

# **Gestione di un server web**

A cura del prof. Gennaro Cavazza

# Come funziona un server web

Un server web è un servizio (e quindi un'applicazione) in esecuzione su un computer host (server) in attesa di connessioni per fornire una serie di informazioni codificate secondo uno specifico protocollo o linguaggio. In pratica un server web permette ad un client (il vostro browser: Internet Explorer, Firefox, Safari, Opera o altro) di collegarsi mediante la porta 80 (specifica del protocollo TCP/IP) e di richiedere informazioni secondo un determinato protocollo. Il server Web, alla richiesta, fornisce le informazioni codificate mediante un determinato linguaggio (HTML, XML, XHTML).

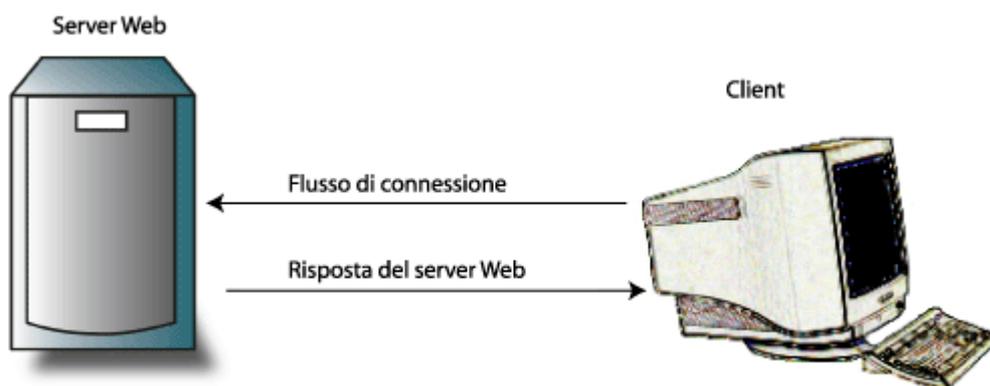


Figura 1. Connessione server-client nel flusso HTTP

Questa guida ha l'intenzione di descrivere nel particolare la configurazione del server web di Microsoft: Internet Information Services (IIS) versione 6.0. Questa applicazione fa parte del sistema operativo Microsoft Windows 2003 Server e si trova sul Cd di installazione del sistema operativo. La guida tratterà la configurazione del server Web, del server Ftp e del server di posta elettronica. Molte immagini guideranno l'utente nella perfetta messa a punto del sistema.

# Installazione di Microsoft IIS 6

La versione di IIS progettata per essere eseguita su un sistema operativo host specifico **non può** essere installata su nessun altro sistema operativo. IIS non è indipendente dal sistema operativo. Ad esempio, IIS 6 non può essere installato su Windows 2000 (versione precedente a Windows 2003) e IIS 5 non può essere installato su Windows NT 4 (versione precedente a Windows 2000), e la versione 6 non può essere installata su Windows XP. Questa limitazione è dovuta alla strettissima integrazione fra IIS e il sistema operativo specifico.

Analizziamo ora i passi necessari per installare IIS 6 su Windows 2003 Server.

Per prima cosa, ipotizzando di aver già il sistema operativo Windows 2003 installato, inseriamo il cd di installazione di Windows 2003 Server.

Per procedere con l'installazione selezionare il menu *Start* e quindi *Pannello di controllo*. Quindi selezionare *Installazione Applicazioni*, successivamente *Installazione componenti di Windows*. Quindi si seleziona *Server Applicazioni* e successivamente *Internet Information Services (IIS)*.

Vengono visualizzate una serie di righe ciascuna con la possibilità di essere aggiunta o eliminata dall'installazione mediante il relativo segno di spunta. Andiamo ad analizzare ogni singola voce, quelle necessarie o comunque molto utili hanno un asterisco all'inizio:

1. **Estensioni del server Bits:** Permette il controllo della larghezza di banda sul trasferimento di file.
2. **Estensioni del server di frontpage 2002:** permette di installare l'insieme delle funzionalità aggiuntive relative alle estensioni di Front page (utile solo se si usa frontpage come editor di pagine web).
3. \* **File comuni:** l'insieme di tutti i file necessari al corretto funzionamento del server web, senza questa opzione il servizio non può funzionare.
4. \* **Servizio FTP (File Transfer Protocol):** applicazione per la condivisione dei documenti e contenuti secondo lo specifico protocollo FTP.
5. \* **Servizio SMTP (Simple Mail Transfer Protocol):** sistema di gestione della messaggistica, invio dei messaggi di posta elettronica.
6. **Servizio NNTP(News Network Transfer Protocol):** sistema di gestione delle news (usenet news su internet).
7. \* **Servizio Web:** è a sua volta suddiviso in:
  - o \* **Active Server Pages:** l'opzione installa tutte le funzionalità necessarie all'esecuzione dei file ".asp" normalmente disabilitata.
  - o **Internet Data Connector:** permette la connessione tra il sito web e il database (sistema ormai obsoleto).
  - o **Remote Administration (HTML):** Installando questa opzione si abilita la possibilità di amministrare remotamente il server web con un browser, rispetto alle precedenti versioni è possibile amministrare anche server diversi da quello in cui è installata l'estensione.
  - o **Remote Desktop Web Connection:** l'opzione, se abilitata, installa il controllo ActiveX che permette ad internet Explorer di connettersi al computer via terminal server, usando una pagina web.
  - o \* **Server Side Includes:** questa funzionalità abilita la possibilità di inserire script server side nelle pagine di codice.
  - o **WebDAV Publishing:** questa opzione abilita la possibilità di usare lo standard WebDAV (Distributed Authoring and Versioning) per pubblicare i documenti.
  - o \* **Servizio Web:** insieme delle funzionalità base per il protocollo HTTP.

8. \* **Gestione Internet Information Server:** installa il componente che permette di gestire il server web dalla Microsoft Management Console (MMC).
9. **Stampa Internet:** questa funzione permette di condividere le stampanti mediante il protocollo http.

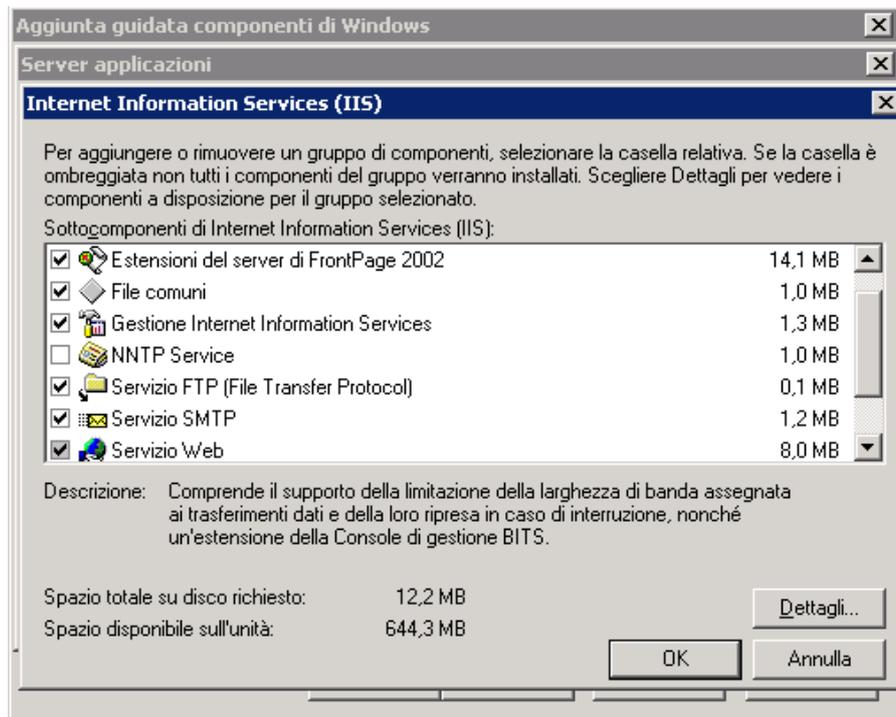


Figura 2. Terza finestra di installazione (si apre cliccando su Internet Information Server)

Una volta selezionate le voci di interesse (un esempio è dato dalle figure sopra) si procede all'installazione. È importante ricordare che eventualmente in ogni momento, seguendo la procedura indicata, possono essere rimossi o aggiunti alcuni componenti. Ad esempio il server SMTP può essere aggiunto in un secondo tempo selezionando l'apposita casellina (checkbox).

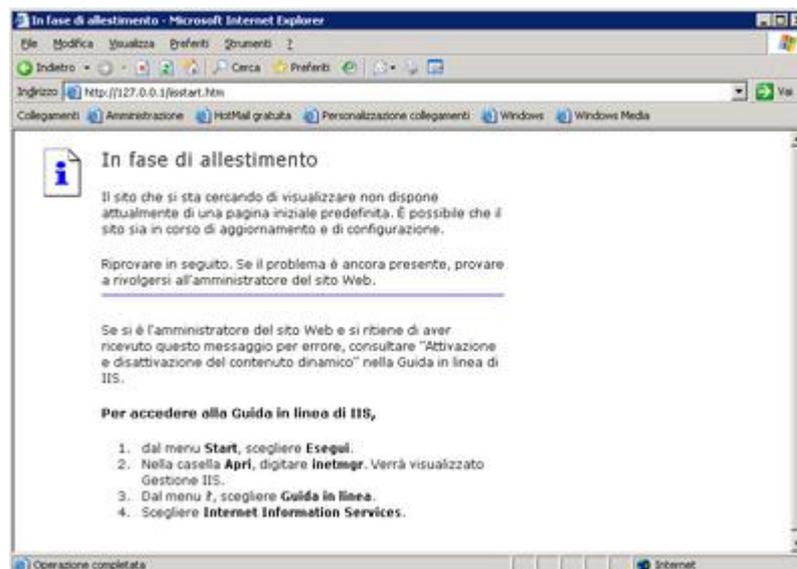


Figura 3. Risultato della chiamata http://localhost

Una volta completata l'installazione il server Web è funzionante e può essere provato digitando <http://127.0.0.1> oppure <http://localhost> all'interno del browser. Il risultato è mostrato in Figura 3. Durante l'installazione sono state create delle cartelle nel filesystem del computer, vedremo adesso quali sono.

## Le cartelle e gli strumenti di amministrazione

### La cartella *Inetpub*

Normalmente viene creata una cartella del tipo "c:\inetpub" che al suo interno contiene quello che è l'insieme delle cartelle per far funzionare il sito principale e il server SMTP. Nulla vieta che una volta installato si possa cambiare tutte queste impostazioni. All'interno di inetpub troverete anche altre cartelle, ognuna definita da alcune funzioni specifiche, così come descritto di seguito.

- **adminscripts** – cartella dove sono contenuti gli script per eseguire alcune funzionalità di amministrazione come creare siti web o directory virtuali.
- **ftproot** – cartella base per il sito ftp creato durante l'installazione (buona norma disattivarlo nel caso in cui non servisse)
- **mailroot** – cartella contenente altre sottodirectory per il corretto funzionamento del server SMTP predefinito.
- **nntpfile** – cartella per il corretto funzionamento del server NNTP.
- **wwwroot** – cartella in cui si trovano i file e le sottodirectory per il corretto funzionamento del *Default Web Site*

### Utilizzo degli strumenti di configurazione

Per poter gestire i siti web e tutte le altre funzionalità fornite con IIS 6.0 si usa la MMC (Microsoft Management Console), un framework che permette di controllare un insieme non omogeneo di funzionalità, ad esempio IIS 6.0, SQL Server 2000, Windows services, e quasi tutte le funzioni Amministrative di windows mediante degli add-on che sono chiamati snap-in. In ogni caso l'interfaccia di amministrazione di IIS 6.0 lo ritrova all'interno del menu; *Programmi /Strumenti di amministrazione / Internet Information Services*.

Una volta aperta la console si visualizza un albero come quello mostrato in Figura 4.

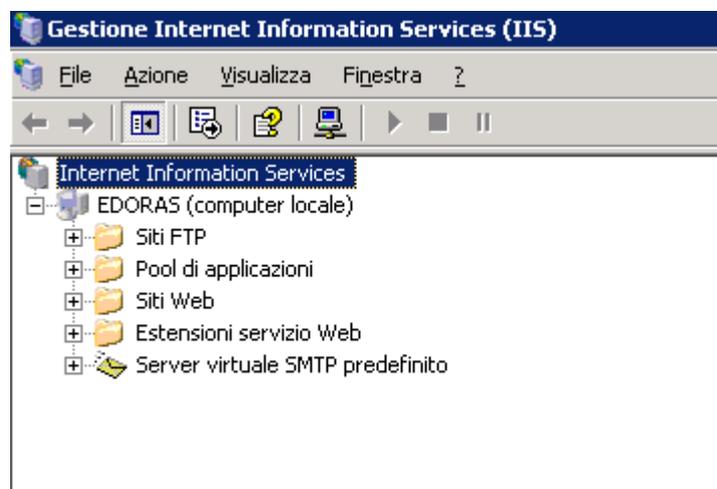


Figura 4. Interfaccia della MMC relativa a IIS

Nella colonna di sinistra possiamo trovare un'icona che rappresenta il server dove è installato il servizio web, il nome indica il nome della macchina ospite (host). Cliccando sul "più" (+) accanto al nome si aprono alcune nuove voci relative alle funzionalità installate, ad esempio siti FTP, Pool di applicazioni, siti Web, Estensioni servizio Web, Server virtuale SMTP predefinito.

