Microsoft IIS

Internet Information Services (IIS)

Lezione 5

https://www.gabrieledelgiovine.it

Microsoft IIS

Internet Information Services (IIS)

Lezione 5

Nella Lezione 5:

- Metteremo in pratica tutto quello che abbiamo imparato sinora!

LABORATORIO:

- Recupero delle informazioni e requisiti sul sito:
  - IIS accessibile da reti non trusted?
  - IIS Server come member server in Active Directory?
  - Requisiti di sicurezza relativi all’accesso ulteriori?
  - Verifica dei moduli installati
  - Versioni di ASP.NET presenti
  - Meccanismi di autenticazione
  - Utenti per Application Pool
  - Configurazioni Application Pool
  - Indirizzi IP, Porte e Nomi per il Binding
  - Certificati SSL
  - Directory/Share di rete e relativi utenti
  - Connection Strings verso DB SQLServer
  - Documentazione da parte degli sviluppatori
  - Modalita e livelli di logging

LABORATORIO:

- Attività di deployment:
  - Creazione degli utenti per Application Pool nella sicurezza locale del server e/o Active Directory
  - Creazione delle cartelle per sito e virtual directory e delle identità di accesso ad eventuali Share di rete
  - Verifica dell'effettivo accesso alle cartelle fisiche con le identità predisposte
  - Verifica dei nomi DNS da usare
  - Verifica eventuali certificati SSL da usare
  - Verifica raggiungibilità risorse esterne ad IIS usate dal sito (Esempio uso dei files UDL per la verifica di accesso al DB)
  - Se si usano ASP.NET Providers verificarne la configurazione con gli sviluppatori
  - Verificare con gli sviluppatori i Trust level richiesti dall'applicazione

LABORATORIO:

- Attività di deployment:
  - Creazione dell'Application Pool
  - Creazione del sito
  - Associazione dei binding
  - Impostazione delle modalità di logging
  - Impostazione iniziale per accesso anomino
  - Creazione di due semplici pagine per verifica funzionalità HTML ed ASP.NET: test.html e test.aspx
  - Verifica di raggiungibilità e funzionamento delle due pagine di test
  - Verifica dell'effettivo funzionamento del logging
  - Impostazione di eventuali restrizioni IP richieste e verifica del loro funzionamento

LABORATORIO:

- Attività di deployment:
  - Copia dei files constituenti l'applicazione
  - Impostazione del Web.Config per ogni applicazione presente nel Web Site. *Tenere presente le modalità di informazione degli errori HTTP 400 e 500 all'utente*.
  - Verifica dei parametri di configurazione del Web.Config con la documentazione fornita dagli sviluppatori
  - Verifica della presenza delle pagine di login previste e definite nella configurazione in Web.Config quando viene usata la FORMS AUTHENTICATION
  - Impostare i documenti di default (default.aspx ecc.) richiesti dall'applicazione per l'avvio

LABORATORIO:

- Attività di post deployment – Test Applicazione
  - Avviare l’applicazione e verificarne il comportamento e la presenza di pagine di errore HTTP 400 e 500
  - In caso di malfunzionamenti segnalati con errori HTTP 400 verificare la correttezza delle URL richieste, la presenza fisica dei files nelle cartelle, la coerenza dei permessi di accesso, regole di filtraggio ecc…
  - In caso di malfunzionamenti segnalati con errori HTTP 500 verificare le registrazioni di REQUEST TRACING e MONITORING

LABORATORIO:

- Attività di post deployment – Mantenimento
  - Monitorare periodicamente i log HTTP ed eventuali FAILED REQUEST TRACING
    - Usate possibilmente dei tools di analisi dei log. Sono elementi importanti da tracciare gli errori 401, 403 legati all'autenticazione e 404 legati all'inesistenza della risorsa che potrebbero essere indicatori di tentativi di accesso non autorizzato e/o ricerca di vulnerabilità.
  - Monitorare periodicamente i log proprio delle applicazioni predisposti dagli sviluppatori
  - Impostare le politiche di Riciclo automatico degli Application Pool per preservare/mitigare problematiche di memory leak delle applicazioni, eccessivi errori o eccessivo uso di CPU.

