Configurazione e gestione server IIS (Information Internet Services)

Server Web

Il browser Web ed il protocollo HTTP

- Il protocollo HTTP specifica come i dati sono trasferiti (HTTP nulla dice sul tipo dei dati o su come essi sono elaborati);
- Il web browser sulla macchina client ha il compito di elaborare i dati ricevuti.

Uniform Resource Locator (1/2)

- Ogni documento del WWW è identificato per il tramite di un identificatore detto URL (Uniforme Resource Locator) costruito secondo la sintassi seguente:
  <metodo>://<nome host>:<numero porta>/<cammino directory>;
- Il metodo d'accesso puo' avere valori http, telnet, mailto, file, https (l'aggettivo Uniform indica che possono essere locate risorse differenti);

Uniform Resource Locator (2/2)

- telnet: per aprire una sessione telnet sulla macchina remota;
- mailto: apre il cliente di posta elettronica configurato sulclient;
- file: da usarsi quando la risorsa è un file locale;
- https: se il client deve accedere ad una pagina sicura (vedi dispense "Gli aspetti di sicurezza").

Cosa fa un browser web (1/2)

- Elaborazione dell'input dell'utente;
- Gestione dei protocolli applicativi (http, ftp, telnet...);
- Interpretazione del codice HTML caricato:
  - Rappresentazione del testo, opportunamente formattato;
  - Riconoscimento all'interno del codice HTML delle „etichette" (tags) dei links alle altre pagine per rappresentarli in modo differenziato;

Cosa fa un browser web (2/2)

  - Riconoscimento all'interno del codice HTML delle etichette IMG, che rinviano a files di immagine, per scaricarli dal server e rappresentarli nella pagina (se il browser comprende il formato);
  - Caching di pagine e di immagini per incrementare la velocità;
- Interpretazione di contenuti particolari quali:
  - Immagini;
  - Files audio, video, tabelle di calcolo, documenti di word processor,…
  - Programmi e codici scripts (JavaScripts, Java, Active-X)

Il protocollo HTTP (1/2)

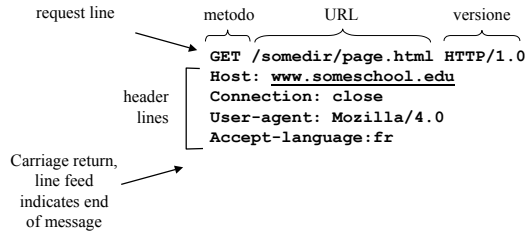
- I messaggi HTTP sono specificati nel RFC 1945 per la versione 1.0 (60 pagine) e nel RFC 2616 per la versione 1.1 (176 pagine);
- A titolo di curiosità: la primissima versione ufficializzata di HTTP, la versione 0.9 del 1991, era contenuta in 2 pagine!

Il protocollo HTTP (2/2)

- La grossa novità offerta dalla versione HTTP 1.1 rispetto alle precedenti è la possibilità (anzi l'obbligo) per il cliente di specificare il nome sito. In tal modo siti multipli possono essere ospitati sul medesimo indirizzo IP;
- I messaggi HTTP sono di due tipi:
  - Messaggi di richiesta e messaggi di risposta.

I messaggi HTTP di richiesta (1/7)

- La struttura di un messaggio di richiesta (full request):



I messaggi HTTP di richiesta (2/7)

- I campi della linea di richiesta:
  - Metodo: GET ¦ POST ¦ HEAD ¦ ....
  - URL;
  - Versione del protocollo: di ovvio significato;
- La maggior parte dei messaggi di richiesta HTTP usa il metodo GET (il browser richiede un oggetto) specificando l'oggetto specificato tramite l'URL;

I messaggi HTTP di richiesta (3/7)

- Alla linea di richiesta segue un blocco di intestazione fatto di linee (linee di intestazione) costruite da "tag", doppio punto, valore del tag in analogie alle intestazioni usate nei messaggi di posta elettronica e per il MIME.
- Le linee del blocco intestazione servono al client per fornire informazioni su se stesso, sulla richiesta inoltrata ed eventualmente sul blocco dati richiesto se il metodo è associato alla trasmissione di un blocco dati.