Analizziamo ora i vari sottoservizi di IIS 6.0, da questa guida è esclusa la descrizione del pool di applicazioni e del server NNTP. Il pool di applicazioni serve a configurare i diversi comportamenti delle applicazioni (Aspe Asp.net) all'interno dei singoli siti e richiede conoscenze di programmazione e debugging che esulano da questa guida. Il server NNTP serve invece a creare un'applicazione in grado di gestire una usenet news (una Rete di collegamento ad Internet, per l'interscambio di "conferenze" di messaggi (newsgroup)). Partiamo, come è naturale, dal server di gestione dei siti Web.

# Creazione di un nuovo sito web

Le prime lezioni della nostra guida sono dedicate alla creazione e alla configurazione di un server Web, ossia del servizio che è in grado di ospitare pagine Web e ci rispondere alle richieste del browser. Più avanti nella guida ci soffermeremo sulla configurazione di un servizio Ftp e Sntp. Tutte le impostazioni si riferiscono e vanno eseguite dalla citata Microsoft Management Console, ossia l'interfaccia di configurazione di tutti i servizi di IIS.

Per creare un nuovo sito Web è necessario cliccare con il tasto destro del mouse sull'apposita cartellina, in questo caso **Siti Web**, e scegliere *Nuovo*, una volta che si è aperta una nuova finestra fate clic su *Avanti*.

Si apre una finestra dove è necessario indicare il nome del sito. È solo una descrizione e non influisce sulle proprietà o impostazioni del sito. Successivamente è necessario inserire l'indirizzo internet (IP) del computer da associare al sito e la porta, normalmente 80; è possibile inoltre specificare il nome internet da associare al sito quando si utilizza la funzionalità di virtual hosting. Successivamente, premendo *Avanti*, viene richiesto il percorso sul disco dove verrà montata la directory del sito Web, e se si vuole l'accesso anonimo al sito. Successivamente viene richiesto quali permessi associare alla directory del sito:

- **lettura:** i file sono leggibili via web.
- **esecuzione:** possono essere eseguiti file eseguibili tipo .exe, .com, cgi e così via
- **esecuzione script:** possono essere eseguiti script asp
- **scrittura:** è possibile scrivere all'interno del sito
- **esplorazione:** è possibile vedere le cartelle e il loro contenuto

Infine viene chiesto quale deve essere la tipologia di accesso, cioè se deve essere solo possibile scrivere o leggere o entrambe (Figura 5).

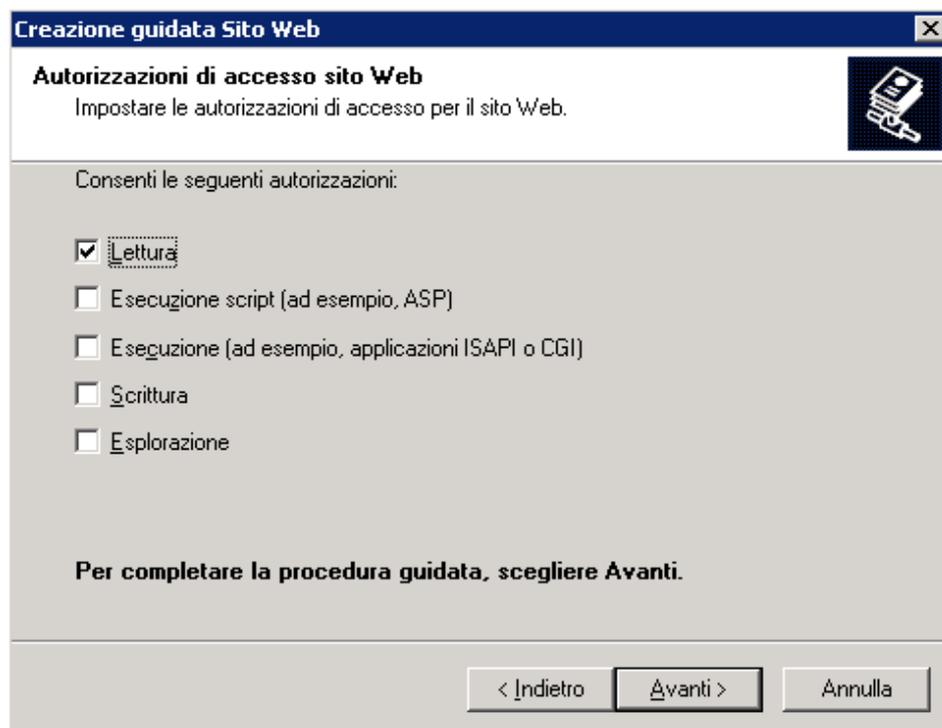


Figura 5. Creazione sito web

# Configurazione generale e prestazioni

Una volta creato il sito, andiamo ad analizzare le configurazioni che possono essere cambiate una volta completata la procedura di creazione e che riguardano sia i parametri che abbiamo inserito durante la creazione del sito sia altre funzionalità. Faremo una breve analisi di **tutte le proprietà** soffermandoci su quelle più utili e tralasciando o brevemente descrivendo quelle più complesse o, per l'obiettivo di questo corso, non necessarie. Poiché la configurazione di un server Web è complessa, abbiamo diviso in quattro diverse lezioni le descrizioni dei parametri.

Premendo con il tasto destro del mouse sul nome del sito e scegliendo *Proprietà* si apre una finestra con alcune schede. Ogni scheda sarà trattata specificando i singoli valori configurabili, gli asterischi presenti all'inizio del nome della proprietà indicano caratteristiche complesse o che richiederebbero un approfondimento maggiore, che esula da questa guida e che sarà trattato in seguito.

1. **Sito Web:** permette di definire e modificare le impostazioni principali del sito.
  - **Descrizione:** è il nome usato per definire il sito nell'albero dei siti web.
  - **Indirizzo IP:** è l'indirizzo associato al server per rispondere alle richieste http. Il pulsante avanzate permette di aggiungere il nome DNS del sito, per abilitare la funzionalità virtual host, in cui più siti rispondono sulla stessa porta e stesso indirizzo, usando come discriminante il nome dns del sito (es. www.html.it).
  - **Porta TCP, porta SSL:** rappresentano rispettivamente il numero della porta per le richieste http e le richieste https.
  - **Timeout connessione:** permette di definire il tempo dopo il quale, senza nessuna richiesta da parte del client, il server interrompe la connessione. In genere il browser invia dei pacchetti "HTTP keep-alive" in modo da mantenere attiva la connessione. Infatti alla conclusione delle operazioni il client chiude la connessione, ma in caso contrario resterebbe aperta indefinitamente, invece con il timeout, il server, trascorso il tempo, chiude comunque la connessione.
  - **Abilita HTTP keep-alive:** permette di accettare i pacchetti keep alive per tenere aperta la connessione. Senza abilitare questa funzione le prestazioni potrebbero degradare.
  - **Consenti registrazione attività:** permette di abilitare il logging delle richieste, sia per fini di debug sia per finalità di statistiche di accesso. I file possono essere salvati sia in formato testo (W3C Extended Log File) sia in formato database. È inoltre possibile specificare la posizione dove inserire i file di log.

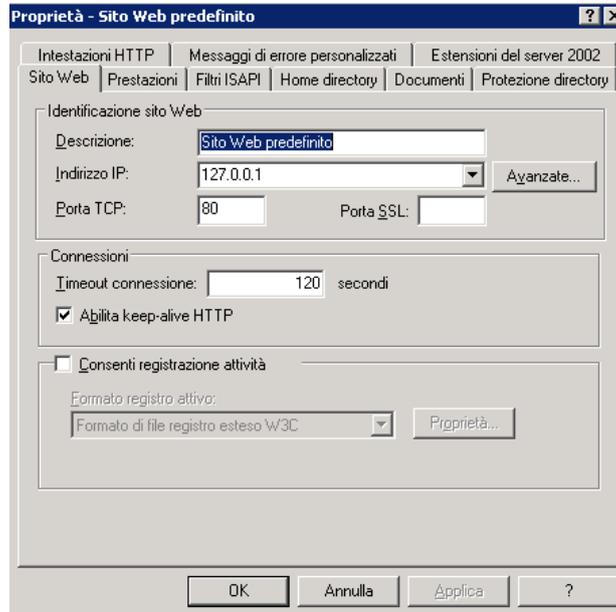


Figura 6. Sito web

2. **Prestazioni:** questa scheda permette di limitare le risorse che il sito può utilizzare.
- **Limitazioni della larghezza di banda:** è possibile definire una larghezza di banda massima che il sito può utilizzare.
  - **Numero di connessioni:** permette di definire il numero massimo di connessioni che il server è in grado di servire contemporaneamente.

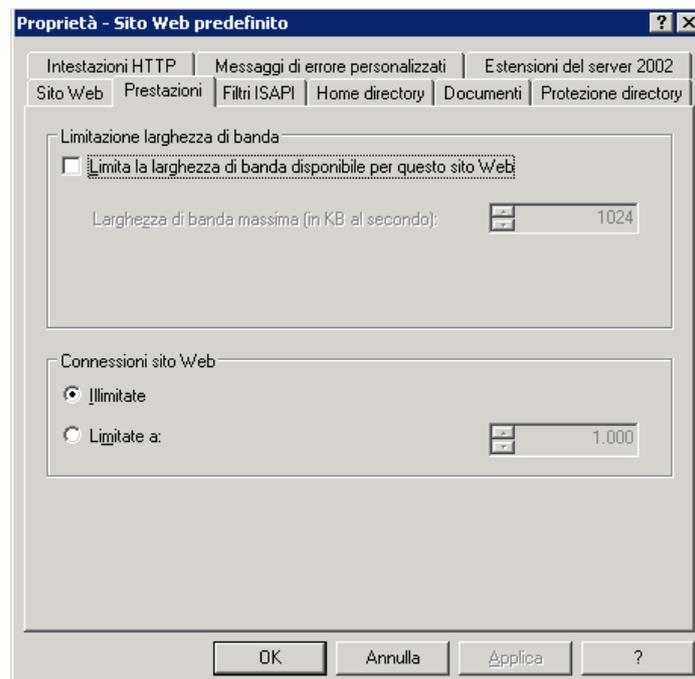


Figura 7. Scheda prestazioni

3. **\*Filtri Isapi:** permette di aggiungere dei filtri al server che serviranno per la gestione di particolari tipologie di connessioni. È una funzionalità avanzata e richiede la conoscenza intrinseca della struttura del server IIS 6.

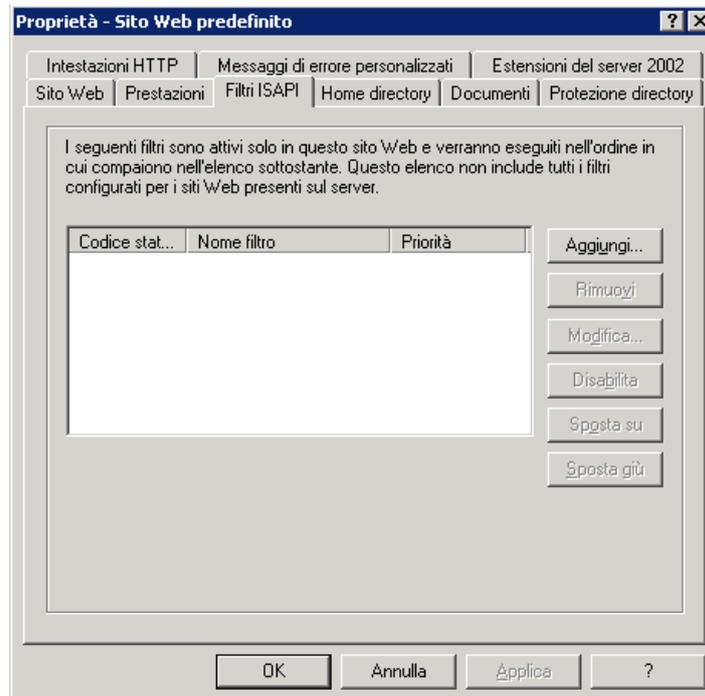


Figura 8. Scheda filtri Isapi

# La Home Directory e i documenti

Continuiamo la descrizione delle proprietà di un sito Web descrivendo le due schede Home Directory e Documenti.

## Home Directory

Questa scheda permette di definire le proprietà relative alla cartella dove risiede al sito web.