IIS, l'HA (High Avalaibility Alta Disponibilit), la Scalabilità e l'Affidabilità

HA (Alta Disponibilità), Scalabilità e Affidabilità sono tre concetti distinti

- HA = Elevata disponibilità del servizio nella dimensione temporale. È la capacità del servizio di rispondere correttamente alle richieste in un arco temporale.
- Scalabilità = capacità del sistema variare il tempo di esecuzione di un compito in funzione delle risorse di elaborazione dedicate all'esecuzione dello specifico compito. Se aumentando le risorse e facendo rimanere costante il numero di compiti, il tempo di esecuzione complessivo dei compiti diminuisce il sistema è intrinsecamente scalabile.
- Affidabilità = È il rapporto fra il totale di richieste di esecuzione di compiti ricevute e il numero di richieste portate a termine con successo. Non coinvolge solo gli aspetti di pura potenza di calcolo ma anche quelli degli algoritmi e la qualità del codice che li implementa.

IIS, l'HA (High Avalaibility Alta Disponibilit), la Scalabilità e l'Affidabilità

HA (Alta Disponibilità), Scalabilità e Affidabilità sono tre concetti distinti

- Esistono quindi delle relazioni fra HA, Scalabilità ed Affidabilità.
- Un sistema che non incrementa la capacità di elaborazione corretta all'incrementare delle risorse di elaborazione (quindi non Scalabile) può ad esempio essere considerato Affidabile a bassi regimi di richieste ma Inaffidabile ad alti regimi di lavoro.
- Un sistema basato su unica unità di elaborazione che ha bisogno di frequenti riavvi per problemi di consumo di memoria , anche se scalabile tramite aggiunta di risorse (es. CPU e Memoria) non può essere considerato nè ad Alta Disponibilità né Affidabile.

IIS, l'HA (High Avalaibility Alta Disponibilit), la Scalabilità e l'Affidabilità

HA (Alta Disponibilità), Scalabilità e Affidabilità sono tre concetti distinti: Quale dobbiamo perseguire in maniera prioritaria?

- L'Affidabilità. Una volta definiti i livelli di servizio in termini di numero compiti da portare a termine correttamente in un arco temporale tale obiettivo viene raggiunto modulando le tecnologie che assicurano l'Affidabilità con quelle che assicurano Alta Disponibilità e Scalabilità.
- Se i nostri algoritmi sono sbagliati o usiamo infrastrutture instabili l'HA e Scalabilità avranno solo l'effetto di assicurarci sempre l'errore di calcolo e la quantità di errori di calcolo.

IIS, l'HA (High Avalaibility Alta Disponibilit), la Scalabilità e l'Affidabilità

La Scalabilità e le sue dimensioni

- La scalabilità si basa su una caratteristica dei sistemi di elaborazione: la capacità dei singoli processi di «collaborare» fra di loro quando resi capaci di comunicare l'uno con l'altro oppure coordinati da un processo coordinatore. Tale capacità può essere estesa fra sistemi fisici diversi quando esiste un qualche canale di comunicazione fra i sistemi (la rete locale)
- Osservando quindi i contesti di comunicazione possiamo avere contesti «verticali-singoli» e contesti «orizzontali-multipli»
  - Verticali = singola entità-sistema che esegue i compiti
  - Orizzontali = più entità-sistemi che eseguono compiti suddividendosi i singoli compiti tramite qualche forma di coordinamento (comunicazione).

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

La Scalabilità e le sue dimensioni

- Possiamo quindi affermare che
  - La Scalabilità Verticale è quella legata alla capacità di espansione del singolo computer in termini di processori (potenza e numero), memoria RAM, meria di massa e canali di comunicazione. Raggiunto il quantitativo massimo di ognuna delle risorse il sistema non può più incrementare la sua capacità di elaborazione.
  - La Scalabilità Orizzontale è quella legata al fatto che possiamo far eseguire l'insieme dei compiti suddividendoli in sottoinsiemi assegnati a distinte unità fisiche di elaborazione, gestendo in qualche maniera l'assegnazione del singolo compito alla singola unità fisica di elaborazione. La Scalabilità Orizzontale non ha teoricamente limiti relativamente alla quantità di compiti da portare a termine in un dato arco temporale: basta aumentare i sistemi fisici. In teoria.

