

## Aprire le applicazioni Mainframe alle SOA e agli ambienti distribuiti

Modernizzare le applicazioni Mainframe aprendole alle architetture SOA e all'uso dei servizi Web può esser fatto seguendo vari approcci, ciascuno dei quali ha i suoi pro e contro.

---

### INDICE

Definizione degli Stati .....	1
Gestione delle sessioni Mainframe come servizi .....	1
Orientarsi tra le varie alternative .....	4
Come procedere .....	5
Il ruolo di Verastream.....	5
Attachmate .....	5

---

# Aprire le applicazioni Mainframe alle SOA e agli ambienti distribuiti

Modernizzare le applicazioni Mainframe aprendole alle architetture SOA e all'uso dei servizi Web può esser fatto seguendo vari approcci, ciascuno dei quali ha i suoi pro e contro.

Innovare, puntando a risultati valutabili in riduzioni dei costi o incrementi di vantaggio competitivo è sempre importante, specie nei periodi di crisi. In tal senso, le applicazioni Mainframe offrono un'ampia gamma di possibilità, consentendo di migliorare i servizi agli utenti o di ridurre i costi di gestione dei sistemi. Occorre però poter contare su azioni che garantiscano ridotti tempi di intervento e ritorno, con bassi rischi.

Indubbiamente, l'adozione delle SOA (Service Oriented Architecture) costituisce un buon passo in avanti per tutte le aziende che oggi basano i propri sistemi sui tradizionali Mainframe, ma quando si inizia a considerare come procedere nella trasformazione in servizi delle applicazioni Legacy esistenti occorre valutare dal punto di vista tecnico come mantenerne l'integrità e garantirne la necessaria sicurezza.

Dal punto di vista del Mainframe, gli utenti di qualsiasi applicazione sono di fatto utenti di sessioni che si svolgono sul Mainframe, indipendentemente da come vengono accedute o attivate. Di conseguenza, dal momento che il mondo Mainframe partiva dal presupposto che gli accessi ai sistemi fossero ben protetti e controllati prima dell'inizio di qualsiasi sessione, per garantire gli stessi livelli di sicurezza del passato serve poter disporre di un affidabile sistema di autenticazione degli utenti e della capacità di tracciare con precisione chi, quando e per fare cosa è entrato nel sistema, considerando che a farlo possono essere stati "servizi" attivati da ovunque sulla rete e non solo da utenti fisici, ma potenzialmente anche da altri servizi.

## Definizione degli Stati

Sebbene queste siano definizioni note a chi opera da sempre sui Mainframe, è bene richiamare alcuni

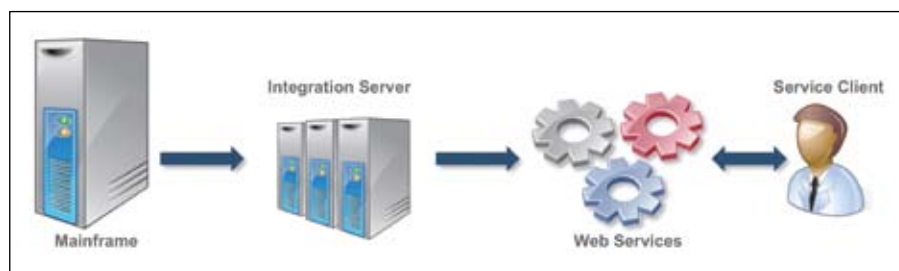
concetti fondamentali per comprendere l'essenza delle considerazioni tecniche che seguono. Questo perché ci sono vari modi per trasformare le applicazioni Mainframe in servizi, ciascuno dei quali risulta più appropriato in determinate circostanze. Vediamone quindi le basi:

- Per stato di una sessione si intende la situazione nella quale si trova in un determinato momento l'interazione che si svolge tra due macchine - o applicazioni, o servizi - diverse. Cosa che vale anche nelle relazioni Client / Server, tra utenti e via dicendo.
- Per sessione stateless si intendono le interazioni di cui sopra, delle quali non viene tenuta traccia della situazione in cui si trovano mano a mano che si svolgono. Di fatto, le interazioni avvengono come sequenze di eventi finiti ed indipendenti gli uni dagli altri.
- Le sessioni stateful sono invece quelle nelle quali si tiene costantemente traccia dello svolgimento delle interazioni, così come del contesto nel quale si svolgono.