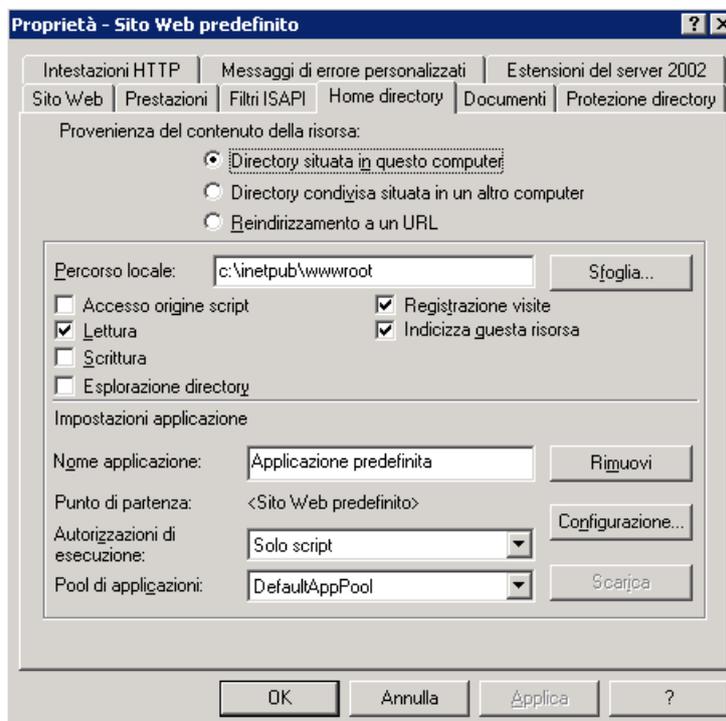


Figura 9. Scheda home directory

- **Provenienza del contenuto della risorsa:** si può specificare il percorso della cartella che conterrà i file del sito web. È anche possibile specificare un indirizzo verso cui redirigere il sito.
- **Permessi:** è possibile specificare il tipo di accesso:
  1. Scrittura, lettura: è possibile scrivere (mediante put HTTP 1.1) o leggere sulla cartella.
  2. Possibilità di eseguire script: è possibile eseguire script asp.
  3. esplorazione directory: permette di vedere il contenuto della cartella come nel filesystem.
  4. Registrazione visite: permette di eseguire la registrazione nel file di log.
  5. Indicizza questa risorsa: permette ad Index Server di Microsoft di indicizzare il contenuto.
- **Nome applicazione:** è il nome associato all'applicazione. Il tasto rimuovi serve a cancellare l'applicazione, mentre il tasto scarica serve a scaricare dalla memoria l'applicazione, che verrà automaticamente ricaricata.
- **Autorizzazione di esecuzione:** ci sono tre possibilità:
  1. nessuna: non possono essere eseguiti script
  2. solo script: possono essere eseguiti solo script asp.
  3. script ed eseguibili: possono essere eseguiti sia eseguibili che script

- **\*Pool di applicazioni:** permette di scegliere che pool di applicazioni deve essere associato all'applicazione in questione. Il pool può essere controllato nella MMC, nell'apposito insieme (non descritto in questa guida). Con il pulsante configurazione si aprono una serie di nuove schede:
  1. **\*Mapping:** permette di associare un'estensione (es. .asp) di file con un file eseguibile o una dll isapi, permettendo che quest'ultima sia salvata nella cache in modo che una volta chiamata le prestazioni del server web non ne siano intaccate. È possibile nella casella nella parte sotto della finestra definire delle applicazioni (dll isapi o file eseguibili) che vengano associate ad ogni estensione
  2. **\*Option:** permette di definire il tempo per il quale permane una sessione in stato sospeso prima di essere chiusa, permette di definire se i dati devono essere scritti nel browser in maniera sequenziale, oppure se aspettare di completare tutto il contenuto e poi inviarlo al client. Abilita percorso principali permette di utilizzare la notazione “../” per accedere da una cartella a quella di un livello superiore, se disabilitato è necessario indicare tutti i percorsi partendo dalla root. Abilita assembly side-by-side permette di decidere la versione dell'applicazione dll che viene eseguita, mediante un file manifest (tipo xml).
  3. **\*Debug:** permette di gestire l'output relativo al debug. Il server-side debug e il client-side debug, permette di effettuare il debug mediante il Microsoft Script Debugger. Mentre “messaggi di errore per gli script” serve a definire se visualizzare dei dati specifici di errore di uno script o pure personalizzati.

## **Documenti**

Questa scheda permette di specificare il nome del documento che deve essere aperto quando l'utente digita solo l'url del sito ad esempio <http://www.kadathinformatica.it> anzichè <http://www.kadathinformatica.it/index.php>. È possibile indicare più nome per i documenti predefiniti, il sistema andrà nell'ordine indicato dal più in alto al più in basso, fino a che non trova nella cartella del sito un file con quel nome. Se non dovesse trovarne neanche uno possono succedere due cose a seconda se è stato abilitato il browsing delle cartelle o no: nel primo caso verrà visualizzato il contenuto del sito come se fosse una cartella del computer, nel secondo caso viene generato un errore del tipo: “Impossibile elencare il contenuto della directory”. È inoltre possibile abilitare un pie' di pagina, cioè un blocco html da aggiungere ad ogni pagina del sito. Questa porzione di codice verrà inserita nella parte bassa di tutte le pagine generate dal web server relativamente al sito in questione.

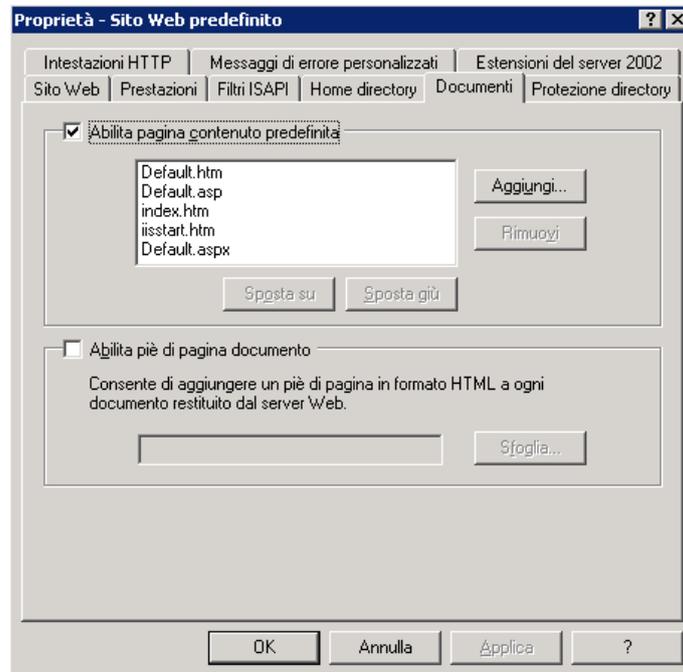


Figura 10. Scheda scelta documenti predefiniti

## Protezione delle directory

**Protezione directory:** in questa scheda vengono definite tutte le politiche di sicurezza che devono essere abilitate per rendere più o meno sicuro l'accesso al sito. Sono presenti tre diverse opzioni.

### **Controllo autenticazione accesso**

È possibile specificare l'utente del sistema che deve impersonificare l'utente anonimo che naviga nel sito per poter definire i permessi di accesso alle risorse del sistema.

Ad esempio: supponiamo che si voglia dare la possibilità ad un utente web di uploadare mediante un'applicazione Asp dei file nella cartella "docs" del nostro sito. In modo predefinito l'utente Web (che d'ora in poi chiameremo anonimo) ha accesso solo in lettura alle cartelle ed ai file del nostro sito, per questo motivo è necessario dargli la possibilità di scrivere all'interno della cartella "docs". Per far questo abilitiamo nelle proprietà della cartella "docs" la possibilità che l'**utente anonimo** possa scrivere. Ma qual'è l'utente di sistema che impersonifica l'utente anonimo? La risposta la troviamo nella scheda *Controllo autenticazione accesso*. Anche in questo caso in modalità predefinita l'utente è "IUSR\_NOMECOMPUTER". Nulla vieta che se ne abbiamo motivo possiamo cambiare questo utente, da quel momento l'utente anonimo sarà impersonificato per l'accesso alle risorse del computer dal nuovo utente del sistema che abbiamo inserito.

Se noi dovessimo rimuovere la spunta dalla casella *Abilita accesso anonimo* per accedere al sito sarà necessario autenticarsi, e utilizzare un utente del computer o del dominio. In questo caso il **tipo di autenticazione** è definito dalla seconda serie di opzioni della scheda, dove è possibile definire se si desidera abilitare l'autenticazione integrata di Windows, autenticazione del digest per il dominio Windows, autenticazione di base (la più usata), autenticazione .NET passport. Queste opzioni saranno descritte più avanti nella guida.

Nelle ultime due caselle è possibile specificare un **dominio windows** in cui eseguire l'autenticazione, in modalità predefinita viene ricercato nel dominio della macchina stessa (nome del computer, cioè utente locale), nella seconda casella può essere indicata l'area di autenticazione, cioè il testo che viene visualizzato sulla finestra di login del browser.

## Limitazione sugli indirizzi ip e sui nomi a dominio

Questo tipo di sistema di sicurezza permette di bloccare degli IP o dei domini che accedono al sito. Si può scegliere l'impostazione predefinita e le scelte sono due: consentito o negato.

Se per impostazione predefinita l'accesso è **consentito** significa che tutti i computer possono accedere al sito eccetto quelli indicati nel box sottostante. Se invece come impostazione predefinita è indicato **negato** significa che l'accesso è negato a tutti i computer eccetto quelli indicati nel box sottostante. Quando si vuole aggiungere un nuovo elemento che possa accedere o a cui sia negato si clicca sul pulsante *Aggiungi* e si sceglie se si vuole specificare un singolo indirizzo IP, oppure una classe indicando quindi anche la sottomaschera di rete, oppure un dominio internet. In quest'ultimo caso, come viene specificato con un alert dal sistema, è necessario eseguire un reverse lookup sul dns, e questa è un'operazione molto costosa in termini di performance.

La scheda relativa alle comunicazioni protette o certificati digitali viene trattata specificatamente nel capitolo della guida dedicato alla sicurezza.

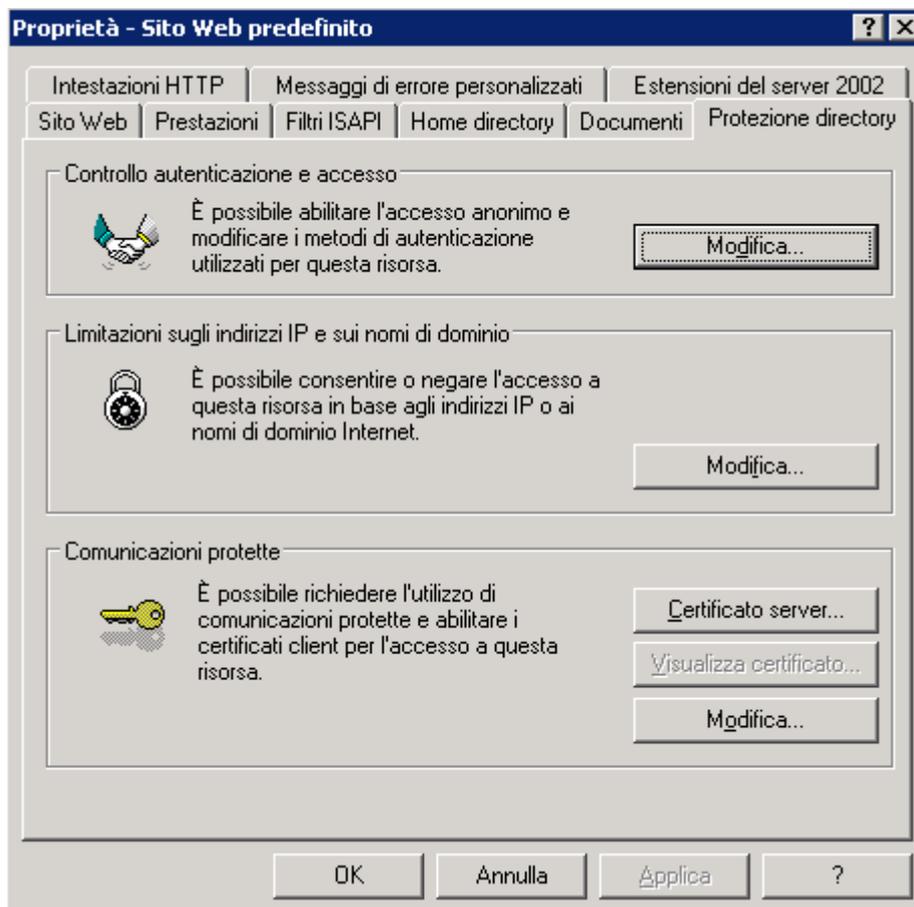


Figura 11. Scheda protezione directory

# Messaggi di errore e intestazioni Http

## Messaggi di errore personalizzati

Questa scheda permette di specificare se utilizzare i file HTML predefiniti per gli errori oppure utilizzarne di personalizzati. Per prima cosa è necessario selezionare il numero di errore, quindi indicare il file HTML che si vuole usare. Ad esempio vogliamo personalizzare l'errore 404, pagina non trovata, selezioniamo il numero 404 e indichiamo al server la pagina HTML che deve essere visualizzata ogni volta che viene individuato tale errore.

