Sicurezza
Implementare appropriate misure di sicurezza in un sito Web

Data la diffusione dei dispositivi che ospitano i siti *Internet*, è naturale attendersi che maggiore è la diffusione, e tanto più si corre il rischio che malintenzionati, conoscendo i limiti ed i difetti della tecnologia impiegata, tentino di forzarne la sicurezza. È di fondamentale importanza per un'azienda definire criteri di protezione specifici. Ad esempio bisogna definire come intervenire in caso di furto, se esiste una strategia di *backup*, e quali utenti hanno accesso a quali risorse facendo distinzione tra porzione pubblica e porzione privata del sistema. Bisogna comunque precisare che è importante valutare bene le impostazioni di sicurezza, in modo da identificare le specifiche più adeguate alla propria situazione aziendale, e non penalizzare eccessivamente le prestazioni. È chiaro che se si eccede nelle politiche di sicurezza si rischia di isolare il proprio sistema dal mondo esterno, rendendolo irraggiungibile ai più.

Poiché il sito *Web* poggia sul *Web server*, è chiaro che le problematiche di sicurezza riguardano principalmente il *Web server*. In questa parte del modulo analizziamo *Microsoft Internet Information Services* (IIS) che è stato introdotto nel **modulo 13**. Di problematiche di sicurezza (di altri sistemi) ci occuperemo anche nel **modulo 17**, quando discuteremo dei *server Web* in generale.

La sicurezza di Microsoft Internet Information Services

Qui descriviamo le procedure consigliate per configurare la sicurezza di un *server Web* che esegue *Microsoft Windows* e *Internet Information Services* (IIS). Essendo il *Web server* un processo, il quale viene eseguito all'interno del sistema operativo, è tacito che una buona sicurezza del sistema inizi proprio nel considerare l'interazione di IIS col sistema.

IPSec: è consigliabile impostare i criteri per il filtraggio di pacchetti IPSec (*Internet Protocol Security*) in ogni *server Web*. Questi criteri implementano un ulteriore livello di sicurezza in caso di violazione dei ***firewall***. È buona norma impostare più livelli di sicurezza: se ne fallisce uno, c'è sempre una seconda porta da forzare. In generale è necessario bloccare tutti i protocolli TCP/IP diversi dai protocolli che si desidera supportare e le porte da utilizzare. Per l'implementazione dei criteri IPSec, è possibile utilizzare lo strumento di amministrazione IPSec o lo strumento della riga di comando IPSecPol.

***Telnet*:** se si prevede di utilizzare il *server Telnet* incluso in *Windows*, è consigliabile specificare gli utenti che sono autorizzati ad accedere al servizio. A tale scopo, eseguire la procedura seguente:

- Avviare lo strumento Utenti e gruppi locali.
- Fare clic con il pulsante destro del *mouse* sul nodo Gruppo e scegliere Nuovo gruppo dal *menu* di scelta rapida.
- Nella casella Nome gruppo digitare >*TelnetClients*.
- Fare clic su Aggiungi e aggiungere gli utenti a cui si desidera consentire l'accesso ***telnet*** al *computer*.
- Fare clic su Crea e quindi su Chiudi.

Dopo l'aggiunta del gruppo *TelnetClients*, il servizio *Telnet* consente l'accesso al ***server* solo** agli utenti appartenenti al gruppo creato in precedenza.

Impostazione degli elenchi ACL appropriati nelle *directory virtuali*: Sebbene la procedura descritta di seguito vari a seconda dell'**applicazione**, è possibile definire alcune regole che permettono di evitare intrusioni comuni nel sistema. Ecco una serie di operazioni utili:

- **Elenchi ACL predefiniti consigliati in base al tipo di *file*:** Anziché impostare gli elenchi **ACL** per ogni *file*, è consigliabile creare nuove *directory* per ogni tipo di *file*, impostare gli

ACL per le *directory* e consentire l'ereditarietà degli elenchi per i *file*. Una struttura di *directory* potrebbe essere simile alla seguente:

- `c:\inetpub\wwwroot\mioserver\static(.html).`
- `c:\inetpub\wwwroot\mioserver\inclusione (.inc).`
- `c:\inetpub\wwwroot\mioserver\script (.asp).`
- `c:\inetpub\wwwroot\mioserver\eseguibili (.dll).`
- `c:\inetpub\wwwroot\mioserver\immagini (.gif, .jpeg).`

È inoltre importante prestare particolare attenzione alle seguenti *directory*:

- `c:\inetpub\ftproot` (***server*** FTP).
- `c:\inetpub\mailroot` (***server*** SMTP).

