
Guida di Installazione

Release 3.3.0.rc1

07 mar 2020

1	Introduzione	1
2	Fase Preliminare	3
3	Esecuzione dell'Installer	5
3.1	Nuova Installazione	5
3.2	Aggiornamento	16
4	Fase di Dispiegamento	21
4.1	Nuova Installazione	21
4.2	Aggiornamento	22
5	Verifica dell'Installazione	25
6	Finalizzazione dell'Installazione	27
6.1	Url di Invocazione	28
6.2	Multi-Tenant	30
6.3	Gestione CORS	31
6.4	Rate Limiting - Numero Complessivo Richieste Simultanee	32
6.5	Tempi Risposta	32
6.6	Caching della Risposta - Disk Cache	33
6.7	Configurazione e Monitoraggio	35
6.8	Configurazione in Load Balancing	35
6.9	Configurazione HTTPS	38
7	Esempio di setup del database PostgreSQL	43

CAPITOLO 1

Introduzione

In questa sezione trovi una guida rapida per l'installazione della versione binaria di GovWay. Verifica e, se necessario, installa il software di base per GovWay come indicato nella Fase Preliminare. Un installer grafico ti guiderà nella personalizzazione della binary release verso la tua piattaforma.

Fase Preliminare

Prima di procedere con l'installazione di GovWay è necessario disporre del software di base nell'ambiente di esercizio. Verificare i passi seguenti, procedendo eventualmente all'installazione dei componenti mancanti.

1. *Java Runtime Environment (JRE) 11* (è possibile scaricare JRE al seguente indirizzo: <https://jdk.java.net/archive/>)

Verificare la configurazione dell'ambiente Java dell'Application Server. Si raccomanda una configurazione minima dei parametri della JVM, come segue:

- `-XX:MaxMetaspaceSize=516m -Xmx1024m`

Verificare inoltre che il charset utilizzato dalla JVM sia UTF-8:

- `-Dfile.encoding=UTF-8`

2. *Application Server WildFly* (<http://wildfly.org>) versione 18. In alternativa è possibile effettuare l'installazione su Apache Tomcat (<http://tomcat.apache.org>) versione 9.

Nota: GovWay supporta anche altri application server j2ee diversi da quelli citati, partendo dalla distribuzione sorgente.

3. Un *RDBMS* accessibile via JDBC. La binary release supporta le seguenti piattaforme:

- *PostgreSQL 8.x o superiore*
- *MySQL 5.7.8 o superiore*
- *Oracle 10g o superiore*
- *HyperSQL 2.0 o superiore*
- *MS SQL Server 2017 o superiore*

La distribuzione GovWay è stata estesamente testata prima del rilascio sulla seguente piattaforma di riferimento:

- *Openjdk 11 (version: 11+28)*
- *PostgreSQL 9 (version: 9.5.10)*

- *WildFly 18 (version: 18.0.1.Final) e Tomcat 9 (version: 9.0.31)*

Esecuzione dell'Installer

1. Scarica [qui](#) la binary release di GovWay
2. Scompatta l'archivio, verifica ed eventualmente imposta la variabile d'ambiente `JAVA_HOME` in modo che riferisca la directory radice dell'installazione di Java. Lancia l'utility di installazione mandando in esecuzione il file `install.sh` su Unix/Linux, oppure `install.cmd` su Windows.

Nota: L'utility di installazione non installa il prodotto ma produce tutti gli elementi necessari che dovranno essere dispiegati nell'ambiente di esercizio. L'utility di installazione mostra all'avvio una pagina introduttiva.

3. Dopo la pagina introduttiva, cliccando sul pulsante *Next*, si procede con la scelta della *Modalità di Installazione*. Le scelte possibili sono:
 - *Nuova Installazione*: scelta da effettuare nel caso in cui si stia procedendo con una nuova installazione di GovWay.
 - *Aggiornamento*: scelta da effettuare nel caso in cui si stia procedendo con l'aggiornamento di una versione di GovWay precedentemente installata.