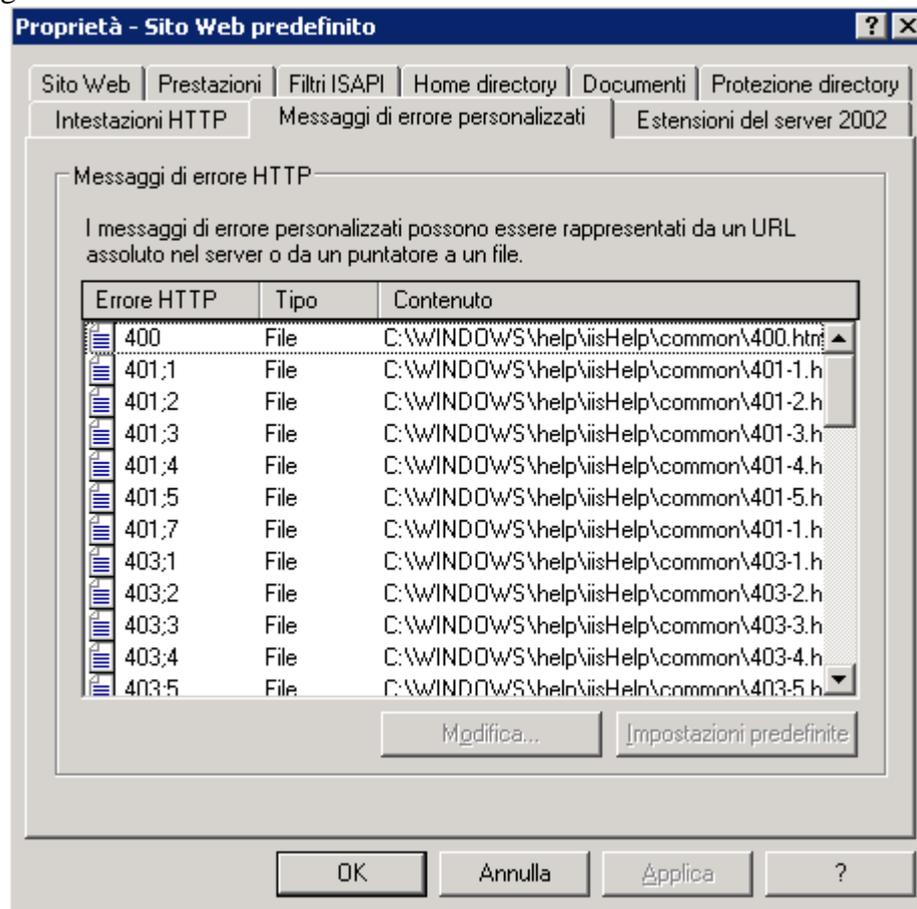


Figura 12. Messaggi di errore personalizzati

## Intestazioni HTTP

La scheda Intestazioni HTTP permette di definire la cache delle pagine, il tipo di contenuto, le intestazioni e il rating di una pagina del sito. Vediamo le opzioni.

- Abilita scadenza contenuto: è possibile indicare la durata in cache della pagina, le opzioni sono tre:
  1. immediata: la pagina viene letta ogni volta e mostrata al browser senza tenerla in cache.
  2. dopo: la pagina rimarrà in cache per il tempo indicato.
  3. scadenza: si definisce una data fino alla quale la pagina verrà tenuta nella cache del server web.
- Intestazioni HTTP personalizzate: permette di inviare al client determinate intestazioni, tipo X-Powered, o altre personalizzate. Per usi comuni non hanno interesse.

- Classificazioni del contenuto (rating): permette di indicare mediante le definizioni standard internet il tipo di contenuto del sito.
- Tipi MIME: se IIS 6.0 deve caricare un file con un'estensione sconosciuta non esegue l'operazione, perciò è necessario specificare un'estensione nei tipi mime affinché possa venire inviata al browser.

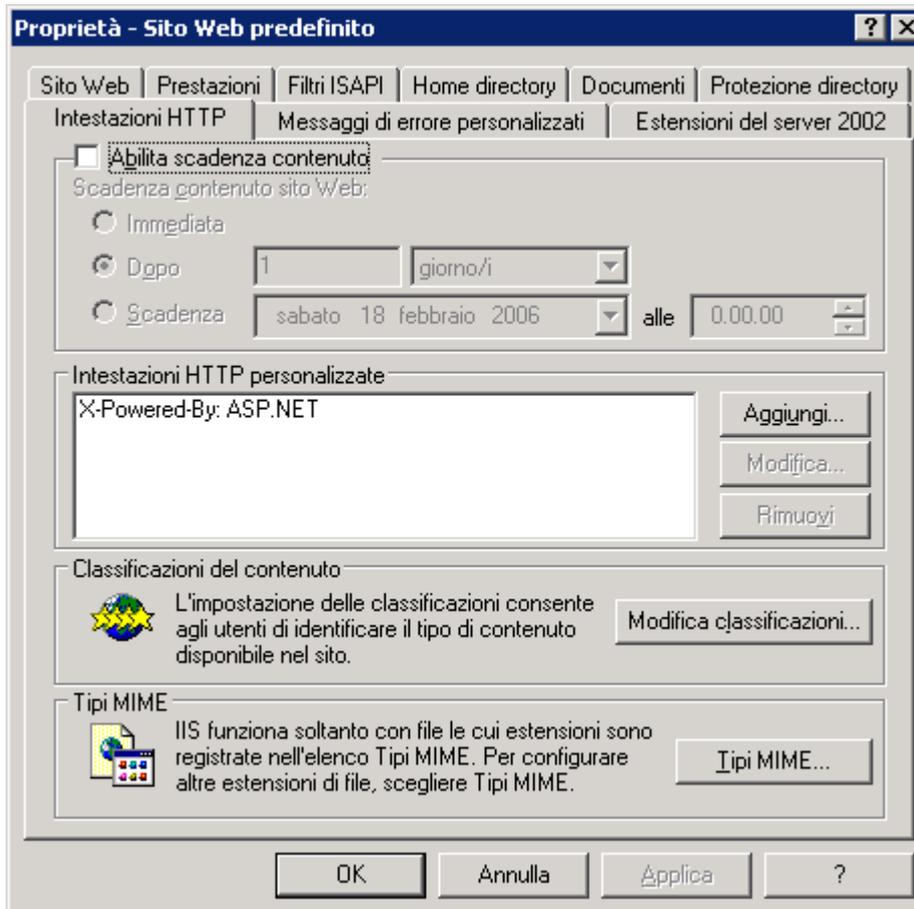


Figura 13. Intestazioni HTTP

Una volta configurato il nostro server web, possiamo decidere di associare al sito cartelle che però sono distribuite nel filesystem e non si trovano all'interno della cartella principale utilizzando le directory virtuali, argomento della prossima lezione.

# Creazione di una directory virtuale

All'interno di ogni sito web si trovano le cartelle fisiche, cioè presenti nella cartella principale del percorso fisico. Ma sarebbe possibile creare un collegamento ad una cartella che fisicamente risiede in un'altra parte del disco e con permessi diversi? La risposta è sì, e queste cartelle collegate si chiamano directory virtuali, proprio perchè sono dei collegamenti e non si trovano fisicamente all'interno del percorso del sito web.

Per creare una cartella virtuale è necessario cliccare con il tasto destro sul sito all'interno del quale la cartella deve essere creata, e selezionare *Nuovo* e quindi *Cartella virtuale*. Quindi si apre una finestra che chiede all'utente di indicare l'alias ossia il nome che la cartella avrà all'interno del sito web e che non necessariamente deve coincidere con il nome fisico. Successivamente è necessario selezionare la collocazione della cartella reale che verrà collegata all'alias. Infine si selezionano i permessi che devono essere associati alla cartella:

- **Lettura:** è possibile leggerne il contenuto
- **Esecuzione Script:** se possono essere eseguiti file .asp
- **Esecuzione cgi:** se possono essere eseguiti file eseguibili, perl, o altro
- **Scrittura:** è possibile scrivere all'interno della cartella
- **Esplorazione:** possono essere visualizzati i contenuti della cartella

In ogni cartella reale o virtuale può essere creata un'applicazione che la rende quindi indipendente dalla configurazione dell'applicazione del sito principale premendo *Crea applicazione* nella scheda *Home directory*.

Ora che tutte le configurazioni per far funzionare il sito web sono state fatte, passiamo a capire come funzionano i sistemi di sicurezza e di impersonificazione del server web IIS 6.0.

## I sistemi di autenticazione base

La sicurezza è uno delle evoluzioni e miglioramenti che Microsoft ha compiuto nel passaggio dalla versione 5 alla 6 di IIS. Uno dei rischi più grossi cui si andava incontro nella versione 5 era relativo alle falle che davano accesso al sistema. Analizziamo ora quali sono in dettaglio i sistemi di autenticazione che IIS 6.0 supporta per l'accesso alle risorse da parte dei navigatori web.

L'autenticazione in IIS 6.0 avviene mediante uno dei metodi sotto indicati:

- Autenticazione anonima
- Autenticazione base
- Digest e Advanced Digest authentication
- Integrated Windows authentication
- .NET Passport authentication

### ***Autenticazione Anonima***

Il server utilizza un utente del sistema per impersonare il navigatore web non autenticato quando vengono richieste risorse al sistema. L'utente predefinito è "iusr\_nomemacchina" (ad esempio se il server Windows si chiama GANDALF il nome dell'utente predefinito che il server utilizzerà per impersonificare un utente che naviga su un sito di IIS 6.0 senza nessun tipo di autenticazione sarà "iusr\_gandalf"). Questa è la situazione più diffusa, quando cioè non compaiono le finestre del browser che richiedono di autenticarsi.

I vantaggi di un tale sistema di autenticazione è che ogni risorsa è accessibile per chiunque, questo è anche uno svantaggio, in quanto non è possibile bloccare l'accesso a determinate risorse.

Ciascuna di queste autenticazioni è presente nell'apposita scheda (vista precedentemente) "Protezione directory".

### ***Autenticazione base***

Con questa autenticazione si obbliga il sito ad accettare solo utenti che possiedono le credenziali corrette.

Quando compare sul browser la finestra di sistema (è importante perché certi siti malintenzionati potrebbero clonare una finestra simile) che chiede nome utente e password, l'utente inserirà le proprie credenziali e il server web utilizzerà tali credenziali di sistema per concedere o negare risorse (quindi pagine web) alla sessione web in corso.

Un grande vantaggio è che tutti i browser la supportano, inoltre è possibile direttamente proteggere alcune risorse. Lo svantaggio è che le password passano in chiaro (codificate in base 64) e possono essere lette da chiunque.

# I sistemi di autenticazione avanzata

## ***Digest e Advanced Digest authentication***

Questo sistema di autenticazione richiede la presenza di Active Directory e funziona nel seguente modo:

1. Il server invia al browser (protocollo http 1.1) la richiesta di credenziali mediante MD5 inviando un apposito hash
2. Il client invia al server la password e username codificata in MD5 mediante la hash inviata dal server
3. Il server controlla mediante un domain controller che i dati siano corretti

La differenza tra Digest e Advanced Digest è che nel secondo metodo la password nel DC (Domain Controller) è già codificata in MD5 e non è inviata come testo in chiaro. Questo comporta naturalmente un maggiore livello di sicurezza.

## ***Integrated Windows authentication***

Esistono due metodi di autenticazione integrata in Windows e sono **Kerberos** (open source) oppure **NTLM** (proprietario di Microsoft). In entrambi i metodi i dati sono passati in forma criptata mediante hash della password ed il controllo avviene su un DC, necessario perciò l'indicazione del dominio di riferimento. Kerberos è un po più complesso e anche sicuro perchè l'autenticità di server e client viene fatta mediante un terzo server, il Key Distribution Center (KDC), il quale rilascia un TGT (Ticket granting ticket) a ciascun utente che lo può usare per accedere alle risorse.

## ***.NET Passport authentication***

Permette di utilizzare il sistema .Net Passport per l'autenticazione dell'utente. Richiede la preregistrazione e la sottoposizione del sito all'approvazione di Microsoft, le richieste dalle proprie pagine devono seguire le specifiche indicate nel [Passport SDK](#). Una trattazione più dettagliata di questo metodo esula dagli obiettivi di questo articolo.

Questi ultimi 3 sistemi sono molto sicuri, anche se richiedono una configurazione anche di infrastrutture, molto più complessa. In pratica la scelta di quale sistema adottare si deve basare sulle richieste di sicurezza, sulla complessità di implementazione, sulle risorse a cui si vuole accedere.

# Gestione dei certificati digitali

I certificati digitali sono uno dei sistemi più sicuri per effettuare comunicazioni protette attraverso internet. IIS 6.0 supporta nativamente, come anche IIS 5.0, la protezione certificata. Non sono impersonificazioni come quelle precedenti, ma sono veri e propri **canali sicuri** in cui possiamo poi stabilire una connessione non sicura. Ad esempio se utilizziamo il certificato digitale e usiamo l'autenticazione base (non criptata quindi) nessuno sarà comunque in grado di leggere le informazioni perchè sarà criptato tutto il flusso di dati, dal client al server e viceversa.

Il funzionamento avviene utilizzando delle **chiavi** con cui il client e il server cifrano le informazioni che si inviano. È come se venisse costruito un tunnel tra il client e il server e tutte le informazioni passano all'interno di questo tunnel. In questo modo anche se usiamo un'autenticazione di base con password in chiaro essa, nel momento in cui viene inviata al server, è criptata mediante la chiave del server e solo chi è in possesso della chiave privata del server può decodificarla e leggerne i contenuti. La presenza di un certificato sul sito è identificata dall'url del sito stesso. L'aggiunta del certificato implica che non si possa più usare il protocollo http ma https, per cui l'indirizzo del sito, ad esempio, html.it sarà https://www.html.it e non http://www.html.it.

In IIS per abilitare l'utilizzo di certificati digitali è necessario entrare nelle proprietà del sito e selezionare la scheda *Protezione directory* quindi *Certificato Server*, in questo modo si apre una scheda che ci permette di creare una chiave, oppure importare un certificato o copiarlo da un altro sito. Per lo scopo di questa guida ci soffermeremo solo sulla creazione di un nuovo certificato.

Seguiamo le indicazioni e **creiamo una chiave** che poi andremo ad inviare ad una Certification Authority (CA) autorizzata che ci consegnerà un certificato da installare sul nostro server web. L'Installation Wizard, durante la creazione della chiave, ci chiederà alcune informazioni che serviranno poi alla CA per generare un certificato. Innanzitutto è necessario specificare il nome corretto del sito web e la dimensione della chiave (questa informazione è necessario recuperarla dalla CA che vogliamo utilizzare, in genere 1024 bit), il punto più importante è il nome comune ossia l'indirizzo dns del sito (se si indicherà un nome sbagliato il certificato non riconoscerà correttamente il sito).