In entrambe queste *directory* l'elenco **ACL** è *Everyone* (Controllo completo) e deve essere sovrascritto con autorizzazioni più restrittive a seconda del livello di funzionalità del sistema in uso. Se si desidera supportare *Everyone* (Scrittura), spostare la cartella in un volume diverso da quello del ***server*** IIS oppure, tramite le quote disco di *Windows* 2000, limitare la quantità di dati che è possibile scrivere in queste *directory*.

Tipo di *file*	**Elenchi di controllo di accesso (ACL>, *Access Control List*)**
Processi *CGI* (.exe, .dll, .cmd, .pl)	*Everyone* (X) *Administrators* (Controllo completo) *System* (Controllo completo)
Inclusioni lato ***server*** (.asp)	*Everyone* (X) *Administrators* (Controllo completo) *System* (Controllo completo)
File di inclusione (.inc, .shtm, .shtml)	*Everyone* (X) *Administrators* (Controllo completo) *System* (Controllo completo)
Oggetti statici (.txt, .gif, . jpg, .html)	*Everyone* (R) *Administrators* (Controllo completo) *System* (Controllo completo)

- **Rimuovere ciò che non serve:** L'installazione delle applicazioni di esempio, che non devono essere mai installate in un ***server*** di produzione, non viene eseguita per impostazione predefinita. Alcune applicazioni vengono installate in modo che siano accessibili solo da http://localhost, o 127.0.0.1. È comunque necessario rimuoverle.

Applicazione di esempio	***Directory* virtuale**	**Posizione**
Applicazioni di esempi IIS	*IISSamples*	`c:\inetpub\iissamples`
Documentazione IIS	*IISHelp*	`c:\winnt\help\iishelp`
Accesso ai dati	\MSADC	`c:\Programmi\Filecomuni\System\Msadc`

Disabilitazione o rimozione di componenti COM non necessari: per la maggior parte delle applicazioni alcuni componenti COM non sono necessari e devono essere rimossi. In particolare, è consigliabile disabilitare il componente *File System Object*. Con questa operazione, tuttavia, viene rimosso anche l'oggetto *Dictionary*. È importante tenere presente che i componenti disabilitati potrebbero essere necessari per alcuni programmi. Ad esempio, *Site Server* 3.0 utilizza il componente *File System Object*, che è possibile disabilitare tramite il comando seguente:

```
regsvr32 scrrun.dll /u
```

Rimozione della *directory* virtuale IISADMPWD: la *directory* virtuale IISADMPWD consente di ripristinare la *password* di *Windows* NT e di *Windows* 2000. La *directory* è stata progettata principalmente per reti *Intranet*. Non viene installata automaticamente insieme a IIS 5 e non viene rimossa quando si aggiorna un ***server*** IIS 4 a IIS 5. È necessario rimuoverla se non si utilizza una

rete *Intranet* o se il ***server*** viene connesso al *Web*.

Rimozione di *mapping* di *script* non utilizzati: IIS è stato preconfigurato per il supporto delle estensioni di nomi di *file* comuni, quali asp e shtm. Le richieste di uno di questi tipi di *file* ricevute da IIS vengono gestite da una DLL. Se alcune di queste estensioni o funzionalità non vengono utilizzate, è necessario rimuovere i riferimenti corrispondenti eseguendo la procedura seguente:

- Aprire Gestione *Internet Services*.
- Fare clic con il pulsante destro del *mouse* sul *server Web* e scegliere Proprietà.
- Proprietà principali.
- Scegliere Servizio WWW, quindi Modifica, *HomeDirectory* e infine Configurazione.
- Rimuovere i riferimenti indicati di seguito.