3.1 Nuova Installazione

Supponiamo che la scelta sia quella di una nuova installazione. Vediamo come si sviluppa il processo di installazione:

1. Si procede con l'inserimento delle *Informazioni Preliminari*, che prevede i seguenti dati:

Operare le scelte sulla maschera di *Informazioni Preliminari* tenendo presente che:

- *Directory di lavoro*: una directory utilizzata da GovWay per inserire i diversi file di tracciamento prodotti. Non è necessario che questa directory esista sulla macchina dove si sta eseguendo l'installer; tale directory dovrà esistere nell'ambiente di esercizio dove verrà effettivamente installato il software GovWay.



Fig. 3.1: Introduzione

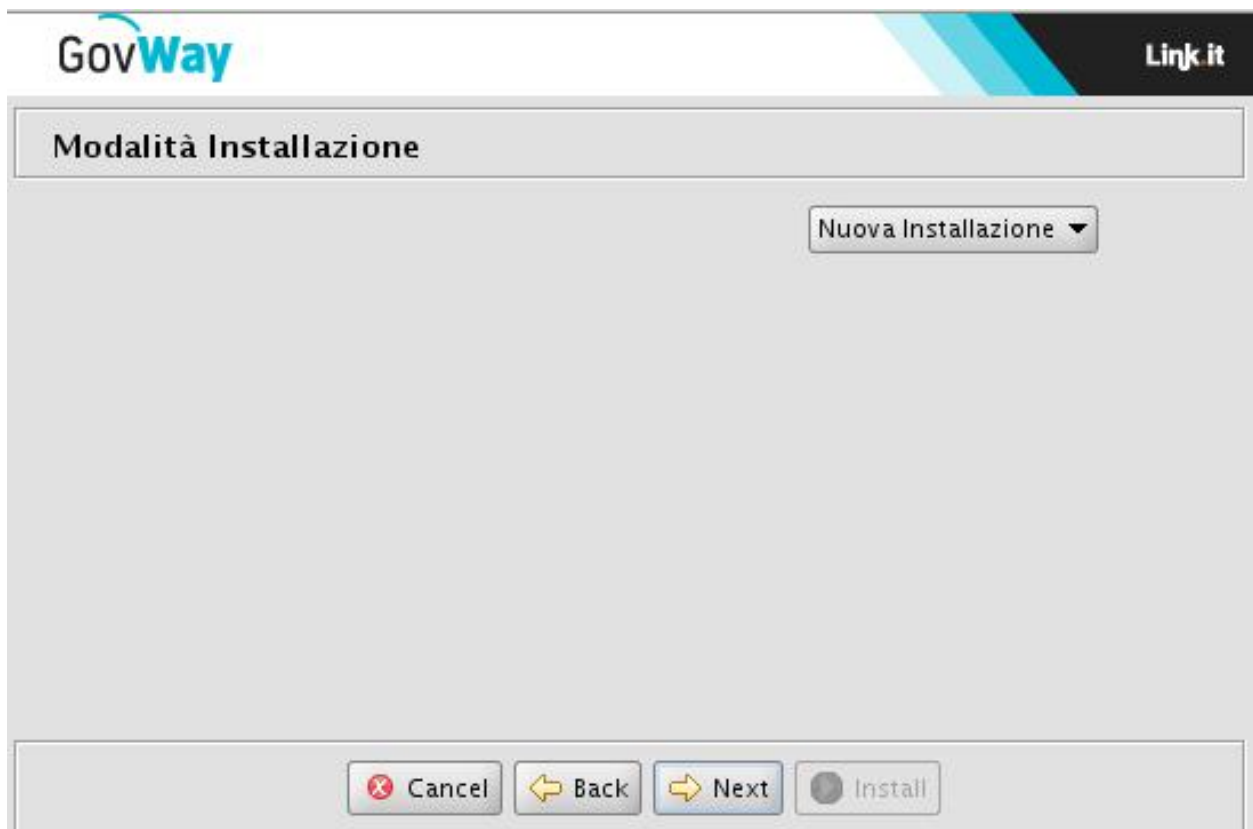
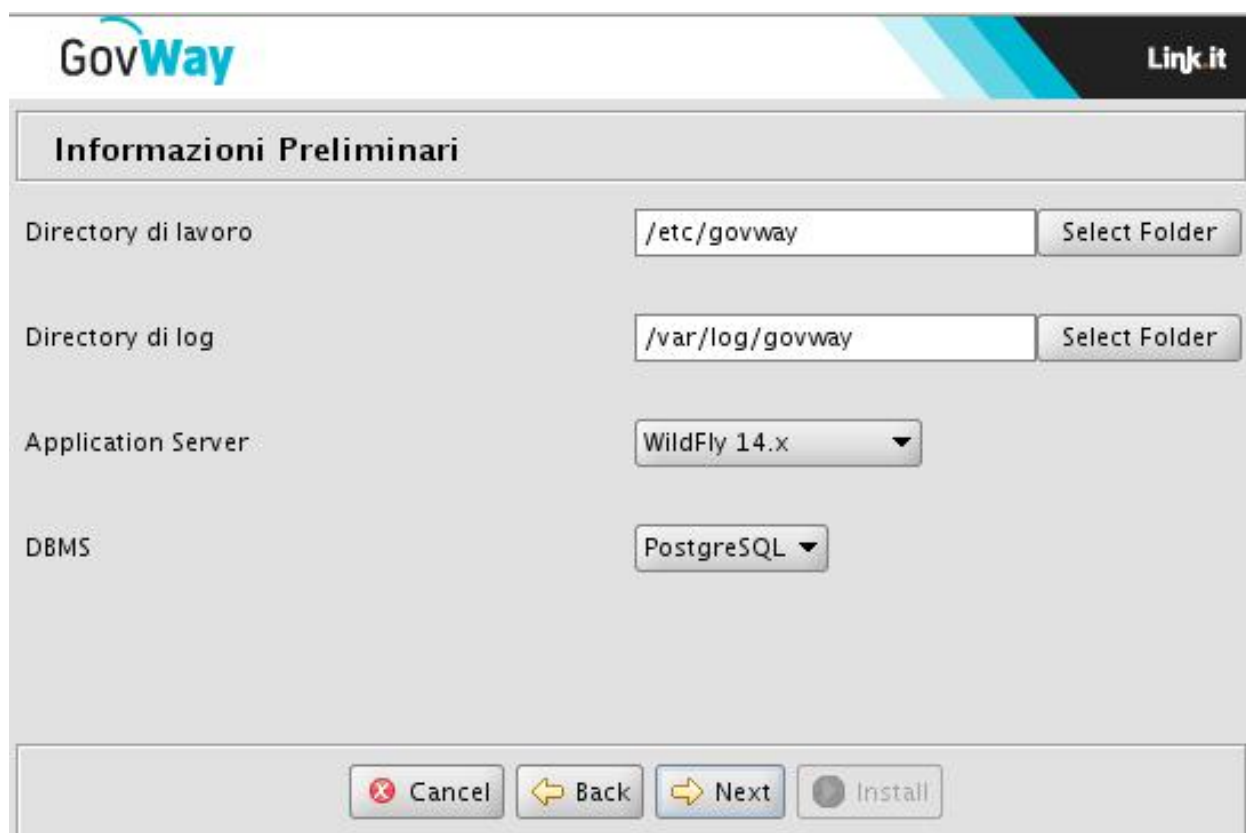