## Gestione delle sessioni Mainframe come servizi

Nella gestione dei servizi derivati dalle applicazioni Mainframe ci sono cinque modi principali per operare e tra i quali ci si deve orientare. Vediamoli in estrema sintesi:

1. **Stateless, senza locking.** L'approccio più semplice è quello tipico del mondo Web, con servizi stateless che accedono ed eseguono le applicazioni Legacy



I servizi stateless creano delle sessioni proprie per consentire all'applicazione mainframe di interfacciarsi direttamente con l'applicazione client utilizzando le linee aperte già esistenti.

direttamente dai Client degli utenti. Questi servizi sono in grado di attivare delle proprie sessioni sull'Host in modo che risultino direttamente accedibili dall'esterno del sistema. Le applicazioni Mainframe interagiscono indirettamente con le applicazioni Client attraverso gli appropriati servizi stateless utilizzando normali linee di comunicazione, indipendentemente da dove si trovino i Client. Vantaggi: poiché si tratta di fatto di una semplice apertura sulla rete delle applicazioni Legacy, non occorre assolutamente modificare queste ultime che così risulteranno riutilizzabili nel nuovo scenario operativo in tempi rapidi e senza rischi. Svantaggi: utilizzando linee aperte e comunicazioni non cifrate, la sicurezza deve esser garantita a livello di rete. Inoltre, dal momento che le interazioni con le applicazioni Legacy avvengono in modalità stateless e senza alcun tracciamento delle attività, le comunicazioni tra applicazioni e Client sono di tipo anonimo. Uso raccomandato: grazie alla semplicità di implementazione e gestione, questo meccanismo risulta perfettamente idoneo in tutti i casi in cui la sicurezza è gestita in modo implicito a livello di dati o di reti, come ad esempio quando gli accessi alla rete sono riservati ad utenti noti ed adeguatamente accreditati. E' questa l'esperienza di numerosi utenti di Attachmate Verastream Host Integrator che hanno adottato questo metodo indiretto di comunicazioni per realizzare rapidamente accessi alle applicazioni Legacy per le quali la gestione degli stati non risulta necessaria. Oltretutto, in tali casi si massimizzano le prestazioni del sistema, senza introdurre alcun carico di lavoro aggiuntivo. Ad esempio, un tipico caso di uso di Verastream in questo scenario è quello in cui un System Administrator vuole controllare lo stato di funzionamento di determinate applicazioni tramite un'apposita Console. Nel momento in cui la richiesta giunge all'applicazione su Mainframe, quest'ultima andrà a popolare l'interfaccia sulla Console con i dati rilevati di suo interesse.

Trattandosi di dati non modificabili e destinati ad uno specifico utente accreditato, non occorre preoccuparsi più di tanto della sicurezza della rete, né della riservatezza dei dati.

2. **Stateless con linee riservate.** Se la sicurezza delle reti non è garantita, può risultare necessario introdurre uno strato di sicurezza al livello di linee

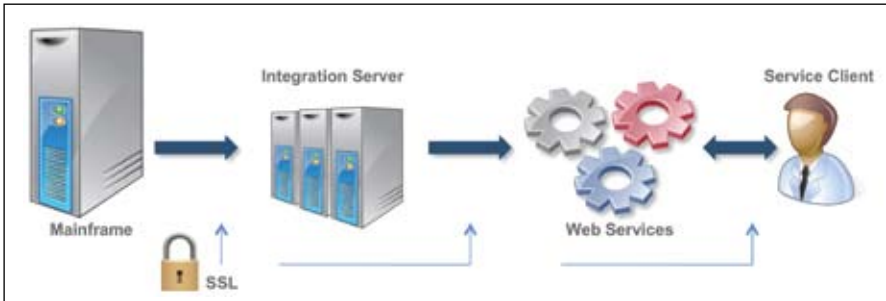
di comunicazione. L'architettura del sistema sarà analoga alla precedente, ma si avrà un servizio aggiuntivo per il controllo e l'apertura delle sessioni sul Mainframe. Rendendo sicure le linee via SSL o altri sistemi equivalenti, le applicazioni risulteranno molto più fruibili all'interno delle SOA, per loro stessa natura distribuite. Vantaggi: con questo approccio, si realizzano in modo non invasivo, servizi flessibili che sfruttano al meglio le applicazioni Legacy sui Mainframe. Fino a quando non si presenta l'esplicita necessità di tracciare le attività del Client, i servizi possono rimanere stateless. Gli accessi hanno buone prestazioni in quanto i servizi possono attivare le sessioni di controllo con le applicazioni Mainframe prima che queste siano accedute dagli utenti. Svantaggi: anche in questo caso, come in quello precedente, né i Mainframe né le applicazioni su di essi possono sapere con precisione chi sono i loro utenti: i servizi di autenticazione, se richiesti, debbono infatti essere effettuati in un livello intermedio dell'infrastruttura, usando ad esempio l'Active Directory. Il problema si può porre quando, per ragioni di normative o controlli, occorre esser in grado di individuare esattamente gli utenti delle applicazioni Legacy. Uso raccomandato: applicazioni Legacy che debbono essere accedute anche dall'esterno delle reti dell'azienda, da Client adeguatamente accreditati ed in grado di rilevarle. Spesso, le installazioni di Verastream vengono fatte per servizi che aggregano dati di vario genere, creati da applicazioni stateless. In tali situazioni, i Client effettuano di continuo richieste di aggiornamento dei dati che non risultano pericolose in quanto si tratta di interrogazioni e non di scritture di nuovi dati.

