{TIME_HOUR}%{TIME_MIN} >0700

RewriteRule ^home\.html$ home_day.html
```

Spostare le home su un webserver differente

```
RewriteEngine on
RewriteRule ^/~(.+) http://newserver/~$1
```

I file di log

/logs/access.log: registra gli accessi avvenuti con successo

/logs/error.log: registra (e descrive brevemente) gli errori

rewrite.log: non esiste di default ma deve essere esplicitamente indicato nella configurazione di rewriting. Registra le modifiche agli URL delle richieste

Nel file di configurazione è possibile settare i nomi dei file di log:

ErrorLog logs/error.log
CustomLog logs/access.log

Utilizziamo i file di log appunto per controllare il flusso di richieste HTTP e (spesso) individuare gli errori

Riferimenti

http://www.microsoft.com/WindowsServer2003/iis/default.mspx

http://msdn.microsoft.com/

http://httpd.apache.org

www.openssl.org