Fig. 3.2: Modalità di Installazione



The screenshot shows the 'Informazioni Preliminari' (Preliminary Information) window of the GovWay installer. The window has a header bar with the 'GovWay' logo on the left and a 'Link it' button on the right. The main area contains four configuration rows: 'Directory di lavoro' (Working Directory) with a text field containing '/etc/govway' and a 'Select Folder' button; 'Directory di log' (Log Directory) with a text field containing '/var/log/govway' and a 'Select Folder' button; 'Application Server' with a dropdown menu showing 'WildFly 14.x'; and 'DBMS' with a dropdown menu showing 'PostgreSQL'. At the bottom, there is a row of four buttons: 'Cancel' (with a red X icon), 'Back' (with a yellow left arrow icon), 'Next' (with a yellow right arrow icon), and 'Install' (with a grey circle icon).

Informazioni Preliminari	
Directory di lavoro	<input type="text" value="/etc/govway"/> <input type="button" value="Select Folder"/>
Directory di log	<input type="text" value="/var/log/govway"/> <input type="button" value="Select Folder"/>
Application Server	<input type="button" value="WildFly 14.x"/>
DBMS	<input type="button" value="PostgreSQL"/>

Fig. 3.3: Informazioni Preliminari

- *Directory di log*: una directory utilizzata da GovWay per produrre i file di log. Non è necessario che questa directory esista sulla macchina dove si sta eseguendo l'installer; tale directory dovrà esistere nell'ambiente di esercizio dove verrà effettivamente installato il software GovWay.
- *DBMS*: il tipo di database scelto tra quelli supportati: PostgreSQL, MySQL, Oracle, HyperSQL, SQLServer.
- *Application Server*: Application server utilizzato selezionato tra: WildFly (versione 18) e Apache Tomcat (versione 9).

2. Al passo successivo si dovranno inserire tutti i dati per l'accesso al database ed in particolare:



Fig. 3.4: Informazioni Accesso Database

- *Hostname*: indirizzo per raggiungere il database
- *Porta*: la porta da associare all'host per la connessione al database
- *Nome Database*: il nome dell'istanza del database a supporto di GovWay. Non è necessario che questo database esista in questa fase. Il database di GovWay infatti potrà essere creato nella fase successiva purché il nome assegnato coincida con il valore inserito in questo campo.
- *Username*: l'utente con diritti di lettura/scrittura sul database sopra indicato. Analogamente al punto precedente, l'utente potrà essere creato nella fase successiva dopo aver creato il database. Ricordarsi però di utilizzare il medesimo username indicato in questo campo.
- *Password*: la password dell'utente del database.

3. Il successivo passo richiede di stabilire le credenziali relative alle utenze di amministrazione per l'accesso ai cruscotti di gestione:

I dati da inserire sono:



GovWay Link it

Configurazione Utente

Username Amministratore (govwayConsole)

Password Amministratore

Username Operatore (govwayMonitor)

Password Operatore

Raccomandazioni sulla password sono indicate di seguito:

- differente dall'username
- contenga almeno 8 caratteri
- contenga almeno un carattere alfabetico, un numero ed un simbolo non alfanumerico

Fig. 3.5: Informazioni Utente Amministratore

- *Username/Password* relativi all'utente amministratore della govwayConsole.
 - *Username/Password* relativi all'utente operatore della govwayMonitor.
4. Nel successivo passo è possibile indicare se tra gli archivi generati devono essere inclusi i servizi che permettono la configurazione ed il monitoraggio di GovWay tramite API REST.

