Linee Guida di Interoperabilità

Direzione Sistemi Informativi, Comune di Firenze

Introduzione

Con questo documento la Direzione Sistemi Informativi del Comune di Firenze si pone l'obiettivo di stabilire delle linee guida da seguire al fine di avere uno standard ed una uniformità di gestione dei servizi API.

In tal modo si rendono espliciti gli scenari in cui poter utilizzare WSO2 in modo esteso oppure utilizzarlo solamente come gateway unico. Si evidenziano inoltre gli standard da applicare nello sviluppo e nell'esposizione delle API.

Criteri per la creazione di una nuova API: dentro WSO2 o fuori da WSO2?

Quando ci si appresta a realizzare una nuova API, è necessario individuare in fase di progetto se realizzarla esternamente a WSO2 e poi pubblicarla mediante API Manager, oppure realizzarla integralmente su WSO2 tramite gli strumenti forniti da tale piattaforma.

Per poter supportare la scelta, si riportano di seguito dei criteri da soppesare, che possono indirizzare su una metodologia o sull'altra.

Complessità della API

L'API necessita di operazioni semplici (operazioni CRUD) di complessità ridotta? WSO2 fornisce degli strumenti automatici per la realizzazione di semplici CRUD. È possibile anche inserire facilmente delle componenti per la gestione di semplici deviazioni rispetto al comportamento di base. Se si necessita di inserire operazioni più complesse la situazione si complica e potrebbe essere preferibile lavorare esternamente per avere un controllo maggiore su quanto deve essere realizzato.

Tipologia della base dati

L'API coinvolge una base dati distribuita su molte tabelle? Nel caso in cui la base dati sulla quale si appoggiano le API da costruire sia composta da molteplici tabelle con foreign key di collegamento fra le tabelle stesse, è preferibile costruire le API fuori da WSO2 e poi procedere alla loro pubblicazione.

Interventi futuri di manutenzione evolutiva e correttiva

Si prevede che gli interventi futuri di manutenzione correttiva ed evolutiva verranno realizzati da personale esterno? WSO2 è una piattaforma conosciuta e diffusa. Essa si pone in un punto di mezzo per quanto riguarda "Completeness of vision" e "Ability of execute" (si veda Magic Quadrant for Full Life Cycle API Management del 2020, Gartner).

Figure 1. Magic Quadrant for Full Life Cycle API Management

Source: Gartner (September 2020)

L'intervento da parte di personale esterno e la facilità di poter incaricare aziende diverse per l'espletazione della manutenzione, dovrebbe far prediligere la creazione delle API interamente su WSO2. Infatti, la creazione di API all'interno di WSO2 rende possibile l'intervento da parte di personale esterno formato sulla piattaforma WSO2. Tuttavia, va tenuto in considerazione che le aziende "certificate" WSO2 in Italia ad oggi (2021) sono solamente 2; mentre esistono tanti fornitori che sono formati su WSO2 e forniscono assistenza e supporto, pur non essendo certificati.

Realizzazione della API internamente all'ente

Si prevede che l'API venga realizzata e manutenuta da personale interno all'ente? Se le API vengono realizzate internamente all'ente, allora esistono team specifici che a seconda del processo, realizzano le API secondo propri stack tecnologici di team. La formazione sulla piattaforma WSO2 non è completa per tutto il personale, e dunque per consentire una intercambiabilità di risorse da allocare sui progetti, è preferibile proseguire con la realizzazione di API esternamente a WSO2 e poi procedere con la loro pubblicazione sulla piattaforma WSO2, almeno fintanto che la formazione del personale non sia stata completata in modo sufficiente da operare sulla piattaforma. Sul punto della formazione, potranno avere un ruolo importante le persone che ad oggi sono state formate su WSO2 e che dunque potranno diffondere le conoscenze acquisite.

Facilità di abbandono di WSO2

In caso di cessazione dell'utilizzo di WSO2, quanto è oneroso attuare una migrazione della API ad altra piattaforma/modalità di fruizione? La costruzione della API internamente a WSO2 crea una dipendenza con la piattaforma (espone ad un vendor lock-in). In fase di progettazione è necessario chiedersi quanto può essere facile e snello attuare delle procedure di migrazione dalla piattaforma WSO2 ad altra piattaforma (exit-strategy), combinato con l'importanza nevralgica della API per l'ente. Nel caso di una API strategica per l'ente, deve essere facile e sicuro poterla migrare su altra locazione per poter decidere di svilupparla interamente su piattaforma WSO2.