I messaggi HTTP di richiesta (4/7)

- Accept: tipo dati che il client puo'accettare dal server secondo la specifica tipo MIME (text/html, video (mpeg, image/gif…)
- Accept-charset. Insieme caratteri che ilclient puo' accettare
- Authorization: informazioni di autenticazione per pagine protette;
- If-Modified-Since: il client ha una copia della pagina nella cache e richiede al server la trasmissione solo se modificata nel frattempo;

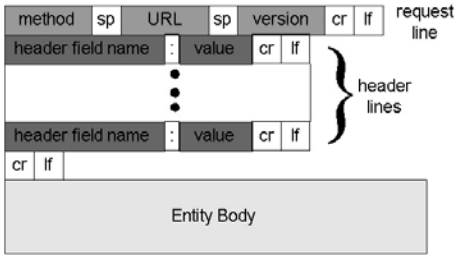
I messaggi HTTP di richiesta (5/7)

- Host: quale pagina web è richiesta;
- User-agent: nome e versione del browser;
- Referrer: l'URL della pagina contenente il link cliccato per ottenere la pagina;

I messaggi HTTP di richiesta (6/7)

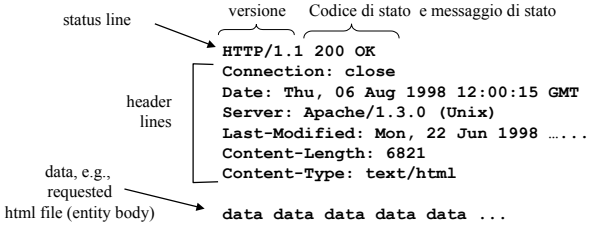
- I campi dell'header devono essere terminati da una riga bianca che serve al server per identificare la fine del blocco intestazioni;
- Dopo la linea bianca puo' essere presente il blocco dati che il client trasmette al server se richiesto dal metodo (p.es. POST o PUT).

I messaggi HTTP di richiesta (7/7)



I messaggi HTTP di risposta (1/7)

- La struttura di un messaggio di risposta



I messaggi HTTP di risposta (2/7)

- Il messaggio di risposta s'inizia con la "linea di stato" per informare il client sull'esito della richiesta effettuata;
- I campi della linea di stato:
  - Versione del protocollo: di ovvio significato;
  - Un codice di stato di 3 cifre;
  - Il corrispondente messaggio di stato.

I messaggi HTTP di risposta (3/7)

- I codici di stato piu' comuni:

200 OK
  - request succeeded, requested object later in this message

301 Moved Permanently
  - requested object moved, new location specified later in this message (Location:)

400 Bad Request
  - request message not understood by server

404 Not Found
  - requested document not found on this server

505 HTTP Version Not Supported

I messaggi HTTP di risposta (4/7)

- La lista completa dei codici di stato puo' essere reperita nella RFC 2616;
- Il codice è costruito secondo lo schema:
  - 1xx: informativi;
  - 2xx: successo;
  - 3xx: riindirizzamento;
  - 4xx: errore del client;
  - 5xx: errore del server.

I messaggi HTTP di risposta (5/7)

- Alla "linea di stato" il blocco intestazione fatto da linee (linee d'intestazione) costruite da "tag", doppio punto, valore del tag in analogia alle intestazioni usate nei messaggi di posta elettronica e per il MIME;
- Gli headers servono al server per fornire informazioni su se stesso e sui dati trasmessi al client.

I messaggi HTTP di risposta (6/7)

- Il blocco intestazione deve essere terminato con una riga bianca che segnala la fine del blocco intestazione;
- Dopo la linea bianca segue il blocco dati (entity body). Esso è il piatto forte del messaggio di richiesta e contiene l'oggetto richiesto (rappresentato schematicamente tramite *data data data* ...).