Una volta completato il processo noi avremo un file da inviare alla CA per creare un **vero certificato digitale**. Premendo con il tasto sinistro del mouse sul pulsante certificato server le opzioni sono cambiate e il sistema si aspetta che noi gli forniamo il certificato digitale creato con la chiave. Quando la CA ci avrà fornito il file con estensione .cer, potremo completare la procedura installandolo mediante il pulsante certificato server e indicando la locazione sul disco del file.

Successivamente, nella scheda *Comunicazioni protette*, sarà possibile indicare una serie di **opzioni da associare al nostro certificato**. Ad esempio spuntando la prima casella, la protezione SSL viene attivata e può essere resa più sicura indicando codifica 128 bit (se il certificato li supporta). È possibile inoltre abilitare i certificati lato client oppure eseguire il mapping mediante Active directory con utenti certificati. Per completare la procedura e rendere effettivo il sito SSL è necessario indicare la porta SSL nella scheda delle proprietà generali del sito come 443. A questo punto scrivendo https://nomedelsito, abbiamo reso effettivo il nostro sito in https.

Andiamo ora più in dettaglio e vediamo come funziona il cuore stesso del server web, come esso può concedere le risorse.

# La sicurezza profonda di IIS 6

IIS 6.0, è stato totalmente reingegnerizzato supportando nativamente Asp.NET. Microsoft, quindi, ha rilasciato un web server molto più performante e affidabile.

Rispetto a IIS 5.0 sono stati migliorati tutti gli aspetti legati alla sicurezza. In IIS 5.0 tutti i processi (eccetto eccezioni particolari) venivano processati all'interno di inetinfo.exe, che veniva eseguito con i permessi di "Local System Account", che ha più permessi addirittura di administrator. Era chiaro che in caso di un bug del server web e di un buffer overrun, con relativa apertura di nuova sessione, **l'utente era local system account e aveva l'assoluto controllo del sistema!** Con IIS 6.0 è stata ricostruita completamente tutta la struttura del web server come mostra la figura sottostante.

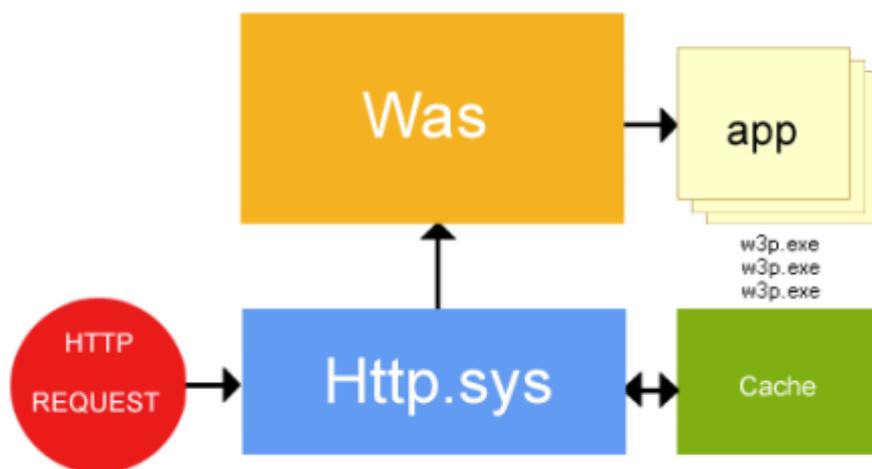


Figura 14. Processo di richiesta di pagina Web

Come si può vedere dall'immagine, ogni richiesta Web viene accettata dal processo http.sys che lavora in modalità Kernel Mode e non più in modalità User Mode come nel IIS 5.0 con Inetinfo.exe.

Questo processo accetta e accoda tutte le richieste in arrivo e le passa al gestore dei Pool, cioè al Was (**Web Administration Service**), che si occupa di controllare e monitorare lo stato delle applicazioni web e di riciclare i worker process (overlapping).

Ogni Pool di processi può essere costituito da uno o più worker process. I pool di processi gestiscono la configurazione dei siti web e permettono di gestire le impostazioni e configurazioni per il riciclo, lo stato e le prestazioni dei singoli worker process. La situazione ottimale (predefinita) si ha quando si associa ad ogni pool di applicazioni un solo sito web, in quanto un suo malfunzionamento non implicherebbe un degrado delle prestazioni anche degli altri nello stesso pool.

## Worker process

Sono i processi finali in cui girano le applicazioni, i filtri ISAPI ed eventuali estensioni. Il processo che esegue ciascun worker process è W3WP.EXE, ossia il sostituto in IIS 6.0 di DLLHOST.EXE di IIS 5.0. Le richieste sono controllate e gestite mediante una coda di tipo FIFO (First In, First

Out, cioè il primo che arriva è il primo ad essere servito, come agli sportelli delle banche o della posta, ci si mette in coda fino al proprio turno).

Sempre rispetto al suo predecessore IIS 6.0 è configurato in maniera più sicura in quanto molte delle impostazioni che in IIS 5.0 era necessario disabilitare qui lo sono già. Ad esempio, la dimensione dei file pubblicabili sul web via browser è di default molto piccola (200 Kb).

Poichè esistono ancora alcune applicazioni che giravano in "modalità isolamento" di IIS 5.0 (Isolation Mode) e che non funzionerebbero usando i worker process di IIS 6 è possibile eseguire l'Isolation mode di IIS 6 come se fosse l'Isolation mode di IIS 5.0. Cliccando con il tasto destro sulla voce *Siti web* si sceglie *Proprietà* e rispetto alle schede del singolo sito web si trova la scheda *Service*. Si selezioni *Esegui il servizio WWW in modalità isolamento IIS 5.0*. In questo modo anche quelle rare applicazioni che non avrebbero girato su IIS 6 ora lo faranno.

# Creazione del server Ftp

Per creare un nuovo sito Ftp, ossia un server che sarà in grado di accettare non visualizzazioni di pagine web ma upload e download di file, è necessario cliccare con il tasto destro del mouse sopra la cartellina siti Ftp e scegliere *Nuovo*, quindi premere su *Avanti*. Si apre una finestra dove è necessario indicare il nome del nuovo sito (ha valenza solo indicativa in quanto il nome sarà mostrato solo sull'albero dei siti Ftp), premendo poi ancora *Avanti* viene chiesto l'indirizzo internet (Ip) da associare al sito e la porta, normalmente 21. Successivamente, premendo ancora *Avanti*, viene chiesto che livello di sicurezza associare al sito (figura 15), cioè se è necessario proteggere le home directory in modo tale che gli utenti condividano la stessa cartella e possano entrare nelle home di altri utenti, oppure se devono essere separate, o addirittura controllate mediante *Active Directory*.

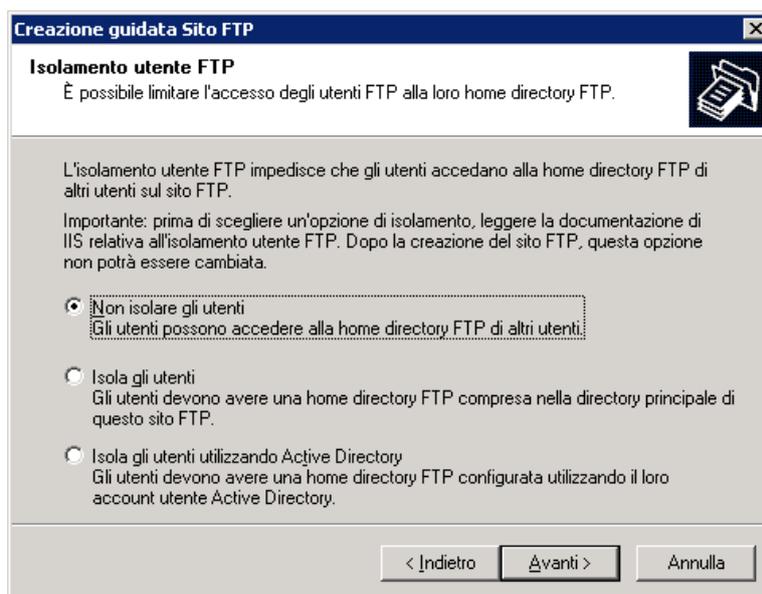


Figura 15. Livello di sicurezza

Successivamente, premendo *Avanti*, viene richiesto il percorso sul disco dove verrà montata la directory del sito Ftp. Infine viene chiesto quale deve essere la tipologia di accesso, cioè se gli utenti possono solo leggere i dati contenuti nella cartella o anche scrivere al suo interno (figura 16).

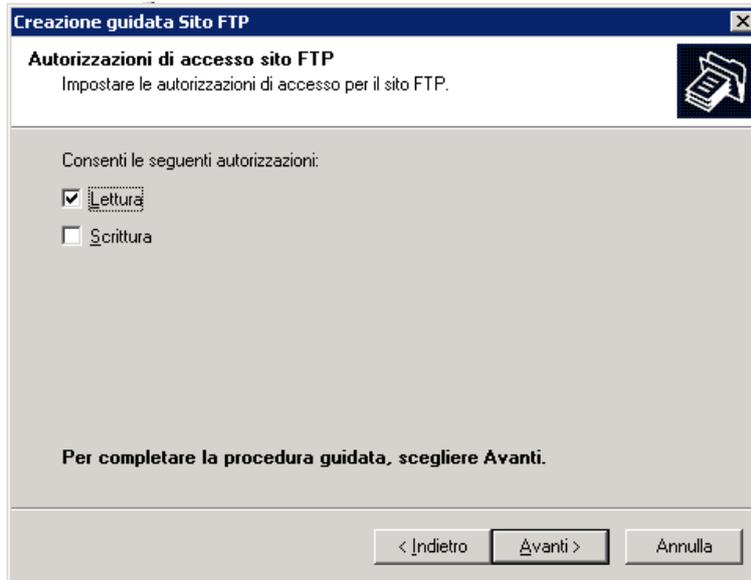


Figura 16. Nuovo sito ftp

# Configurazione generale

Vediamo ora come è possibile modificare tutte le proprietà di un sito Ftp che possono essere configurate mediante l'apposita finestra della MMC, proprio come abbiamo fatto per il server Web. Dopo aver creato il sito, cliccate con il tasto destro del mouse sul nome del sito e scegliere *Proprietà* tra le varie voci. Si apre, quindi, una finestra con 5 linguette (o tab o schede) che analizzeremo in dettaglio in questo e nel seguente capitolo.

## **Sito Ftp**

È la sottofinestra predefinita che contiene le proprietà fondamentali per il corretto funzionamento del sito ed è visualizzata in figura 17.

- **Descrizione:** indica il nome assegnato al sito ha solo la funzionalità di identificare nell'albero dei siti, il sito appena creato (sarà il nome con cui noi vedremo il sito ftp nella console).
- **Indirizzo IP:** indirizzo internet a cui risponde il servizio FTP una volta avviato per il sito in questione. Per ogni copia IP-porta è possibile creare un solo sito FTP. Infatti, mentre per i siti Web è possibile utilizzare la funzionalità di Virtual hosting, per i siti FTP ciò non è possibile quindi se si vuole creare più siti FTP rispondenti sullo stesso IP è necessario collegarli a porte diverse (in gergo eseguire il binding). In realtà esiste un altro metodo per eseguire un'operazione simile al virtual hosting, e sarà descritta in seguito.
- **Porta TCP:** è un numero compreso tra 0 e 65535 e consente di abilitare il sito ad accettare connessioni su una determinata copia IP-porta, di default la porta FTP è la numero 21. Se viene modificata ed usata un'altra, ad esempio 8888, anche i client che si connettono al server dovranno definire come porta FTP la 8888 e non la porta 21, altrimenti il client darà un errore di server non trovato.
- **Connessioni a sito:** ci sono 2 possibilità, illimitate (predefinita), e limitate, specificando inoltre il valore da indicare per le quali il server accetta connessioni, superato il quale invece rifiuta.
- **Consenti registrazione attività:** spuntando questo checkbox è possibile registrare gli accessi degli utenti su database o in formato testo.

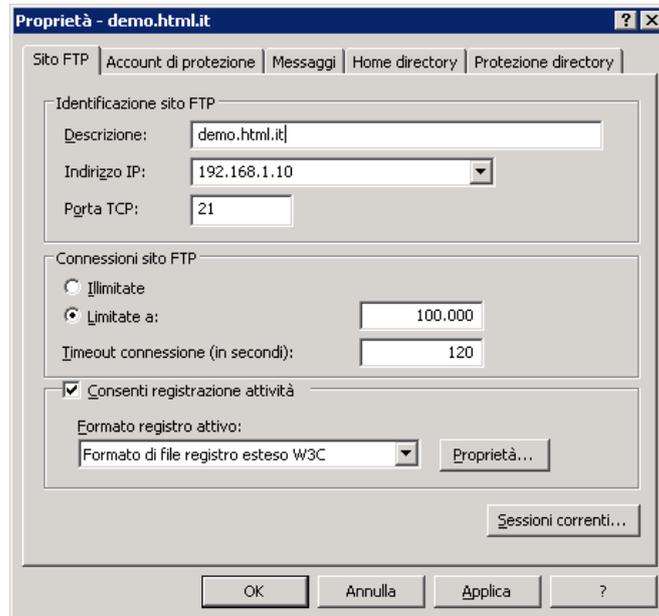


Figura 17. Linguetta principale

## **Messaggi**

Questa funzione (figura 18) permette di definire i messaggi che il servizio FTP produce in output in determinate situazioni:

- **Banner:** rappresenta il testo che viene sempre visualizzato al momento della richiesta di username e password o genericamente di connessione.
- **Alla connessione:** è il testo che viene visualizzato una volta completata la connessione (in genere dopo il login, o la connessione in caso di accesso anonimo).
- **Alla disconnessione:** una volta che l'utente è uscito dal server FTP.
- **Numero massimo di connessioni:** è il testo visualizzato quando si raggiunge il numero massimo di connessioni.