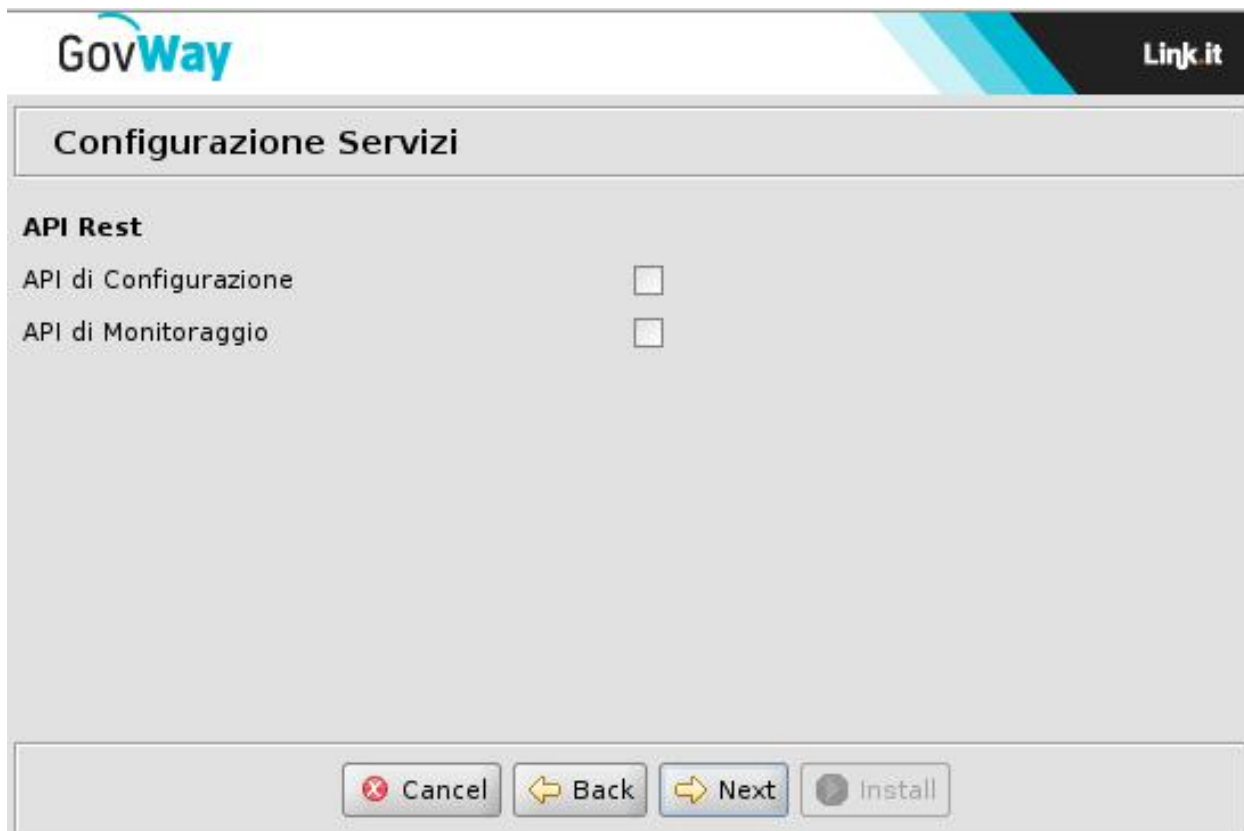


Fig. 3.6: Configurazione Servizi

5. Al passo successivo si dovranno inserire i dati relativi ai profili di interoperabilità supportati dal gateway:
- *Profilo*: contrassegnare con un flag i profili aggiuntivi che saranno gestite da GovWay, scelti tra quelli offerti built-in dal prodotto:
 - *ModI PA*
 - *SPCoop*
 - *eDelivery*
 - *SdI (Fatturazione Elettronica)*

Nota: Il profilo “API Gateway” viene sempre installato.

- *Soggetto*: nome del soggetto interno che verrà creato automaticamente.
6. Se si è scelto di includere il profilo eDelivery verranno presentati tre ulteriori tre passi di installazione. Nel primo passo viene richiesto di immettere la versione dell'Application Server e del Database associato alla versione di Domibus utilizzata.

GovWay Link it

Profili di Interoperabilità

Profilo

API Gateway	<input checked="" type="checkbox"/>
ModI PA	<input type="checkbox"/>
SPCoop	<input type="checkbox"/>
eDelivery	<input type="checkbox"/>
Fatturazione Elettronica	<input type="checkbox"/>

Soggetto

Fig. 3.7: Profili di Interoperabilità

GovWay Link it

Configurazione Profilo eDelivery (1/3)

Domibus v4.x

Application Server wildfly12 ▼

DBMS Oracle ▼

Cancel Back Next Install

Fig. 3.8: Configurazione eDelivery

7. Nel secondo passo, relativamente alla configurazione del profilo eDelivery, viene richiesto di immettere i relativi dati di configurazione.