I messaggi HTTP di risposta (7/7)

- Il server fa uso dell'intestazione MIME Content-type: type/subtype per informare il client a riguardo del del tipo di contenuto.

Pagine statiche e dinamiche (1/4)

- I documenti WWW sono scritti in un particolare linguaggio (HTML, HyperText Markup Language) e sono multimediali e ipertestuali;
- Estensioni del linguaggio:
  - Documenti generati dinamicamente (CGI, Common Gateway Interface);
  - Applets Java;

Pagine statiche e dinamiche (2/2)

- Nel caso di documenti generati dinamicamente il server fa partire un programma e rilancia i dai ricevuti dal client. ILl programma genera in uscite pagine HTML che il server rilancia al client;
- Si parla di scritti CGI o di programmi CGI perché lo scambio d informazioni tra server e applicazione ha luogo tramite l'interfaccia Common Gateway Interface (CGI);

Pagine statiche e dinamiche (3/4)

- Nel caso di applet Java il server scarica sul client un codice (Java) che successivamente viene processato sul client;
- Un altro tipo di pagina sono quelle memorizzate come HTML sul server e contenenti comandi speciali che il server interpreta prima di rilanciarle sul client;

Pagine statiche e dinamiche (4/4)

- Esempi sono Server-side includes, Active Server Pages (ASP) di Microsoft e PHP.
- Si possono in tale maniera realizzare sia funzionalità semplici (ad es. inserire nella pagina una data di ultimo aggiornamento in modo automatico) quanto applicazioni complesse come interrogazioni e aggiornamenti di banche dati.

Caching a livello browser (1/2)

- Per minimizzare lo scambio dati il browser opera il caching (memorizzazione) delle pagine scaricate;
- Per decidere dell'aggiornamento il bowser adopera due tecniche differenti:
  - Il browser conosce la data di scaricamento della pagina (la prima volta) e fa la richiesta al server con l'header If-Modified-Since impostato;

Caching a livello browser (2/2)

  - Il browser adopera l'header „Expires" della pagina scaricata oppure il server puo'far uso dell'intestazione specifica: „Cache-Control";

Autenticazione (1/4)

- Pagine od oggetti specifici possono essere protetti a livello server cosi' che l'utente si deve autenticare prima di poter avere accesso alla pagina;
- La sequenza temporale degli eventi:
- (1) Il cliente richiede un oggetto soggetto a protezione dal server;

Autenticazione (2/4)

- (2) il server risponde con un messaggio avente la linea di stato posta alvalore 401 „Unauthorized“ e tramite le linee di headers specifica il tipo di autenticazione richiesto (p.es. Basic e il Realm cioè la regione ove il server si trova);
- (3) il client ricollega il messaggio di errore alla mancata autorizzazione e presenta la maschera del dialogo di autenticazione;

Autenticazione (3/4)

- (4) l‘utente introduce i dati richiesti e il browser ripete la richiesta di scaricamento della pagina dal server questa volta con l‘header Authorization dando come parametroiltipo di autorizzazione Basic e il nome utente e la parola chiave convertiti incodice base64;

Autenticazione (4/4)

- (4) Se l‘autenticazione ha luogo il server scarica la pagina, altrimenti ripete il messaggio 401 e la sequenza si ripete; dopo un numero predefinitodi tentativi (di solito 3) il browser „rinuncia“ e rappresenta la pagina „Authorization required“.

Hosting di piu' siti su un singolo server (1/4)

- Ogni sito web possiede una identità univoca fatta di:
  - Numero porta;
  - Indirizzo IP;
  - Intestazione host;
- Piu' siti possono essere ospitati su di un medesimo server usando differenti combinazioni di numero porta, indirizzo IP e intestazione host;

Hosting di piu' siti su un singolo server (2/4)

- Numero di porta:
  - Ogni sito web viene configurato con un differente numero di porta (un unico indirizzo IP per tutti i siti);
  - Affinchè il client possa raggiungere il sito Web l'indirizzo IP del sito deve essere completato con il numero di porta;
  - Questa tecnica di hosting è la meno diffusa in ambito produttivo (problematica firewall);