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

Come ottenere l'HA Alta Disponibilità in IIS

- Il metodo più semplice è quello di utilizzare la funzionalità di Microsoft Failover Cluster Services (MFCS)
- Si tratta di una Feature di Windows Server e fornisce il supporto alla gestione di famiglie di servizi di Windows coordinandone l'esecuzione Attiva-Passiva fra almeno DUE nodi (l'insieme dei nodi si chiama Cluster) assicurando che almeno uno dei nodi abbia attivo quel servizio in un dato istante. Se il nodo attivo viene spento il servizio verrà attivato su uno degli altri nodi.
- Ogni nodo del «cluster» richiede l'installazione del servizio/ruolo monitorato dal «cluster» ed ovviamente la medesima configurazione e l'accesso ai medesimi dati. In sostanza ogni nodo ha una copia delle cose che deve gestire (poi vedremo come la copia fisica in realtà non sia necessaria).
- Nella sostanza MFCS crea un indirizzo IP Comune usato da tutti i nodi del cluster ed associa a tale indirizzo la raggiungibilità di un insieme di servizi, fra i quali nel nostro caso IIS. In un determinato istante un IP è gestito da un nodo. Questo perché il cluster MFCS è un cluster «shared-nothing»

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

Come ottenere l'HA Alta Disponibilità in IIS

- Il metodo più semplice è quello di utilizzare la funzionalità di Microsoft Failover Cluster Services (MFCS)
- Come potete intuire MFCS, anche se composto da N nodi non fornisce Scalabilità orizzontale al singolo sito IIS. Quel sito verrà servito sempre solo da un IIS.
- MFCS fornisce solo HA, sarebbe a dire ci garantisce che comunque per la maggior parte del tempo avremo quel sito IIS funzionante o per lo meno capace di ricevere richieste.

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

Come ottenere l'HA Alta Disponibilità in IIS

- Nel mondo reale l'uso di MFCS per clusterizzare IIS è molto raro.
- La tecnica comunemente usata è quella del Cluster NLB.
- Cluster NLB racchiude un insieme eterogeneo di strumenti anche molto diversi fra di loro, accomunati da un obiettivo comune: distribuire richieste di connessioni IP (TCP/UDP) verso un nome/indirizzo IP fra più macchine con indirizzi IP diversi da quello originariamente richiesto.

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

Come ottenere l'HA Alta Disponibilità in IIS

- Il mondo degli NLB
- La forma più semplice di NLB è un DNS server con dei records HOST con lo stesso nome host ma indirizzi IP diversi. Il DNS server fornirà per quel nome hosto prima il primo IP, poi l'IP successivo e cosi via a rotazione (round robin)
- I Server NLB veri e propri gestiscono logiche aggiuntive che prevedono logiche di controllo, autenticazione, ispezione dei pacchetti, gestione delle destinazioni ecc. ecc. ecc.
- Spesso le funzionalità di Server NLB (Load Balancer) sono inglobate dentro a sistemi integrati (Appliances) che offrono la gestione estesa dei vari servizi di rete (Firewall, NAT, DNS, Proxy, NLB, VPN ecc. ecc.)

IIS, l’HA (High Avalaibility Alta Disponibilità), la Scalabilità e l’Affidabilità

Come ottenere l’HA Alta Disponibilità in IIS

- Il mondo degli NLB
- Windows ha la sua features di Cluster NLB (Network Load Balancing) che permette di creare un Cluster NLB composto da nodi Windows Server. Può essere una soluzione per creare un Load Balancer che include tutti i server IIS che vogliamo usare nel nostro Cluster NLB.
- Windows NLB non è la soluzione migliore per assicurare la scalabilità a siti IIS. Manca infatti di tutta una serie di strumenti di diagnostica idonei a gestire il cluster dato che l’unico controllo che può fare è che su nodo cluster la combinazione IP clusterizzato/porta TCP/UDP sia operativa. Capite che quando usiamo i Binding Host Name di IIS Windows NLB non ci da nessun aiuto, anzi ci rende la vita ancora più difficile.