3. **Stateless con servizi di logging.** Un livello superiore di controllo si ottiene aggiungendo ai meccanismi precedenti la registrazione delle attività in un File di Log che consente di abbinare l'esecuzione dei singoli servizi ai loro richiedenti. Ad esempio, con Verastream Host Integrator, si possono creare e memorizzare i Log con le identità degli utenti di ciascuna applicazione su Host. Si possono così documentare l'impiego delle risorse sull'Host e rispondere alle richieste di Audit senza compromettere le prestazioni del sistema. I servizi stateless creano una sessione per ciascuna applicazione Mainframe stabilendo una connessione indiretta con i servizi sui Client,

analogamente a quanto già visto al punto 1, si procede con la protezione delle reti. Si tratta di un modello che si sposa molto bene con le SOA, sebbene dal punto di vista del Mainframe presenti ancora dei rischi. In particolare, creando servizi controllati dall'esterno che inglobano le applicazioni Mainframe, diventa

circostanze, occorre creare servizi che identifichino perfettamente gli utenti e li rendano noti alle applicazioni. In altre situazioni, ciascun utente accede a dati che lo riguardano personalmente e sui quali lui solo è autorizzato ad operare. In questi casi, i servizi debbono registrare l'utente e verificarne le credenziali prima di offrirgli

l'accesso alle applicazioni. Cosa per la quale occorre creare dei servizi in grado di verificare l'identità degli utenti ed i loro livelli di autorizzazione, che verranno trasmessi all'applicazione su Mainframe o ai suoi meccanismi di controllo, tipo RACF (Resource Access Control Facility). Una volta autorizzato, l'utente eseguirà la propria sessione come fosse direttamente



I servizi stateless creano una sessione per consentire all'applicazione mainframe di interfacciarsi indirettamente con l'applicazione client, come nell'opzione 1, ma in questo caso le linee sono chiuse.

indispensabile disporre di un'infrastruttura che gestisca la sicurezza dall'esterno del Mainframe. In tal modo, non è più necessario che il Mainframe sappia chi vi sta accedendo, in quanto questo compito viene demandato ai servizi di infrastruttura esterni. Vantaggi: buone prestazioni ed elevata flessibilità nell'uso di servizi stateless, sfruttando al massimo la condivisione delle risorse e delle sessioni su Mainframe, mentre i servizi di logging registrano chi sta accedendo al sistema e cosa vi sta facendo. Svantaggi: se la qualità dei controlli effettuati dall'infrastruttura esterna non è elevata, i dati e le applicazioni su Mainframe possono trovarsi esposti a rischi molto gravi. Uso raccomandato: quando si può contare su un'infrastruttura di sicurezza esterna al Mainframe affidabile e robusta, nella quale i dati non devono essere controllati esclusivamente dalle applicazioni sull'Host. Ad esempio, un importante editore statunitense ha adottato le funzioni di logging di Verastream per gestire le applicazioni SOA stateless che offrono servizi di Self-service agli acquirenti di inserzioni pubblicitarie. Gli utenti accreditati accedono tramite i loro browser alle applicazioni sul Mainframe per inserire e pagare gli annunci che dovranno apparire sui giornali. I livelli di sicurezza di questo sistema sono stati considerati adeguati alle circostanze in quanto gli utenti sono noti, le linee protette da SSL e tutte le operazioni vengono documentate e registrate dall'apposito servizio.