Se non è usato	Disabilitare l'estensione
Reimpostazione di *password* basate su *Web*	.htr, a meno che questa funzionalità non sia assolutamente necessaria!!
Internet Database Connector (in tutti i siti dove è in uso ADO o una tecnologia simile)	.idc
File di inclusione del lato ***server***	.stm, .shtm e .shtml
Stampa *Internet*	.printer
Index Server	.htw, .ida e .idq

Disabilitazione dei percorsi principali: L'opzione Abilita percorsi principali consente di utilizzare .. nelle chiamate a funzioni quali *MapPath*. Per impostazione predefinita, l'opzione è selezionata e deve essere disattivata. A tale scopo, eseguire la procedura seguente:

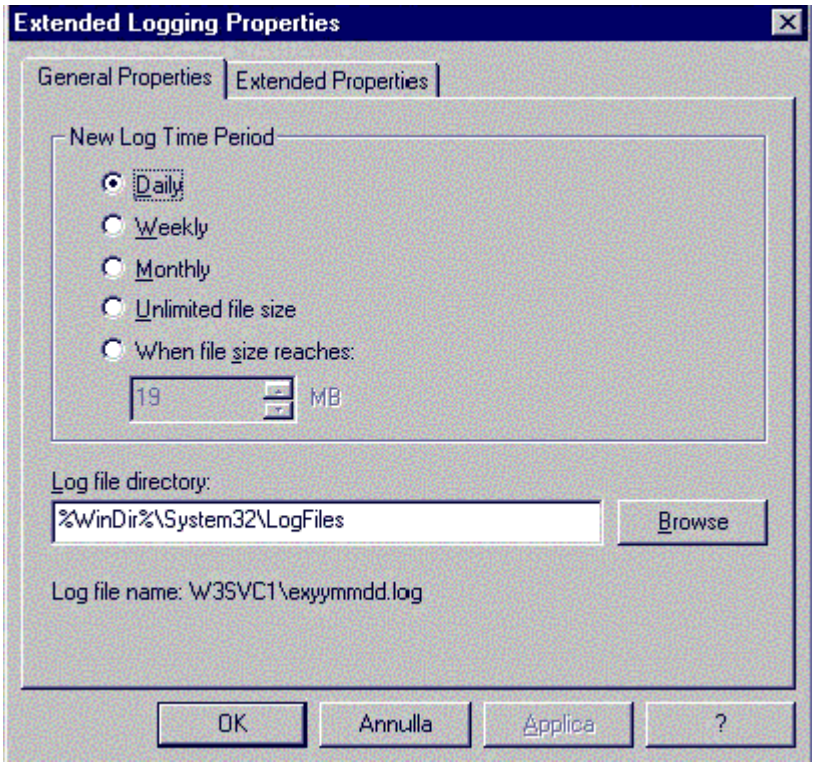
- Fare clic con il pulsante destro del *mouse* sulla radice del sito *Web* e scegliere Proprietà dal menu di scelta rapida.
- Fare clic sulla scheda *Home directory*.
- Fare clic su Configurazione.
- Fare clic sulla scheda Opzioni **applicazione**.
- Deselezionare la casella di controllo Abilita percorsi principali.

Usare e valutare i risultati di uno strumento di memorizzazione delle visite al sito

Per controllare eventuali danni causati da utenti malintenzionati, bisogna tener traccia delle visite al sito. Ciò è realizzato attraverso i *file* di *log*. In questa sezione continuiamo ancora ad occuparci di *Microsoft* IIS.