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

Come ottenere l'HA Alta Disponibilità in IIS

- Il mondo degli NLB
- Perché ho bisogno di strumenti di diagnostica dello stato del singolo IIS Web Site quando uso NLB?
  - Perché a differenza di MFCS (dove in realtà IIS che funziona ne è sempre solo uno) bilancio il carico di lavoro fra tutti i nodi e pertanto il bilanciatore deve sapere che QUEL sito o che QUELLA parte di QUEL sito funzione e funziona correttamente (es. QUEL nodo del cluster riesce a parlare con il DB?). L'obiettivo è evitare di instradare la richiesta verso un nodo che poi non è in grado di servire per qualsiasi motivo la richiesta.

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

Come ottenere l'HA Alta Disponibilità in IIS

- Il mondo degli NLB
- Quali sono i parametri di diagnostica dello stato del singolo IIS Web Site quando uso NLB?
  - I più svariati, Il numero di utenti già collegati a quel server, la quantità di RAM usata, la CPU impegnata, il fatto che il server acceda ad uno share di rete o ad un DB, il numero di licenze consumate dall'applicativo.
  - I bilanciatori di carico possono usare delle API per farsi dare dai vari server i dati di carico di lavoro generico e/o delegare nel caso di server WEB l'uso di speciali pagine di diagnostica scritte dagli sviluppatori, pagine che internamente fanno i test del caso e rispondono con un HTTP 200 (OK) o con un Json/text….

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

Come ottenere l'HA Alta Disponibilità in IIS

- Il mondo degli NLB. Quali sono gli NLB (Load Balancer) più usati?
  - F5 BIG-IP, RADWARE, Citrix ADC, KEMP, AWS Elastic LB, BARRACUDA, HA-PROXY e tanti tanti altri.
  - Tenete presente che tutti questi oggetti sono ANCHE dei Reverse Proxy.
  - Se avete la necessità di implementare un NLB efficace per i vostri IIS e non avete un NLB già esistente nella vostra LAN due consigli:
    - pfSense 2.7.0 Community con HA-PROXY. Nessun intervento su Windows e IIS.
    - Il modulo opzionale di IIS: ARR (Application Routing Request) https://www.iis.net/downloads/microsoft/application-request-routing Pesanti azioni di configurazione in IIS
  - NOTA: OGNI SISTEMA DI NLB ha la sua procedura/metodo per attivare la funzionalità.

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

- E la Scalabilita Orizzontale?
  - Usando un NLB come quelli indicati precedentemente otterrete anche la Scalabilità Orizzontale.
- E l'Affidabilità?
  - Qui entrano in gioco gli sviluppatori per quanto riguarda la qualità del codice delle Applicazioni Web.
  - Voi come sistemisti dovete applicare la vostra buona diligenza per non aggiungere ai bug delle applicazione ulteriori malfunzionamenti dovuti ad errate configurazioni di IIS.

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

- OK, ora abbiamo HA e Scalabilità (e speriamo Affidabilità). Ma che debbo fare su IIS per eliminare tutti i possibili Single Point-Of-Failure (SPOF)?
- Avere a monte dei nostri IIS un sistema NLB in effetti è solo una parte della soluzione. Abbiamo ancora tutta una serie di SPOF. Quali?
  - La configurazione dei siti Web
  - I files che contengono le risorse
  - La locazione dei files che contengono le risorse
  - I meccanismi di gestione della Sessione
  - Le trappole dell'Affinità di Sessione introdotte dai vari NLB
- Vediamo questi problemi e come risolverli o mitigarli.