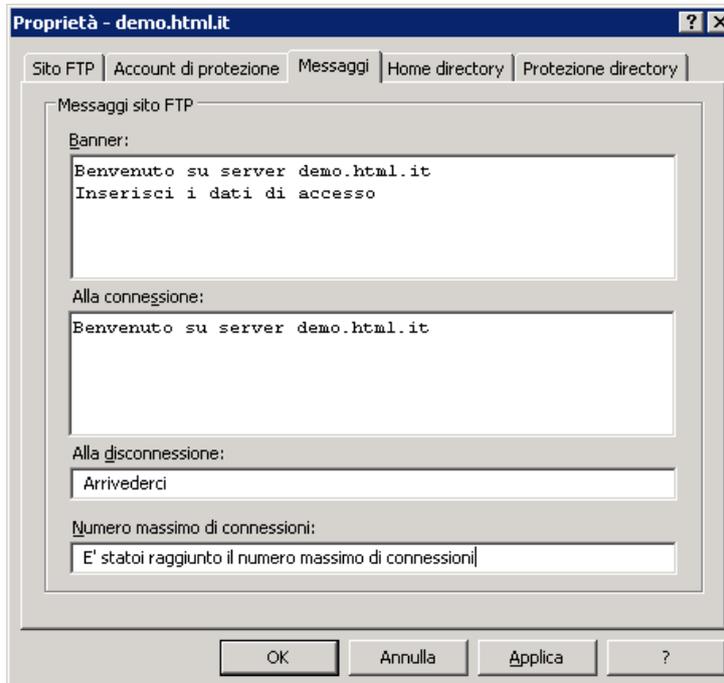


Figura 18. Messaggi

## ***Home Directory***

In questa sottofinestra (figura 19) viene definito il posizionamento e le permissions dei contenuti del sito FTP.

- **Provenienza della directory:** questa configurazione permette di scegliere tra una cartella locale oppure situata su un'altro computer.
- **Directory sito Ftp:** permette di specificare il percorso fisico alla cartella che contiene le informazioni accessibili mediante il sito e ne identifica il tipo di operazione che è consentito fare: lettura, scrittura oppure logging delle visite.
- **Stile visualizzazione directory:** permette di definire se le modalità di visualizzazione e interrogazione al prompt sono stile Unix o Dos.

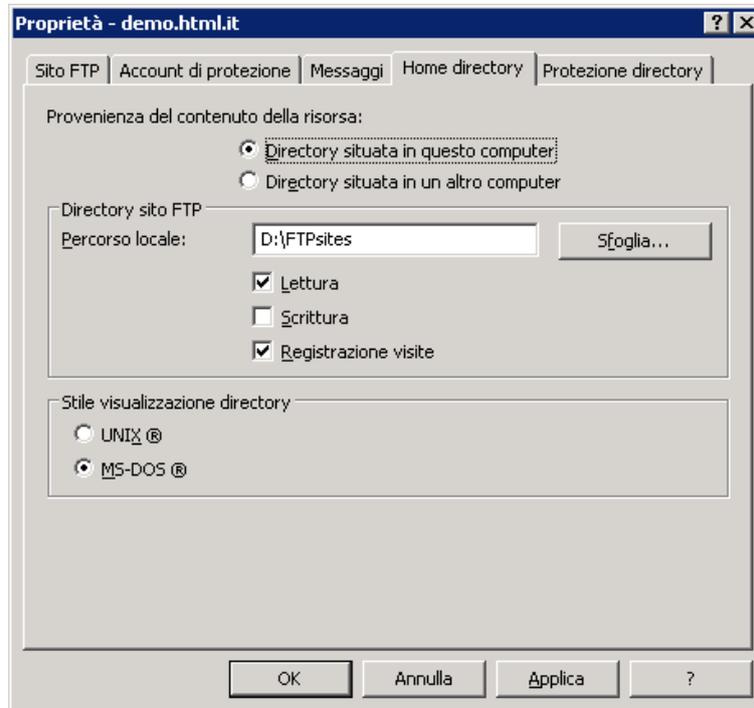


Figura 19. Home Directory

# Configurazione delle protezioni

Sempre nelle linguette del pannello di configurazione esistono due strumenti in grado di proteggere il server Ftp da connessioni non autorizzate.

## **Account di protezione**

Questa funzionalità (figura 20) definisce il tipo di accesso che è permesso al sito Ftp. Se il sito deve permettere le connessioni anonime, cioè se non è richiesto l'inserimento di nome utente e password per poter accedere al sito, è necessario spuntare il checkbox ed eventualmente indicare quale utente della macchina usare per impersonare l'utente anonimo. In caso si lasci l'utente predefinito, il suo valore è *IUSR\_nomemacchina*, e, a meno di particolari necessità, conviene lasciarlo così configurato. Se invece è necessario richiedere username e password di accesso, si lascia senza spunta il checkbox *Consenti connessioni anonime*, così il servizio permetterà l'accesso solo a quegli utenti che si saranno autenticati al login e avranno i privilegi sul filesystem per poter leggere ed eventualmente scrivere sulla cartella del sito.

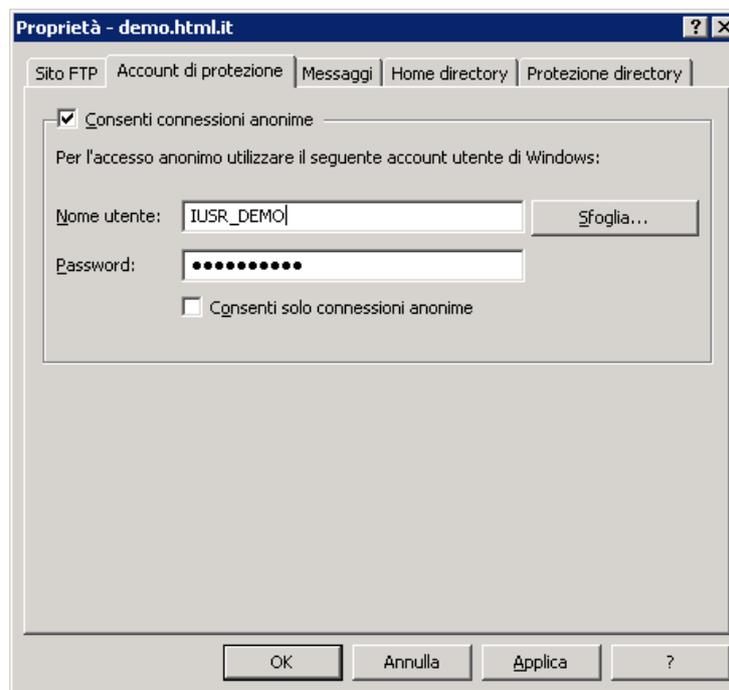


Figura 20. Account di protezione

## **Protezione directory**

In questa linguetta (figura 21) è possibile configurare le proprietà di accesso a livello di Ip di chi si connette. Attraverso il pulsante di opzione posto a destra è possibile definire se permettere di default l'accesso a chiunque e negarlo a qualcuno in particolare, oppure negarlo di default e permettere a qualcuno in particolare di accedervi. Il pulsante *Aggiungi* permette di definire un singolo computer, una classe di IP, oppure un dominio al quale applicare i criteri di cui sopra (nel caso di un dominio, è necessario evidenziare che verrà eseguito un reverse lookup per ogni clients che si connette e quindi richiederà del tempo aggiuntivo e delle risorse: è un'operazione sconsigliabile, a meno di motivi validi).

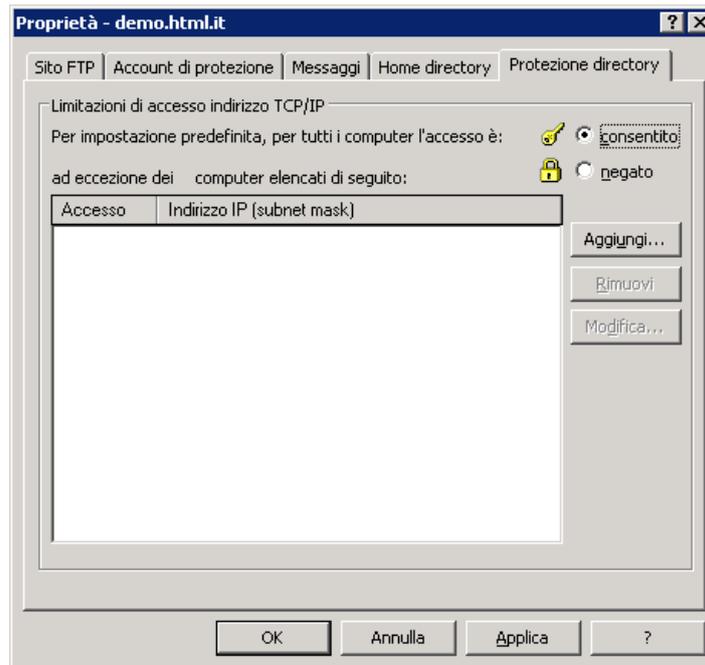


Figura 21. Protezione directory

# Sicurezza di un server Ftp

Le possibili configurazioni di sicurezza sono tantissime e dipendono da ciò che si vuole fare con il sito Ftp. Ad esempio, se vogliamo che gli utenti che si collegano possano solo recuperare materiale precedentemente inserito nella cartella del server si può abilitare la sola lettura nelle proprietà della home directory. Se si vuole permettere l'accesso solo alla LAN aziendale, si può inserire nella protezione directory la subnet relativa alla LAN. Perciò sarà compito dell'amministratore del sito decidere le possibili configurazioni delle proprietà.

Sia per il sito Ftp sia per il sito web le configurazioni per l'accesso mediante utenti avviene utilizzando gli **utenti standard della macchina** (è possibile altrimenti utilizzare utenti di dominio Active Directory se configurati).

Andando sul desktop e cliccando con il tasto destro su *Gestione risorse* e selezionando *Gestisci*, si apre una finestra in cui ci sono vari funzioni. Apriamo la voce *Utenti e gruppi locali*, si vedranno sulla parte destra della finestra due cartelle: *Utenti* e *Gruppi*. Cliccando con il tasto destro sulla voce *Utenti*, selezioniamo *Nuovo utente*, come mostrato in Figura 22. La finestra che si apre consente di definire un nuovo utente della macchina che può accedere a determinate risorse.

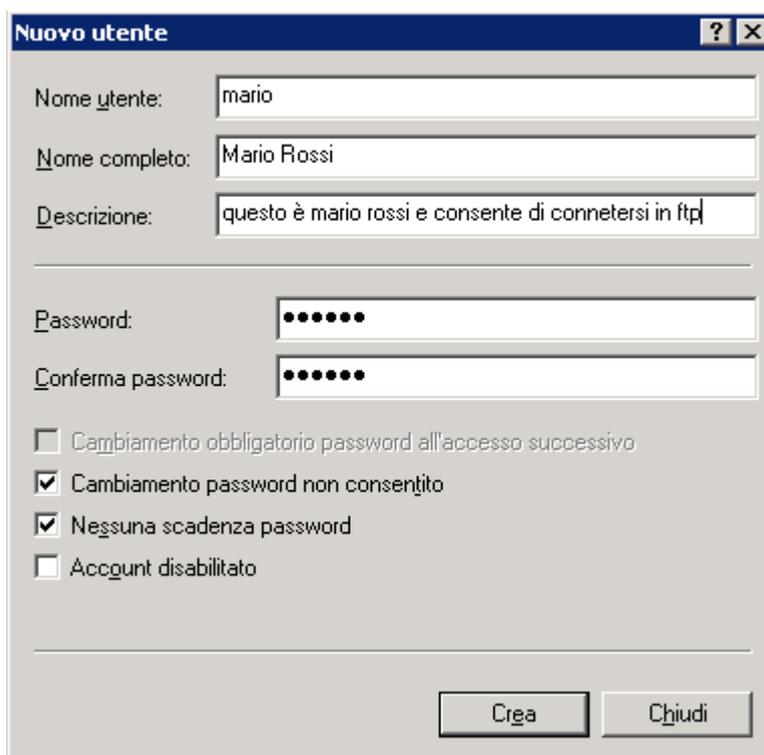


Figura 22. Creazione di un utente di Windows

Vediamo un esempio pratico di come permettere all'utente Mario Rossi di accedere al sito Ftp appena creato:

Per prima cosa creiamo l'utente mario con password 123456. Come mostrato nella Figura 22, specificare mario nello spazio del nome utente e la password nel relativo campo. Selezionare i segni di spunta come in figura.

Supponiamo che la directory in cui è stato creato il nostro sito ftp sia *d:\ftpsites*. Andiamo in *d:\* e clicchiamo con il tasto destro sulla cartella *ftpsites* (sarà stata nostra premura crearla prima di creare

il sito Ftp). Selezioniamo *Proprietà* e successivamente *Protezione*. Clicchiamo su *Aggiungi* e si aprirà una finestra come in Figura 23.