***File* di *log* in *Microsoft* IIS**

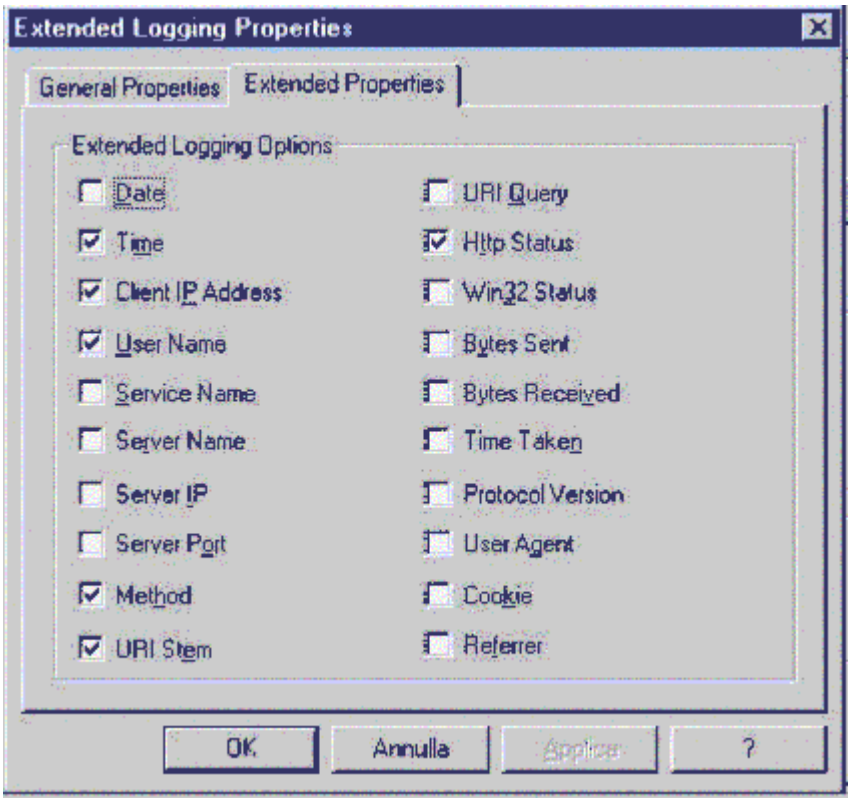
Le operazioni di registrazione relative a un sito *Web* o FTP vengono svolte da moduli che operano indipendentemente dalle altre attività del ***server***. È possibile scegliere il formato dei registri per ogni sito *Web* o FTP. Se si attiva la registrazione a livello di sito, è comunque possibile disattivarla per singole *directory*.



I registri creati da IIS possono essere letti con un *editor* di testo, ma in genere si preferisce caricare i *file* in un programma per la creazione di rapporti. I dati raccolti con la registrazione ODBC vengono registrati in un *database*, da cui è possibile generare rapporti, mentre i registri di conteggio dei processi vengono creati insieme ai normali registri W3C estesi per ogni sito *Web*.

I formati di registrazione utilizzano fusi orari diversi per la registrazione degli orari. Il formato di registrazione W3C esteso utilizza l'orario UTC (*Universal Time Coordinate*), precedentemente noto come GMT (*Greenwich Mean Time*). Gli altri formati utilizzano orari locali. Gli orari riportati nei *file* registro indicano il tempo impiegato dal ***server*** per elaborare richieste e risposte, escluso il tempo impiegato dai dati per arrivare al *client* e il tempo impiegato dal *client* per elaborare i dati.

Il *folder Extended Properties*, permette di scegliere gli obiettivi che dovranno essere monitorati dal LOG. La grandezza dei *file* di *Log* sarà proporzionale al numero di opzioni selezionate. È possibile indicare nel *file* di *Log* i campi che vorremmo vedere. Questo argomento sarà trattato diffusamente in seguito.



La parte relativa alla generazione dei LOG, è molto importante da valutare. Infatti la mancata osservanza di alcune regole fondamentali potrebbe portare a creare dei *file* di LOG da qualche *Gigabyte*. Abilitando il LOG (ricordiamo che per *default* è abilitato), ogni richiesta effettuata al ***server*** (anche quelle che non hanno esito e quelle errate) verranno registrate. Dal più semplice LOG di testo, al formato *Microsoft*, fino a W3C che è un formato esteso di *Logging* che permette la personalizzazione degli obbiettivi da monitorare. Il LOG però assorbe risorse dal ***server***, è quindi consigliata l'attivazione solo quando se ne ritiene fondamentale il suo uso. Nelle proprietà del *Logging* è possibile stabilire se deve essere: Giornaliero Settimanale Mensile Illimitato (Sconsigliatissimo) personalizzato nella grandezza. È possibile stabilire in quale *directory* dovrà essere contenuto (*default* `WINNT/SYSTEM32/LogFiles`).