Sviluppo API tramite Enterprise Integrator

Come per la gestione standard dei progetti di sviluppo software, sarà necessario utilizzare un repository per il codice prodotto, che rende possibile archiviare il codice sorgente, condividerlo internamente, gestirne le versioni e ripristinarlo in caso di necessità.

Per i progetti di questo tipo verrà utilizzata una repository interna basata su **Git**. Ogni progetto di integrazione realizzato sul tool di sviluppo WSO2 Integration Studio corrisponderà ad un repository Git.

Durante la fase di sviluppo su WSO2, si suggerisce l'applicazione di un approccio "Git Flow", per rendere lineare e controllato il flusso di lavoro.

Per mantenere la separazione degli ambienti (produzione, staging, etc) si consiglia di separare in sotto progetti specifici le entità i cui valori dipendono dall'ambiente di deployment (ad es. URL, riferimenti ai database, etc).

Disposizioni specifiche per il deploy automatico tramite procedure di CI/CD potrebbero essere sviluppate in versioni successive di questo documento.

Sviluppo API esterne a WSO2 ma compatibili per la pubblicazione tramite API Manager

Le API devono essere rappresentate mediante un Interface Description Language standard (IDL). Nello specifico:

- per REST, swagger 2.0 e successive, raccomandato OpenAPI 3.0;
- per SOAP, WSDL 1.1 e successive.

Si può applicare un meccanismo di autenticazione per le API che rientrano nei seguenti casi:

- espongono dati personali
- espongono servizi di aggiornamento dei dati che possono alterare in modo non controllato le relative risorse

Tale meccanismo impedisce che siano liberamente interrogabili dalla rete locale. Ad esempio, si possono implementare Basic Authentication per le API di tipo REST e WS-Security con utilizzo di UsernameToken per le API di tipo SOAP.

Esposizione API tramite API Manager

Tutte le API vengono esposte tramite WSO2 API Manager che opera come "reverse proxy evoluto" con le funzioni di autenticazione e autorizzazione, throttling delle richieste e gestione del lifecycle. Come raccomandato dalle linee guida AGID per l'interoperabilità[1], il numero di versione non deve essere presente all'interno del nome della API esposta perché viene gestito tramite API Manager.

Nell'esposizione tramite API Manager si indicano il numero di versione e la tecnologia nell'endpoint delle API secondo la seguente struttura:

https://api.comune.fi.it/[rest|soap]/<nome-api>/v<major>[.<minor>[.<patch>]]/<risorsa>

dove:

- [rest|soap] indica la tecnologia della API;
- <nome-api> indica il servizio che contiene le API relative. Potrebbe essere il nome di una applicazione specifica ("sigedo") oppure il nome di un servizio generico ("organigramma");
- v<major>[.<minor>[.<patch>]] indica il numero di versione in coerenza con Semantic Versioning 2.0.0;
- <risorsa> è il nome della risorsa specifica.

Ad esempio una API Rest relativa al servizio "anagrafe" potrebbe esporre i seguenti end point:

Risorsa	Endpoint
Lettura anagrafica di un cittadino	GET https://api.comune.fi.it/rest/anagrafe/v1.0.0/anagrafica/{codice_fiscale}
Lettura dei nuovi nati in uno specifico anno	GET https://api.comune.fi.it/rest/anagrafe/v1.0.0/nuovi-nati/{anno}

[1] Linee guida: https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita/il-nuovo-modello-interoperabilita
Raccomandazioni:
https://www.agid.gov.it/sites/default/files/repository_files/04_raccomandazioni_di_implementazione.pdf

Sicurezza delle API: servizi di Autenticazione e Autorizzazione per le API

Le API esposte tramite API Gateway saranno protette tramite il protocollo Oauth2; per ogni applicazione verranno rilasciate una coppia di chiavi (consumer key e consumer secret) utili per l'accesso a tutte e sole le API necessarie per quell'applicazione.

Non è consentito l'utilizzo di una stessa coppia di chiavi da parte di più di una applicazione. Per ogni applicazione che vuole utilizzare i servizi esposti da WSO2, è necessario effettuare una sottoscrizione specifica ed ottenere una coppia di chiavi personalizzata e non cedibile.

Robustezza e sicurezza del sistema

L'infrastruttura è stata realizzata con una struttura di tipo cluster sfruttando le configurazioni messe a disposizione da WSO2, sono state esposte su internet solo le URL strettamente necessarie e comunque attraverso un bilanciatore centralizzato (in configurazione cluster active-passive) con funzionalità tipiche di Intrusion Detection, Intrusion Prevention e Web Application Firewall.

BENEDETTO
FEMIA
Comune di
Firenze
09.09.2022
12:13:31
GMT+01:00