connesso al Mainframe, dal quale verrà scollegato al termine delle operazioni. Seguendo questo modello, ciascun servizio Client viene abbinato alla singola sessione tramite gli appositi Log gestiti dall'esterno del sistema e realizzati impiegando tecnologie di service-wrapping. Quando il Mainframe effettua i propri controlli sugli accessi, in realtà invoca i servizi di sicurezza che forniscono i dati ed i livelli di autorizzazione degli utenti. Vantaggi: la sicurezza ed i controlli sono svolti ai massimi livelli, esattamente come accade in ambienti unicamente Mainframe. Svantaggi: nonostante l'impiego di servizi esterni per la gestione della sicurezza, sul Mainframe vengono usate delle risorse in proporzione alla quantità di servizi invocati. Supponendo che sul Mainframe giungano 1.000 richieste di accesso, dovranno essere gestite 1.000 sessioni Host, ciascuna delle quali durerà tanto quanto si protrarranno le interazioni con i singoli Client degli utenti. Per contro, con i meccanismi di tipo stateless si possono gestire carichi di lavoro analoghi con solo poche sessioni condivise sull'Host. I tempi di risposta possono risultare ulteriormente peggiorati all'inizio delle attività, in quanto per ogni connessione occorre attivare una nuova sessione sul Mainframe per gestirne gli stati. Uso raccomandato: questo tipo di approccio dà il meglio di sé quando le applicazioni su Mainframe richiedono il controllo diretto sulle risorse e degli utenti, così come quando le attività sequenziali dei servizi sono strettamente associate alle singole identità degli utenti. Ad esempio, in un'Università

4. **Sessioni basate su servizi Stateful.** In alcuni casi, sono le stesse applicazioni su Mainframe a governare il proprio funzionamento. In tali

di grandi dimensioni questo metodo viene impiegato per registrare gli studenti ai corsi ed agli esami. Quando lo studente richiede un'iscrizione, si attiva una routine di sicurezza che controlla l'identità dell'utente, richiedendone User ID e Password. Dopo di che, sull'Host parte la sessione che gestisce i dati dello studente. L'applicazione sul Mainframe utilizza uno stretto abbinamento tra i dati dello studente e le azioni che quest'ultimo può svolgere sul sistema. In pratica, il Service Client diviene così un'estensione dell'applicazione sul Mainframe.

5. **Servizi stateful ad alte prestazioni.** Per le applicazioni che risiedono interamente sotto CICS (Customer Information Control System), si può adottare un modello ibrido. Con il CICS, è possibile creare servizi wrapped che non richiedono alcuna sessione separata sull'Host, in quanto è possibile creare una connessione diretta tra l'applicazione CICS ed il servizio esterno per la gestione dei controlli e dei flussi di dati. Questo grazie alle capacità, ad esempio, di Verastream Bridge Integrator. Tale soluzione sfrutta le capacità di bridging di IBM Link3270 che consente di eseguire l'autenticazione direttamente sul Mainframe, utilizzando sia i meccanismi di autorizzazione del RACF, sia quelli delle singole applicazioni. Benché in questo caso i sistemi di autenticazione siano gli stessi dell'approccio precedente (con i servizi di logging, monitoraggio e visibilità gestiti direttamente dal Mainframe), non risulta più necessario attivare ogni volta una nuova sessione sul Mainframe per autenticare gli utenti ed associarli ai relativi processi. Le sessioni vengono infatti gestite direttamente all'interno del CICS in associazione ai vari servizi e non ai singoli utenti. Con questo approccio basato sulla gestione diretta degli accessi, quando un'applicazione Client, da un qualsiasi sito Web, richiama un servizio, i parametri di sicurezza del Mainframe vengono passati come parte del servizio stesso. Dopo di che, il servizio crea una connessione diretta ed autenticata con l'applicazione CICS di destinazione, esegue le azioni richieste e quindi disconnette l'utente e chiude la connessione. Vantaggi: si eliminano i costi (in termini di risorse e prestazioni)

richiesti per creare le sessioni Host dedicate alla gestione degli stati. Si può inoltre fare a meno di allestire uno strato intermedio per la gestione dei controlli, semplificando le comunicazioni via SSL. Svantaggi: sono di due generi. Innanzitutto, il metodo è adottabile solo per le applicazioni CICS, per cui potrebbe risultare necessario creare un mix di servizi basati su meccanismi di tipo diverso. In secondo luogo, diventa necessario aggiungere l'esecuzione di un nuovo componente all'interno delle partizioni CICS in uso nell'azienda. Cosa che può risultare complessa più che altro a livello organizzativo per via degli iter di approvazione e dell'attribuzione delle responsabilità di installazione, manutenzione, esercizio. Uso raccomandato: approccio tipicamente impiegato per applicazioni transazionali che richiedono massima sicurezza e buone prestazioni, tipo quelle per i Cash Dispenser.