Hosting di piu' siti su un singolo server (3/4)

- Indirizzi IP multipli:
  - Ogni sito web viene configurato con un differente indirizzo IP;
  - In questo caso molteplici indirizzi IP vanno legati alla medesima scheda di rete (o molteplici schede di rete vanno inserite nel server);
  - il client raggiunge il sito Web per il tramite dell'indirizzo IP ad esso corrispondente;

Hosting di piu' siti su un singolo server (4/4)

- Intestazione host:
  - Ciascuno dei siti web viene configurato con un'intestazione host specifica, con un indirizzo IP (eguale per tutti i siti) e con un numero di porta (eguale per tutti i siti);
  - L'intestazione host deve corrispondere alle regole DNS (registrato e risolvibile tramite DNS);
  - Il client raggiunge il sito Web per il tramite di indirizzo IP, numero porta e intestazione host, che è una delle linee di intestazione definite in HTTP 1.1 per il messaggio di richiesta (linea obbligatoria!).

Prestazioni (1/3)

- La disponibilità delle risorse puo' essere limitata per tutti i siti web del server o per ogni singolo sito agendo su:
  - Dati previsione visite giornaliere (ottimizzazione memoria);
  - Limitazione larghezza di banda;
  - Limitazione del processo.

Prestazioni (2/3)

- A livello di configurazione è possibile configurare (limitare):
  - Il numero massimo di connessioni simultanee per il sito;
  - Il tempo di timeout nel caso di connessione inattiva.

Prestazioni (3/3)

- Keep-alive HTTP migliora la prestazione del server IIS mantenendo la connessione con il browser aperta anche dopo iltrasferimento di un oggetto.

Compressione HTTP

- La compressione HTTP permette la piu‘sollecita trasmissione di pagine tra il server ed il client;
- La scelta di effettuare uno scambio compresso di pagine con il client presuppone una precedente accurata analisi del carico del processore.

Registrazione degli accessi (1/2)

- Le opzioni seguenti sono disponibili:
  - Formato file di registrazione comune NCSA (National Center Supercomputing Applications): fomato ASCII fisso;
  - Formato file di registrazione Microsoft IIS: formato ASCII fisso con visibilità piu‘ ampia rispetto a NCSA;

Registrazione degli accessi (2/2)

- Formato file di registrazione W3C (World Wide Web Consortium):
- Registrazione ODBC.

Formato file di registrazione comune NCSA (1/2)

- Il file è costituita da righe con 7 campi;
- I campi sono separati da spazi bianchi;
- Campi che non contengono un valore sono marcati con un trattino „-“;
- I 7 campi sono:

Formato file di registrazione comune NCSA (2/2)

Nome campo	**Descrizione**
Indirizzo IP del client	
Utilizzatore	
Data	Data richiesta
Ora	Ora richiesta
Richiesta	Riga richiesta
Stato	Stato HTTP
Bytes	Numero bytes trasferiti al client

Formato file di registrazione Microsoft IIS (1/3)

- Il file è costituita da righe con 14 campi (una riga per accesso);
- I campi sono separati da spazi bianchi;
- Campi che non contengono un valore sono marcati con un trattino „-“;
- I 14 campi sono:

Formato file di registrazione Microsoft IIS (2/3)

Nome campo	Descrizione
Indirizzo IP del client	
Utilizzatore	Nome autenticato utente
Data	Data transazione
Ora	Ora transazione
Servizio	Nome servizio Web che registra la transazione
Nome computer	Nome del computer che ha eseguito la richiesta
Indirizzo IP del server	Indirizzo IP server web

Formato file di registrazione Microsoft IIS (3/3)

Nome campo	Descrizione
Tempo impiegato	Tempo impiegato per completare la transizione (in ms)
Bytes ricevuti	Numero bytes che il server riceve dal client
Bytes trasmessi	Numerobytes trasmessi al client
Stato HTTP	Codice stato HTTP
Stato Win32	Codice di stato Windows
Nome operazione	Metodo di richiesta HTTP
Obiettivo	File richiesto

Formato files di registrazione esteso W3 (1/4)

- Questo formato è oggetto di configurazione e offre un grande numero di opzioni;
- Oltre alle informazioni legate all'accesso è possibile aggiungere campi con informazioni di processo;
- Il file s'inizia con una "testa" (le righe sono identificate con il simbolo #) contenenti informazioni del server. Seguono poi le righe legate alle richieste di files (una riga per richiesta).