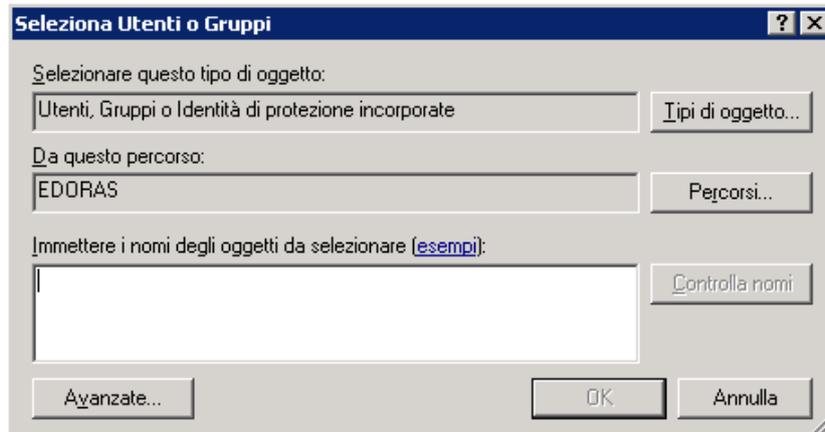


Figura 23. Aggiunta di un utente in una cartella del filesystem

Scriviamo mario nella casella bianca e premiamo *Controlla nomi* e quindi *Ok*. Ora si mostrerà una finestra come in Figura 24, selezioniamo l'utente mario e spuntiamo nella casella sotto le permissions che vogliamo abilitare (*Lettura*, *Scrittura* o *Modifica*). *Lettura* permetterà che l'utente non possa scrivere, *Scrittura* permetterà che l'utente possa anche scrivere ma non cancellare e *Modifica* può fare ogni cosa ai file (leggere, scrivere, cancellare).

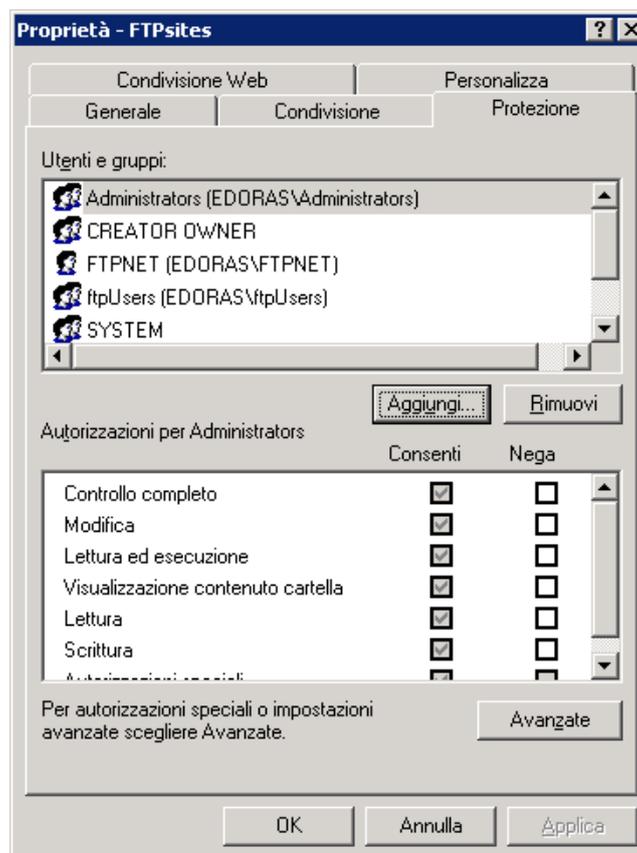


Figura 24. Aggiunta di un utente in una cartella del filesystem

A questo punto l'utente mario può entrare nel sito eseguendo l'autenticazione con il proprio programma Ftp.



# Cartelle virtuali Ftp

Ad ogni sito Ftp possono essere associate una o più directory virtuali. Come dice la parola stessa, sono degli alias di directory che puntano ad una determinata cartella del filesystem. Possono essere usate per creare un contenitore di cartelle distribuite sul filesystem, indipendentemente dalla cartella associata al sito Ftp.

Il loro maggiore utilizzo, però, è per gestire più siti Ftp con un **solo indirizzo IP**. Infatti capita spesso di dover creare più siti Ftp distinti con utenti diversi che possono accedervi. Abbiamo visto, però, che non è possibile avere due siti Ftp sullo stesso indirizzo IP e sulla stessa porta. Mediante le directory virtuali, è, però, possibile risolvere questo problema. Creato un sito Ftp alla cui cartella principale devono poter accedere tutti gli utenti che accederanno al sito, creeremo una cartella virtuale che rappresenterà il sito Ftp "virtuale" o in "virtual-hosting". Il nome della cartella deve essere uguale allo username dell'utente della macchina che vi accederà (nell'esempio precedente mario). In questo modo al login l'utente verrà reindirizzato alla sottocartella (directory virtuale), come se fosse un sito diverso, senza passare per la home directory del sito principale. Come si può facilmente capire, l'unico limite è dato dal fatto che vi potrà essere solo un utente che automaticamente verrà reindirizzato sul sito in modo automatico.

Vediamo un **esempio** per chiarire la cosa: abbiamo necessità di creare tre siti Ftp, uno per l'area sviluppo, uno per l'amministrazione ed uno per tenere la documentazione. Creiamo, come spiegato nella lezione precedente, un unico sito Ftp che risponde sulla porta 21 e lo chiamiamo MainFTP. Creiamo poi tre utenti della macchina: development, administration, documentation con relative password, inoltre creiamo tre cartelle, una per ciascuna directory virtuale, dove andranno a scaricare o caricare i documenti mediante Ftp.

A questo punto dentro al sito MainFTP (nella MMC) creiamo tre cartelle virtuali con gli stessi nomi degli utenti, quindi: development, administration, documentation e che punteranno alle tre cartelle fisiche descritte sopra. I tre utenti devono poter accedere in lettura alla cartella principale del sito, altrimenti il sistema negherà l'accesso. A questo punto eseguendo il login al sito MainFTP con uno dei tre login si verrà reindirizzati automaticamente all'interno della cartella virtuale. Con questo sistema abbiamo aggirato il problema di creare più siti Ftp sullo stesso indirizzo ip con la stessa porta.

Le directory virtuali, una volta create, hanno una scheda delle proprietà in cui è possibile, come per il sito Ftp, modificarle proprietà della cartella e i permessi di accesso.

# Creazione di un server Smtip

IIS 6.0 ha al suo interno un connettore che permette di funzionare come server Smtip. Ciò significa che è possibile utilizzare questo servizio per inviare e-mail da script nei vari siti. Il sistema appena installato prevede un server Smtip predefinito che ha per dominio predefinito il nome della macchina e tutte le cartelle per farlo funzionare installate in *c:\inetpub\mailroot*. È inoltre possibile creare **altri server virtuali** che rispondono su Ip diversi. È possibile ottimizzare l'invio delle mail creando domini locali, alias o domini remoti, in modo tale da verificare per ciascun dominio tutta una serie di parametri.

Per prima cosa vediamo come creare un server virtuale di posta. Cliccando con il tasto destro sul server virtuale Smtip predefinito si seleziona *Nuovo*. Viene aperta una nuova finestra in cui è necessario indicare il nome del server virtuale, utilizzato solo in visualizzazione nell'albero della console amministrativa del server Web, come in figura 25. Successivamente è necessario specificare l'Ip a cui associare il server Smtip. In seguito è necessario indicare una cartella nel filesystem dove è possibile installare tutte le directory necessarie al buon funzionamento del connettore Smtip e del dominio virtuale. Infine è necessario indicare il nome del dominio che verrà associato al connettore creato e che risponderà per esso.

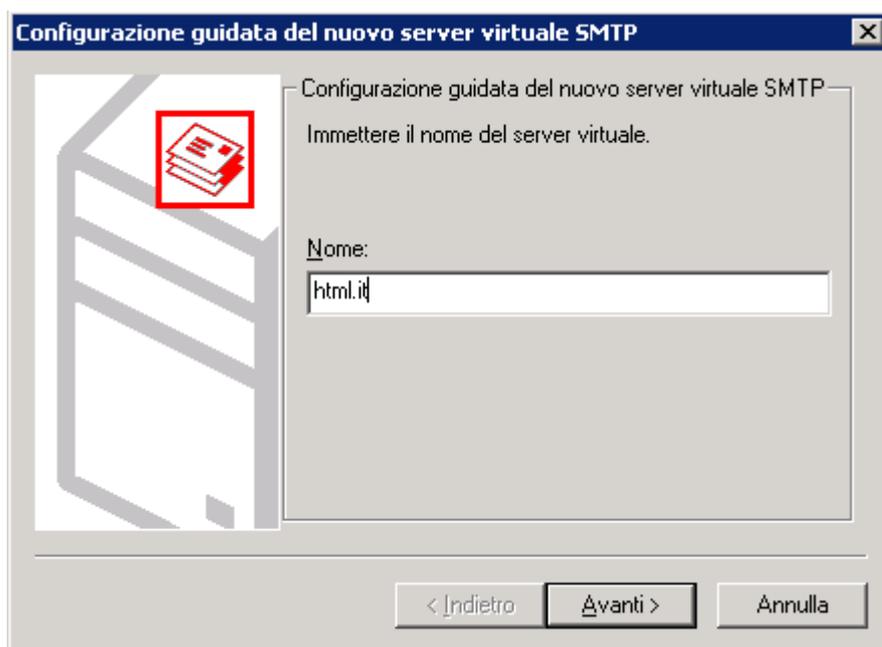


Figura 25. Nuovo server virtuale

Andiamo ora a vedere, una volta creato il dominio virtuale, quali sono le eventuali configurazioni che possiamo andare a cambiare. È chiaro che la configurazione è presente anche nel dominio virtuale di default creato dal sistema durante l'installazione.

# Configurazione delle opzioni generali

## Generale

Questa scheda permette di configurare le impostazioni relative all'Ip alla porta, al numero massimo di connessioni e alla configurazione del logging delle connessioni.



Figura 26. Scheda Generale

## Accesso

Questa scheda permette di configurare le modalità di accesso e connessione verso il server Smtip.

- **Autenticazione:** è possibile indicare se l'invio delle mail a questo server può essere fatto senza autenticarsi oppure usando un sistema di autenticazione (in genere lasciare la connessione anonima, altrimenti non si ricevono mail dai normali server di posta).
- **Comunicazione protetta:** è possibile installare un certificato con cui proteggere le comunicazioni
- **Connessione:** è possibile indicare i server o le reti che possono connettersi sulla porta 25 di questo server per consegnare delle mail (la configurazione è simile a quella della sicurezza sul server web).
- **Inoltro:** come per la connessione, anche qui è possibile specificare l'Ip dei server o in generale computer che possono connettersi per inviare mediante questo connettore Smtip le e-mail. In genere si inserisce l'indirizzo 127.0.0.1 e i vari Ip del server su cui è installato il web, in modo tale che dai vari script sulla macchina possono essere inviate mail. Questa

funzione è molto importante per la gestione della funzione anti "open relay" (argomento che tratteremo più avanti).

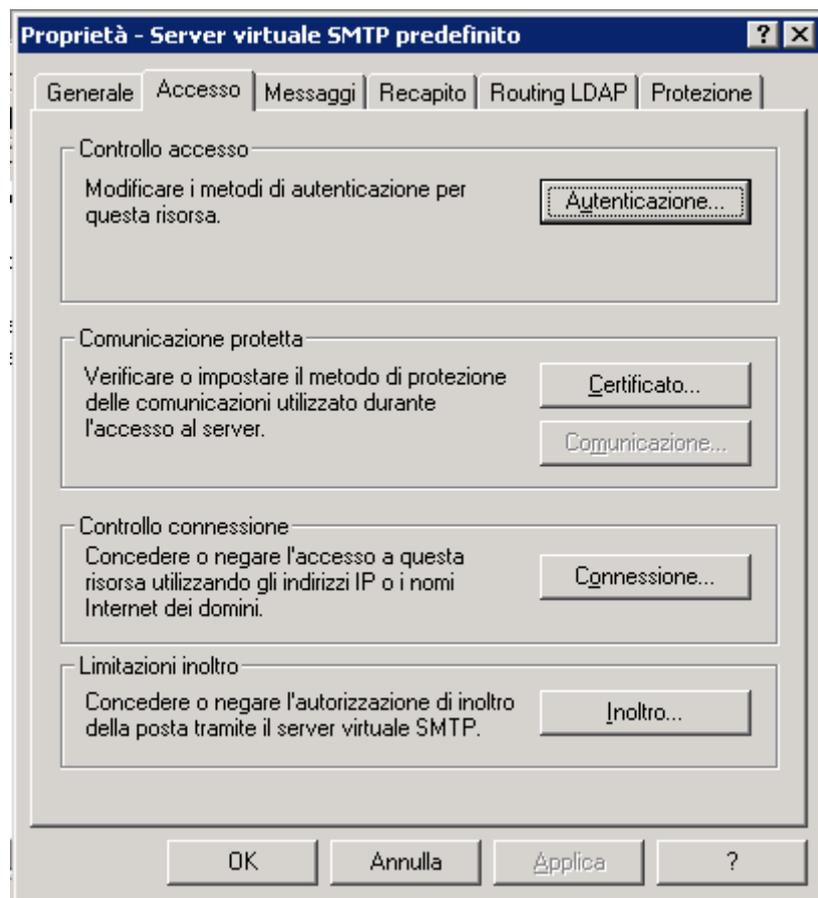


Figura 27. Scheda Accesso

# Configurazione delle opzioni specifiche

## Messaggi

In questa scheda possono essere specificate le opzioni relative alla dimensione dei messaggi per invio e per sessione, il numero massimo di messaggi per connessione e il numero massimo di destinatari per invio. È possibile inoltre indicare un indirizzo di posta elettronica a cui inviare una mail indicante il non riuscito invio e la cartella in cui sono salvate le e-mail non inviate perchè errate (errore di qualsiasi genere: rifiutate dal server destinazione, indirizzo destinatario inesistente, etc...).