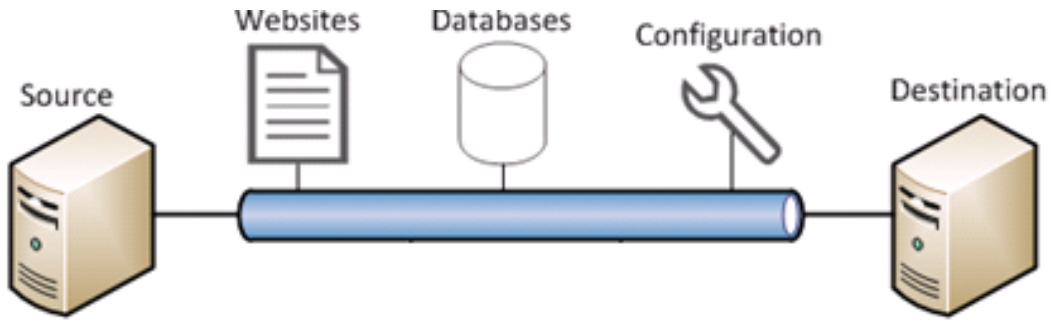
IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità
SPOF: La configurazione ed i Contenuti dei siti Web

- I siti inclusi in un sistema di NLB debbono avere accesso alle medesime configurazioni in termini di sistemi di autenticazione, gestione dello stato di sessione, servizi esterni (es. Database) e configurazioni applicative specifiche.
- Inoltre debbono accedere agli stessi contenuti statici ed eseguibili delle applicazioni web.
- Queste operazioni possono essere fatte in maniera totalmente manuale, parzialmente manuale/scriptata (AppCmd/PowerShell) o usando tools specifici di sincronizzazione delle configurazioni e dei contenuti.
- Relativamente ai contenti questi potrebbero anche NON richiedere sincronizzazione se posizionati in Virtual Directory mappate su Share di Rete (ovviamente anche loro in HA)
- IIS ci mette a disposizione una Estensione chiamata IIS WEB DEPLOY https://www.iis.net/downloads/microsoft/web-deploy

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

SPOF: La configurazione dei siti Web – IIS WEB DEPLOY

- IIS Web Deploy è uno strumento client-server estendibile per la sincronizzazione del contenuto e della configurazione in IIS. La distribuzione Web viene usata principalmente in due scenari:
- Gli sviluppatori lo usano per sincronizzare (ovvero "pubblica") applicazioni Web compilate (ASP .Net, PHP e così via) da strumenti di sviluppo (Visual Studio, WebMatrix e così via) a IIS
- I professionisti IT lo usano per eseguire la distribuzione fra servers o la migrazione di applicazioni Web & da un sistema operativo che esegue una versione precedente di IIS a un sistema operativo che esegue una versione più recente di IIS



IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

SPOF: La configurazione dei siti Web – IIS WEB DEPLOY

- IIS WEB DEPLOY COPIA I CONTENUTI e LA CONFIGURAZIONE DI UNO O PIU' SITI DA UN SERVER MASTER VERSO I SERVER DI DEPLOY.
- Non confondete la cosa con quello che fa la feature «Shared Configuration» che trovate a livello di gestione del Server IIS.
- Shared Configuration serve a condividire/copiare LA CONFIGURAZIONE DI IIS (di tutto IIS) da un server all'altro!!! Non copia i contenuti…

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

SPOF I meccanismi di gestione della Sessione

- Abbiamo già trattato questo argomento ma fa sempre bene tenerlo presente:
  - Quando siamo in NLB in teoria ogni singola richiesta potrebbe essere servita da uno qualsiasi dei server IIS inclusi nel meccanismo di NLB per quel sito
  - Se l'applicazione usa Session per memorizzare lo stato di una pagina fra una chiamata e l'altra queste informazioni non possiamo usare un meccanismo di gestione della Sessione che memorizzi tali informazioni nella memoria del W3WP.EXE associato all'Application Pool, semplicemente per il fatto che tale memoria non può essere condivisa fra i server IIS.
  - L'applicazione deve quindi usare uno dei provider di Session che memorizza tali dati su «cose» che possono essere accedute da TUTTI i server inclusi nel cluster NLB:
  - Queste «cose» sono gli state server di IIS o il server state basato su SQLServer o qualsiasi altra cosa che implementi le interfacce di Session