Formato files di registrazione esteso W3 (2/4)

Nome campo	Descrizione
Data	Data transazione
Ora	Ora transazione
Indirizzo IP del client	
Nome utente	
Nome del servizio	Nome servizio Web che registra la transazione
Nome computer	Nome del computer che ha eseguito la richiesta
Servizio	
Indirizzo IP del server	Indirizzo IP server web

Formato files di registrazione esteso W3 (3/4)

Nome campo	Descrizione
Porta del server	Tempo impiegato per completare la transizione (in ms)
Metodo	Metodo HTTP
URI stem	
Richiesta URI	Codice stato HTTP
Stato protocollo	Codice di stato Windows
Stato Win32	Metodo di richiesta HTTP
Bytes trasmessi	Numero bytes trasmessi

Formato files di registrazione esteso W3 (4/4)

Nome campo	Descrizione
Bytes ricevuti	Numero bytes che il server riceve dal client
Tempo preso	Tempo impiegato in ms per soddisfare la richiesta
Versione del protocollo	Numerobytes trasmessi al client
Host	Nome del computere client
User agent	Informazioni sul sw del client
Cookie	Informazioni sui cookies
Riferimento	Sito che ha fornito il collegamento al sito corrente

Formato files di registrazione esteso W3 (5/5)

Nome campo	Descrizione
Tipo di processo	Tipo di processoche ha attivatol'evento
Evento di processo	Evento attivato
Tempo utilizzatore	Tempo processore in modalità utente
Tempo Kernel	Tempo totale in modalità kernel
Errori pagina	Numero errori pagina memoria
Numero processi	Numero applicazioni create
Processi attivi	Nmero di applicazioni regiatrate

Formato files di registrazione esteso W3 (5/5)

Nome campo	Descrizione
Processi terminati	Tipo di processoche ha attivatol'evento

Configurazione documenti predefiniti

- Con questa configurazione vengono gestite le richieste senza il nome del documento (richieste su nome directory oppure /):
  - Se sono disponibili dei documenti predefiniti, IIS restituisce il primo di tali documenti;
  - Se non ci sono documenti predefiniti e la casella „sfoglia la directory“ è abilitata, IIS restituisce un listato della directory;
  - Se i due punti precedenti sono nok IIS resituisce un messaggio di errore 404 .

Configurazione documento piè di pagina

- IL documento piè di pagina è un documento HTML contenente informazioni che si desiderano essere presenti a piè di ogni pagina web (a livello sito, a livello directory)
- Tale documento puo‘ essere configurato per l‘inserimento automatico di ogni pagina restituita dal server (registro Documenti).

Scadenza contenuto

- Con Scadenza contenuto è possibile regolare il comportamento caching del browser;
- Le impostazioni si possono fare a livello di sito, directory, file per il tramite del registro Proprietà con le seguenti opzioni:
  - Scadenza contenuto immediata (no caching);
  - Scadenza contenuto ad un tempo definito;
  - Scadenza contenuto dopo un intervallo di tempo definito.

Personalizzazione intestazione HTTP

- Il server risponde alle richieste del browser con un messaggio di risposta formato da riga di stato, righe di intestazione, blocco dati risposta.
- E‘ possible per scopi specifici personalizzare le righe di intestazione con informazioni ulteriori.
- La sintassi è la consueta: tag, doppio punto,valore tag.