Formati dei file registro

È possibile scegliere il formato utilizzato dal *server Web* per registrare l'attività dell'utente. Sono disponibili i seguenti formati:

- Formato Registrazione W3C estesa.
- Formato Registrazione *Microsoft* IIS.
- Formato Registrazione comune NCSA.
- Registrazione ODBC.

I formati Registrazione W3C estesa, *Microsoft* IIS e NCSA sono formati di testo ASCII. I formati Registrazione W3C estesa e NCSA registrano le informazioni sugli anni in un formato a quattro cifre, mentre il formato *Microsoft* IIS utilizza per gli anni un formato a due cifre ed è compatibile con le versioni precedenti di IIS. È inoltre possibile creare formati di registrazione personalizzati che prevedano esclusivamente i campi di interesse.

Formato Registrazione W3C estesa

Il formato Registrazione W3C estesa è un formato ASCII personalizzabile che include numerosi campi. È possibile scegliere i campi di interesse e omettere quelli non desiderati, così da limitare le

dimensioni del registro. I campi sono separati da spazi. Gli orari vengono registrati in formato UTC (*Universal Time Coordinate*). Per informazioni sulla personalizzazione di questo formato, vedere Personalizzazione della registrazione W3C estesa. Per ulteriori informazioni sulla specifica alla base della registrazione W3C estesa, vedere il sito di W3C all'indirizzo http://www.w3.org (informazioni in lingua inglese).

Nell'esempio che segue vengono riportate alcune righe da un *file* per il quale sono stati scelti i campi: Ora, Indirizzo IP *client*, Metodo, Origine URI, Stato HTTP e Versione HTTP.

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0 #Date: 1998-05-02 17:42:15
#Fields: time c-ip cs-method cs-uri-stem sc-status cs-version 17.42.15
172.16.255.255 GET /default.htm 200 HTTP/1.0
```

Queste voci indicano che il 2 maggio 1998 alle ore 17.42 (ora UTC) un utente con HTTP versione 1.0 e indirizzo IP 172.16.255.255 ha eseguito un comando HTTP *GET* per il *file Default.htm*. La richiesta è stata soddisfatta senza errori. Il campo *#Date:* indica quando è avvenuta la registrazione della prima voce, ovvero quando è stato creato il registro. Il campo *#Version:* indica che è stato utilizzato il formato di registrazione W3C.

È possibile selezionare qualsiasi campo, ma alcuni potrebbero non contenere informazioni per alcune richieste. Nei campi selezionati che non presentano informazioni registrabili viene visualizzato un trattino (-).

Formato Registrazione Microsoft IIS

Il formato di registrazione *Microsoft* IIS è un formato ASCII fisso, non personalizzabile, in grado di registrare più informazioni rispetto al formato Registrazione comune NCSA. Include elementi di base, quali l'indirizzo IP e il nome dell'utente, la data e l'ora della richiesta, il codice di stato HTTP e il numero di *byte* ricevuti, nonché elementi dettagliati, quali il tempo trascorso, il numero di *byte* inviati, l'azione, ad esempio un processo di scaricamento eseguito tramite un comando *GET*, e il *file* di destinazione. I vari elementi sono separati da virgole, e questo semplifica la lettura di tale formato rispetto agli altri formati ASCII che utilizzano gli spazi come separatori. L'ora viene registrata in base al fuso orario locale.

Quando si apre un *file* registro in formato *Microsoft* IIS con un *editor* di testo, le voci in esso contenute risulteranno simili a quelle riportate negli esempi seguenti:

```
&gt; 192.168.114.201,-, 20/03/98, 7.55.20, W3SVC2, VENDITE1, 192.168.114.201,
4502, 163, 3223, 200, 0, GET, LogoDip.gif 172.16.255.255, anonymous, 20/03/98,
23.58.11, MSFTPSVC, VENDITE1, 192.168.114.201, 60, 275, 0, 0, 0, PASS, intro.htm
```

Le voci dell'esempio precedente vengono spiegate nelle tabelle riportate di seguito. La prima riga di entrambe le tabelle deriva dalla seconda istanza del sito *Web* (che appare nella sezione Servizio come W3SVC2). L'ultima riga deriva dalla prima istanza del sito FTP (che appare nella sezione Servizio come MSFTPSVC1). Per motivi legati alla larghezza della pagina, è stato necessario utilizzare due tabelle per descrivere l'esempio.

Indirizzo IP dell'utente	Nome utente	Data	Ora	Servizio e istanza	Nome del *computer*	Indirizzo IP del *server*
192.168.114.201	-	03/20/98	7:55:20	W3SVC2	VENDITE1	172.21.13.45
172.16.255.255	anonimo	03/20/98	23:58:11	MSFTPSVC1	VENDITE1	172.21.13.45

Tempo	*Byte* ricevuti	*Byte* inviati	Codice dello stato del servizio	Codice dello stato di *Win* 2000	Tipo di richiesta	Destinazione dell'operazione
4502	163	3223	200	0	*GET*	LogoDip.gif
60	275	0	0	0	[376] PASS	intro

Nell'esempio precedente, la prima voce indica che alle ore 7.55 del giorno 20 marzo 1998 un utente anonimo con indirizzo IP 102.168.114.201 ha eseguito un comando HTTP *GET* per scaricare il *file* immagine LogoDip.gif da un ***server*** chiamato VENDITE1 con indirizzo IP 172.21.13.45. Il tempo di elaborazione necessario per completare questa richiesta HTTP di 163 *byte* è stato di 4502 millisecondi, ovvero 4,5 secondi. All'utente anonimo sono stati restituiti 3223 *byte* di dati, senza errori. Tutti i campi presenti nel *file* registro terminano con una virgola (,). Eventuali trattini vengono utilizzati come segnaposto per indicare la non disponibilità di un valore valido per il campo.

Formato Registrazione comune NCSA

Il formato Registrazione comune NCSA è un formato ASCII fisso, non personalizzabile, disponibile per i siti *Web*, ma non per i siti FTP. Registra le informazioni di base relative alle richieste degli utenti, ad esempio il nome dell'*host* remoto, il nome utente, la data, l'ora e il tipo di richiesta, il codice di stato HTTP e il numero di *byte* ricevuti dal ***server***. Le voci sono separate da spazi e l'ora viene registrata in base al fuso orario locale. Quando si apre un *file* registro in formato comune NCSA con un *editor* di testo, le voci in esso contenute risulteranno simili a quelle riportate nell'esempio seguente:

```
172.21.13.45- ROMA\pippo [08/Apr/1998.17.39.04 -0800]
GET /script/iisadmin/ism.dll?http/serv HTTP/1.0 200 3401
```

Nella voce precedente, il secondo campo, che dovrebbe contenere il nome del registro remoto dell'utente, è vuoto ed è rappresentato dal trattino che segue l'indirizzo IP 172.21.13.45. Questa voce viene interpretata nelle tabelle seguenti. Per motivi legati alla larghezza della pagina, è stato necessario utilizzare due tabelle per illustrare l'esempio.

Nome dell'*host* remoto	Nome utente	Data	Ora e differenza GMT
172.21.13.45	ROMA\sergio	08/Apr/1998	17:39:10 -0800

Tipo di richiesta	Stato del servizio	*Byte* inviati
`GET /script/iisadmin/ism.dll?http/serv HTTP/1.0`	200	3401

La voce precedente indica che alle ore 17.39 dell'8 aprile 1998 l'utente Sergio appartenente al dominio ROMA, con indirizzo IP 172.21.13.45, ha eseguito un comando HTTP *GET* per scaricare un *file*. All'utente sono stati restituiti, senza errori, 3401 *byte* di dati.

Formato Registrazione ODBC

Il formato di registrazione ODBC registra una serie di campi di dati fissi in un *database* ODBC. L'ora viene registrata in base al fuso orario locale. Se si sceglie questo formato di registrazione è necessario specificare e configurare il *database* in cui registrare i dati. Per utilizzare la registrazione ODBC è necessario procedere come indicato di seguito:

- Creare un *database* contenente una tabella con i campi necessari per la registrazione delle

informazioni. In IIS è disponibile un *file* modello SQL che può essere eseguito in un *database* SQL per creare una tabella predisposta per la registrazione dei dati di IIS. Il *file* si chiama Logtemp.sql, nella *directory* `\IISRoot`. Se durante l'installazione sono state confermate le impostazioni predefinite, la *directory* `\IISRoot` è una sotto*directory* di `\WindowsNT\System32`. I campi obbligatori sono:

Nome campo	Tipo campo
ClientHost	*Varchar*(255)
Username	*Varchar*(255)
LogTime	*datetime*
Service	*Varchar*(255)
Machine	*Varchar*(255)
ServerIP	*Varchar*(50)
ProcessingTime	*int*
BytesRecvd	*int*
BytesSent	*int*
ServiceStatus	*int*
Win32Status	*int*
Operation	*Varchar*(255)
Target	*Varchar*(255)
Parameters	*Varchar*(255)

- Assegnare al *database* un nome DSN (*Data Source Name*), che verrà utilizzato dal *software* ODBC per trovare il *database*.
- In IIS specificare il nome del *database* e della tabella.

Conteggio dei processi e nomi dei file registro

Conteggio dei processi: È una nuova funzione di IIS e aggiunge campi al *file* registro in formato W3C esteso allo scopo di registrare informazioni sull'utilizzo delle risorse della *CPU* del ***server*** da parte dei siti *Web*. Queste informazioni vengono quindi utilizzate per stabilire se i siti impiegano eccessive risorse della *CPU* o per rilevare *script* o processi *CGI* che non funzionano in modo corretto. Il conteggio dei processi può essere attivato a livello di sito. Non fornisce dettagli sull'utilizzo della *CPU* da parte delle singole applicazioni; infatti, registra le informazioni relative solo alle applicazioni *out-of-process*. È disponibile solo per i siti *Web* e viene registrato solo se è selezionato il formato di registrazione W3C estesa. I dati relativi al conteggio dei processi vengono registrati nel *file* insieme agli altri dati. Le informazioni raccolte durante il conteggio dei processi possono essere utilizzate per decidere se attivare o meno la limitazione dei processi in un sito *Web*, ovvero se definire limiti per il tempo del processore utilizzato da un sito.

Nomi dei *file* registro: Le prime lettere dei nomi dei *file* registro indicano il formato di registrazione mentre i restanti numeri indicano la sequenza o l'intervallo temporale di creazione dei *file*. Nella tabella riportata di seguito vengono fornite informazioni più dettagliate. Le lettere in corsivo rappresentano cifre: *nn* indica cifre sequenziali, mentre *aa* indica l'anno, *mm* il mese, *ss* la settimana del mese, *gg* il giorno e *hh* l'ora nel formato 24 ore.

Formato	Criterio di creazione dei nuovi *file* registro	Modello del nome di *file*
	In base alle dimensioni del *file*	**inetsv***nn***.log**

Registrazione *Microsoft* IIS	Ogni ora	**in***aammgghh***.log**
	Ogni giorno	**in***aammgg***.log**
	Ogni settimana	**in***aammss***.log**
	Ogni mese	**in***aamm***.log**
	In base alle dimensioni del *file*	**ncsa***nn***.log**
Registrazione comune NCSA	Ogni ora	**nc***aammgghh***.log**
	Ogni giorno	**nc***aammgg***.log**
	Ogni settimana	**nc***aammss***.log**
	Ogni mese	**nc***aamm***.log**
	In base alle dimensioni del *file*	**extend***nn***.log**
Registrazione W3C estesa	Ogni ora	**ex***aammgghh***.log**
	Ogni giorno	**ex***aammgg***.log**
	Ogni settimana	**ex***aammss***.log**
	Ogni mese	**ex***aamm***.log**