IIS, l’HA (High Avalaibility Alta Disponibilità), la Scalabilità e l’Affidabilità

SPOF I meccanismi di gestione della Sessione - ViewState

- Dei problemi si possono avere anche quando l’applicazione NON usa Session ma usa ViewState di ASP.NET, che è un meccanismo per cui si emula Session (o almeno una sua parte) memorizzando queste informazioni non sul server ma DENTRO la pagina HTML ospitata dal browser.
- Ne abbiamo già parlato nella lezione dedicata al troubleshooting. Per evitare problemi di sicurezza le informazioni del ViewState viene crittografato.
- Quando siamo in NLB è importante che la chiave di crittografia usata sia uguale per tutti i server, perché altrimenti il server che riceva la richiesta potrebbe non decrittare il ViewState ricevuto con la richiesta.

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

SPOF I meccanismi di gestione della Sessione
Le trappole dell'Affinità di Client/Sessione introdotte dai vari NLB

- Ci sono casi per cui non è possibile usare un sistema di gestione della sessione che memorizzi le cose dentro W3WP.EXE.
- Molti framework di sviluppo richiedono la Sessione gestita nel modo di default perché altrimenti perderebbero troppo tempo a recuperare tali dati. Quasi tutti i framework moderni che usano WebSocket, gRPC, il rendering parziale delle pagine e dei widget JavaScript funzionano in questa maniera.
- Dovete chiedere agli sviluppatori.

IIS, l'HA (High Avalaibility Alta Disponibilità), la Scalabilità e l'Affidabilità

SPOF I meccanismi di gestione della Sessione

Le trappole dell'Affinità di Client/Sessione introdotte dai vari NLB

- A prima vista questo sembrerebbe rendere impossibile la scalabilità orizzontale delle Web Application tramite NLB dato che una richiesta potrebbe essere servita da uno qualsiasi dei server in NLB, server che quasi sicuramente non avrà i dati di Sessione corretti o non li avrà proprio.
- I sistemi di NLB ci risolvono parzialmente questo problema introducendo il concetto di «Affinità di Sessione»

IIS, l’HA (High Avalaibility Alta Disponibilità), la Scalabilità e l’Affidabilità

SPOF I meccanismi di gestione della Sessione
Le trappole dell’Affinità di Client/Sessione introdotte dai vari NLB

- Cos’è «l’Affinità di Client/Sessione»?
- È il criterio per il quale un NLB assegna una richiesta ad uno dei server che può elaborarla.
- Noi sappiamo che la prima volta che viene chiesta una risorsa URL da un client HTTP il client presenta il suo IP ed il suo identificativo univoco.
- Quando il server NLB viene istruito ad usare il criterio di Affinità di Sessione di tipo «Sticky» il server NLB dirigerà tutte le richieste di quel client HTTP al server verso cui ha diretto la prima richiesta.

SPOF I meccanismi di gestione della Sessione

Le trappole dell’Affinità di Client/Sessione introdotte dai vari NLB

- Questo criterio ci permette quindi di usare le nostre applicazioni rinunciando alla totale scalabilità orizzontale (da qui la trappola), rendendo applicabile tale criterio SOLO al primo contatto fra Client HTTP e server NLB.
- Inoltre se durante la vita del Client HTTP il server assegnato dall’NLB dovesse essere indisponibile avremo anche una ripercussione sull’Affidabilità perché avremmo un errore e l’utente/Client dovrà ricominciare da capo l’attività.

Microsoft IIS

Internet Information Services (IIS)

Fine della Lezione 5

Nelle Lezioni 6 e 7:

- IIS Come FTP Server
- IIS URL Rewrite
- IIS ARR Application Routing Request
- IIS CORS Module
- IIS.NET ed i componenti aggiuntivi sviluppati da Microsoft e da terze parti
- Il Component Server e quando usarlo