Restrizione contenuto

- IIS supporta la classificazione di contenuti sulla base di criteri sviluppati da Internet Content Rating Association (ICRA);
- La classificazione del contenuto ha luogo per il tramite di un questionario guidato;
- Successivamente il web master puo‘ abilitare le restrizioni sul contenuto ad una categoria di restrizione o disabilitarle.

Servizio Certificati (1/7)

- IIS supporta lo standard SSL 3.0 che permette lo scambio dati protetto tra i browser clients e i server web;
- Nell‘ambito del protocollo SSL i certificati vengono adoperati per la autenticazione del server e del client e, indirettamente, per la trasmissione in forma cifrata della chiave di sessione („avvolta nella chiave pubblica“);

Servizio Certificati (2/7)

- Certificati vengono emessi per attestare il legame tra un sito web e la propria chiave pubblica (in linea con il principio della crittografia a chiave pubblica);
- Tali certificati (conformi allo standard X.509) possono essere generati dalla organizzazione stessa che assume internamente il ruolo di CA o da CA attendibili (vedi la lista nel browser);

Servizio Certificati (3/7)

- Nel caso che l'organizzazione funzioni da CA:
  - Installare Servizio Certificati in un server del dominio e generare il certificato principale (Autocertificazione);
  - Generare i files di richiesta per ogni sito web;
  - Creare i certificati;
  - Installare i certificati e attivare SSL per ogni sito;
  - Installare il certificato principale della CA nell'archivio dell'autorità del browser;

Servizio Certificati (4/7)

- L'installazione di Servizio Certificati pone limitazioni sul server:
  - Cambiamenti di nome non sono ammessi;
  - Cambiamenti nell'appartenenza del dominio non sono ammessi;

Servizio Certificati (5/7)

- La gestione comprende le seguenti attività fondamentali:
  - Accettazione o rifiuto richieste certificati in sospeso;
  - Creazione manuale di certificati;
  - Controllo scadenza e Revoca certificati;
  - Verifica e rinnovo certificato principale;
- La gestione ha luogo tramite uno snap-in dedicato (Autorità di certificazione)

Servizio Certificati (6/7)

- Per ogni sito web sono necessari i passi seguenti:
  - Creare la richiesta di certificato;
  - Inviare la richiesta a Servizio Certificati alla CA esterna (in accordo con un processo formale di registrazione, per posta elettronica o tramite formulario in linea) o alla CA interna (tramite interfaccia web)
  - Gestire la richiesta in sospeso e installare il certificato;
  - Verifica SSL (attivazione, configurazione);

Servizio Certificati (7/7)

- L'utilizzo di SSL presuppone i passi seguenti:
  - Configurazione porta SSL;
  - Import del Certificato Principale del sito nel browser (Archivio di Aurorità);
  - Verifica della correttezza del protocollo SSL scaricando pagine e chiamandone le proprietà;

Encrypting File System (EFS) (1/3)

- All‘interno di partizioni disco NTFS è possibile cifrare cartelle e files in modo che solo la persona che ha cifrato il documento possa successivamente decifrarlo e accedere ad esso come testo chiaro;
- La cifratura ha luogo con metodo ibrido: il testo viene cifrato tramite un algoritmo a chiave simmetrica e la chiave adoperata per la cifratura (chiave di sessione) viene a sua volta cifrata con la chiave pubblica di chi ha chiesto la cifratura del documento;

Encrypting File System (2/3)

- Per la cifratura è necessario un certificato che ha l‘attributo di certificato EFS; esso può essere richiesto a Servizio Certificati dell‘organizzazione interna;
- Per motivi di sicurezza amministrativa la chiave di sessione viene cifrata e memorizzata una seconda volta adoperando la chiave pubblica di un EFS Recovery Agent (Amministratore di rete);

Encrypting File System (3/3)

- Nel caso che Servizio Certificati non sia attivato le chiavi e il certificato vengono generati automaticamente da EFS;
- Analogamente viene creato d‘autorità il certificato per il Recovery Agent, che è l‘amministratore locale oppure l‘amministratore di dominio del primo controller di dominio configurato.