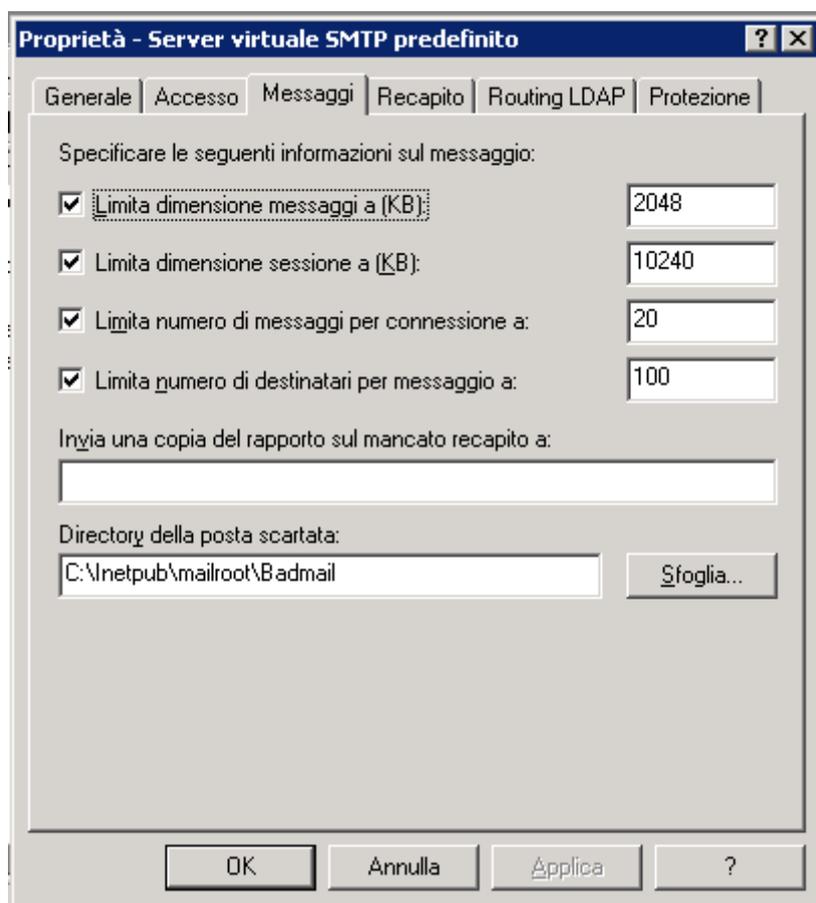


Figura 28. Scheda Messaggi

## Recapito

In questa scheda sono definiti tutte le opzioni a cui il server Smtip deve attenersi per gli invii, dai tempi di retry (tentativo successivo al primo, nel caso non sia stato possibile contattare il server remoto) alla notifica di ritardo e così via.

- **Protezione della posta in uscita:** permette di definire se è necessario che lo script o l'utente che si connette al server Smtip debba autenticarsi per inviare la posta oppure no.
- **Connessioni esterne:** permette di ridefinire le opzioni assegnate in fase di creazione del server Smtip, cioè il numero massimo di connessioni, il numero di connessioni per dominio e la porta a cui il server accetta le connessioni.

- **Avanzate:** permette di definire una serie di operazioni che il server può eseguire, come il numero massimo di passaggi che possono avvenire prima di rifiutare una mail, il dominio di mascheramento, un dominio fittizio che viene usato per inviare le mail, il dominio reale, e infine lo smarthost, e cioè un server verso cui il connettore inoltrerà la posta (ad esempio un server Smtplib esterno ad un sistema di firewalling).

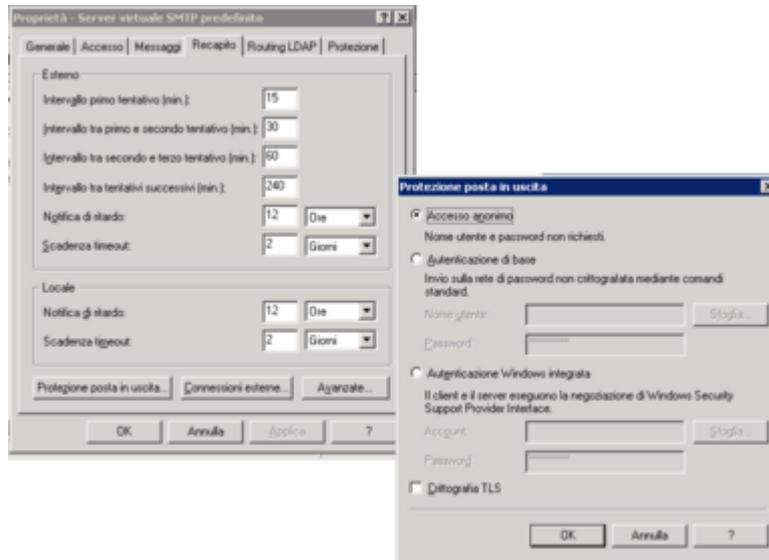


Figura 29. Scheda recapito e sue sottoschede

## ***Routing LDAP e Protezione***

Permettono di configurare rispettivamente un server Ldap per la gestione della posta e l'elenco dei gruppi o degli utenti che possono configurare il connettore.

# Affidabilità di un server Smtip

Affinchè il server Smtip sia riconosciuto affidabile su internet è bene che soddisfi due requisiti importanti:

1. Non sia un open relay
2. Risponda ad un reverse lookup.

Analizziamo meglio questi 2 concetti.

Lo **spam** su internet si è sviluppato mediante la presenza di server Smtip che permettevano a chiunque di utilizzarli per inviare e-mail. Con questo sistema era possibile mandare grosse quantità di e-mail pubblicitarie, lasciando al server il compito di recapitarle. Da un po' di anni esistono delle organizzazioni che tracciano i server aperti, cioè quei sistemi Smtip che non hanno protezione e che permettono a chiunque di utilizzarli per inviare la posta.

Queste organizzazioni creano le cosiddette **blacklist** o liste nere, in cui vengono inseriti questi cosiddetti "open relay", e che possono essere usate dai server di posta per evitare di accettare mail da server Smtip all'interno della blacklist. Detto questo vi sono 2 sistemi che permettono di non essere inseriti in una black list e cioè evitare di essere degli "open relay":

1. Inserire nella scheda "accesso" e poi "inoltrò" solo l'Ip delle macchine o della subnet che vogliamo abilitare per inviare tramite questo server, in questo modo nessun altro può connettersi per inviare.
2. L'altro sistema consiste nel richiedere una username e password per inviare la posta. Sempre nella scheda recapito, protezione della posta in uscita, scegliere autenticazione base ed indicare una username e password che dovrà essere usata per inviare la posta.

In questo modo non saremo degli open relay.

Un altro sistema usato per evitare lo spam da una macchina è usare un **reverse lookup**. Il server destinazione verifica il nome di dominio che noi abbiamo impostato per il nostro connettore (server virtuale) nella scheda *Recapito / Avanzate / Dominio completo* ed esegue un reverse lookup, cioè si fa dare l'indirizzo Ip associato alla macchina o meglio al nome con cui ci siamo presentati. Se questo nome coincide con l'indirizzo con cui ci siamo connessi accetterà la posta, altrimenti la rifiuterà.

È un po' come chiedere la carta d'identità a qualcuno che ci vuole consegnare a casa un pacco. È un sistema che alcuni grossi server Smtip usano (libero, wind e altri). Per risolverlo, l'unico modo è far inserire il nostro Ip nel Dns che gestisce la rete di cui noi abbiamo acquistato l'Ip. Ad esempio se abbiamo una ADSL con 8 Ip statici del gestore X dovremo richiedere che inserisca nella voce della tabella relativa ai Ptr (tipologia di dato presente nel database del Dns) del suo Dns il nome del nostro server di posta con il suo relativo Ip. In questo modo chiunque esegua un reverse lookup del nostro Ip otterrà il nome corretto della macchina e accetterà la posta.

# Il file Metabase: Backup

Per concludere questa guida analizziamo cosa fare se avviene un "disastro" e il nostro server (o il sistema operativo) non vuole proprio saperne di partire.

La **metabase** è il file di configurazione del server web (si intende anche Ftp e Sntp), cioè un file dove il sistema salva le configurazioni fatte mediante l'interfaccia grafica. Diventa utile per modificare alcune impostazioni che via interfaccia grafica non possono essere modificate, ad esempio la dimensione massima dei file che vengono uploadati.

Una grande novità è la sostituzione della complessa metabase di IIS 5.0 con la nuova metabase XML di IIS 6.0. Con IIS 5.0 era necessario installare un apposito editor (presente nel resource kit) che ne permettesse le modifiche, ora invece essendo il formato XML, ogni editor può essere sufficiente per modificare il file.

Il file si trova nella cartella `%systemroot%\system32\inetsrv` (%systemroot% identifica il percorso alla cartella del sistema operativo normalmente essa è c:\windows) e si chiama appunto Metabase.xml. Nella stessa cartella c'è anche lo schema XML nel file MBSchema.xml. I vantaggi nell'utilizzare questo tipo di file sono facilmente evidenti in caso di "corruzione" del file, infatti un file xml può facilmente essere sistemato con qualsiasi editor di testo (notepad ad esempio), mentre il file binario presente nelle precedenti versioni dava dei grossi problemi e spesso era necessario recuperare un backup di IIS.

Il sistema esegue automaticamente delle copie dei file MBSchema e Metabase nella cartella `%systemroot%\system32\inetsrv\history`, ogni copia è evidenziata dal major number e minor number nella forma di metabase\_majornumber\_minornumber.xml, questi file però possono essere usati esclusivamente **sulla macchina dove sono stati creati**. Per questo motivo il tool per la creazione di backup del sistema IIS 6.0 diventa utile in quanto permette di spostare facilmente un server web da una macchina all'altra (chiaramente Windows2003 con IIS6).

Per poter recuperare le configurazioni del server Web (ma, naturalmente, non i dati) è necessario effettuare preventivamente e ad ogni modifica un **backup**. Per eseguire una tale operazione è necessario aprire la MMC di IIS e cliccare con il tasto destro sul nome del server in cui è installato il server web in questione, si aprirà un menù contestuale, selezionare *Tutte le attività* e quindi *Backup o ripristino configurazione*. In questa finestra sono visualizzati i backup eseguiti, inoltre da questa finestra si può selezionare un file per eseguire un restore (tutto il server web prende le configurazioni del file selezionato, attenzione!), o effettuare un nuovo backup, verrà richiesto un nome da dare al file che sarà creato.

Con questo sistema noi possiamo salvare tutto il server web ma è possibile effettuare anche un **backup per singolo sito**, eseguendo un salvataggio della configurazione su file. Si seleziona il sito web interessato e si clicca con il tasto destro del mouse selezionando *Tutte le attività* e quindi *Salva la configurazione in un file*, in questo modo si apre una finestra che ci chiede alcune informazioni per procedere con il salvataggio. È necessario inserire il nome del file con cui vorremo poi identificare il sito salvato e il percorso dove salvarlo. Eventualmente il contenuto può essere criptato mediante una password. In questo modo viene salvato un file in formato XML che successivamente può essere usato per ricreare, anche su un altro computer il sito (attenzione non vengono salvati i dati, ma solo le configurazioni).

# Il file Metabase: Restore

Come eseguire il ripristino delle configurazioni dei server di IIS 6 attraverso la Metabase

Nel caso in cui abbiamo le copie dei file su un disco esterno o su un'altra macchina e perdiamo il server principale, possiamo eseguire un **restore**, cioè possiamo riportare il server web allo stato in cui ho eseguito il backup o del singolo sito o del sistema completo.

Per effettuare un **restore di un solo sito web** (non deve già esistere un sito con quel nome) è sufficiente selezionare sempre con il tasto destro del mouse la voce *Sito web*, quindi *Nuovo* e *Nuovo (da file)*, specificando il file salvato, ci si ritrova il nostro sito come quando l'avevamo salvato. Se l'indirizzo Ip o il percorso fisico non coincidessero con quelli salvati, sarà sufficiente modificarli andando nella apposita scheda del sito, come descritto precedentemente.

Per effettuare, invece, un **restore del server completo**, dopo aver reinstallato un nuovo server web come mostrato all'inizio dell'articolo, e salvato i file di backup nella cartella `%systemroot%\system32\inetsrv\history` o nella cartella `%systemroot%\system32\inetsrv\metaback` si deve aprire la MMC di IIS e cliccare con il tasto destro sul nome del server in cui è installato il server web in questione, si aprirà un menu contestuale, selezionare *Tutte le attività* e quindi *backup o ripristino configurazione*. In questa finestra selezionare il backup da cui recuperare il server web. In questo modo abbiamo ristabilito la situazione come era al momento del backup.