### Orientarsi tra le varie alternative

Esaminate le caratteristiche dei servizi da erogare, in sintesi, si potrà procedere come segue:

- Se l'ambiente IT è chiuso o dotato di reti controllate, la gestione degli accessi in modalità puramente stateless risulterà più che adeguata.
- Per fornire accessi anche all'esterno delle proprie reti, potrebbero bastare anche le comunicazioni protette via SSL.
- Nel caso di applicazioni critiche per l'azienda, ai controlli degli accessi si potranno aggiungere i servizi di logging.
- Se le applicazioni su Mainframe richiedono un controllo diretto sugli utenti, si dovranno allestire servizi con la gestione completa degli stati.
- Quando le applicazioni su Mainframe sono poste sotto CICS, la cosa migliore è adottare l'approccio ibrido descritto al punto 5 che offre eccellenti prestazioni e sicurezza.

La fase di analisi risulta pertanto fondamentale per scegliere il miglior approccio da seguire caso per caso.

## Come procedere

Tutto il discorso presuppone la disponibilità di tre tipologie di competenze all'interno dell'azienda: quelle relative alle architetture Mainframe, quelle dei sistemi distribuiti e dei Web Service, quelle sulle applicazioni in esercizio. Competenze, specie le prime due, che non si improvvisano e che spesso non val neppure la pena di inserire in azienda. Conviene quindi valutare il da farsi, in termini di obiettivi e priorità dell'azienda, affidando a provati specialisti i compiti più squisitamente tecnici, mantenendo all'interno la consapevolezza di cosa fare ed il controllo dei progetti, utilizzando le competenze dei propri sviluppatori COBOL che normalmente conoscono bene i controlli dei quali hanno bisogno ed i cambiamenti a livello applicativo che potrebbero rendersi necessari nelle varie condizioni.

## Il ruolo di Verastream

Per facilitare l'apertura delle applicazioni Mainframe alle SOA, senza doverne modificare il codice, Attachmate ha messo a punto la famiglia di prodotti Verastream che forniscono vari servizi specializzati di tipo non invasivo per coprire tutte le tipologie di gestione degli accessi elencate nei punti precedenti.

Tra le varie possibilità offerte ci si può orientare tra:

- **Integrazione a livello di Screen:** tanto nei tipici ambienti con Mainframe IBM (zSeries, S/390), quanto in quelli IBM iSeries (AS/400), UNIX, OpenVMS o HP e3000, si può utilizzare Verastream Host Integrator per trasformare le applicazioni Legacy in servizi riutilizzabili nell'ambito di applicazioni composite. Verastream Host Integrator facilita la creazione di componenti (COM, .NET, Java, o Web Services) utilizzabili all'interno delle SOA.

- **Integrazione a livello di Transazioni:** con Verastream Transaction Integrator si possono combinare dati e costrutti applicativi dei programmi sviluppati per ambienti IMS e CICS con servizi SOA, disponendo di funzioni per il supporto nativo dei meccanismi di sicurezza esistenti (tipo RACF, ACF2 o TopSecret) e di una gestione centralizzata dei servizi, offrendo accesso diretto alle applicazioni nelle COMMAREA passando via DPL.
- **Integrazione via Bridge CICS 3270.** Verastream Bridge Integrator è un adapter residente su Mainframe, all'interno del CICS Transaction Server, che gestisce l'integrazione ad alte prestazioni con qualsiasi applicazione .NET o J2EE. Le interazioni CICS vengono attivate tramite IBM Link 3270 Bridge in qualsiasi formato richiesto dalle corrispondenti applicazioni CICS.

## Attachmate

Attachmate fornisce soluzioni software evolute per l'emulazione di terminale, l'integrazione di applicazioni e le comunicazioni sicure. La business unit NetIQ offre soluzioni per la gestione delle applicazioni, i sistemi enterprise, la sicurezza e la compliance. Grazie alle nostre tecnologie, oltre 65.000 aziende in tutto il mondo sono ora in grado di far funzionare in modo nuovo e più proficuo le proprie risorse IT. Per ulteriori informazioni visitare il sito [www.attachmate.it](http://www.attachmate.it).



### Sede Centrale

1500 Dexter Avenue North  
Seattle, Washington 98109  
TEL 206 217 7500  
FAX 206 217 7515

### Sede Centrale EMEA

Paesi Bassi  
TEL +31 172 50 55 55  
FAX +31 172 50 55 51

### Sede Italiana di Milano

TEL +39 02 99060201  
FAX +39 02 99044784

### Sede Italiana di Roma

TEL +39 06 5423281  
FAX +39 06 5408851

WEB [www.attachmate.it](http://www.attachmate.it)

EMAIL [informazioni.italia@attachmate.com](mailto:informazioni.italia@attachmate.com)

Per le informazioni sulle sedi locali, visitare [www.attachmate.it](http://www.attachmate.it)