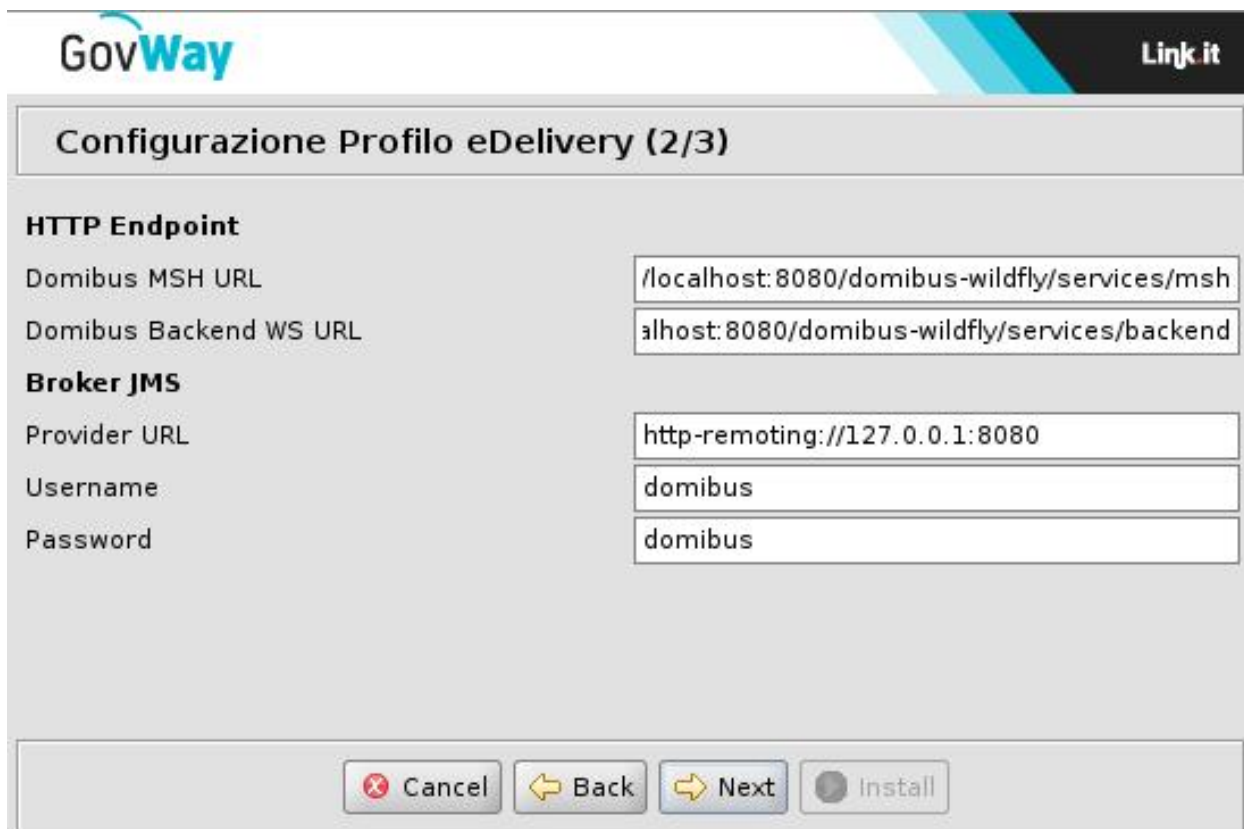


Fig. 3.9: Configurazione eDelivery (HTTP/JMS)

I dati di configurazione da immettere in questo step riguardano l'installazione di Domibus con la quale GovWay deve integrarsi per il dialogo con altri access point tramite il protocollo eDelivery. I dati richiesti sono:

- **HTTP Endpoint:** gli endpoint per contattare l'access point domibus interno
 - Domibus MSH URL: endpoint pubblico per la raggiungibilità dagli altri access point
 - Domibus Backend WS URL: endpoint dei servizi di backend che saranno utilizzati da GovWay per l'integrazione a Domibus
- **Broker JMS:** i dati di accesso al broker JMS utilizzato internamente da Domibus
 - Provider URL: endpoint del Broker JMS
 - Username/Password: credenziali per l'accesso ai servizi del Broker JMS

8. Nell'ultimo passo, relativamente alla configurazione del profilo eDelivery, verranno richiesti i dati di accesso al database utilizzato da Domibus:

- *Hostname*: indirizzo per raggiungere il database
- *Porta*: la porta da associare all'host per la connessione al database
- *Nome Database*: il nome dell'istanza del database a supporto di Domibus.
- *Username*: l'utente con diritti di lettura/scrittura sul database sopra indicato.
- *Password*: la password dell'utente del database.

GovWay Link it

Configurazione Profilo eDelivery (3/3)

DBMS

Hostname	127.0.0.1
Porta	1521
Tipo Accesso	SID ▼
Nome Database	XE
Username	domibus
Password	domibus

Fig. 3.10: Configurazione eDelivery (DBMS)

9. All'ultimo passo, premendo il pulsante *Install* il processo di configurazione si conclude con la produzione dei file necessari per l'installazione di GovWay che verranno inseriti nella nuova directory *dist* creata al termine di questo processo.



Fig. 3.11: Installazione

I files presenti nella directory **dist** dovranno essere utilizzati nella fase successiva di dispiegamento di GovWay

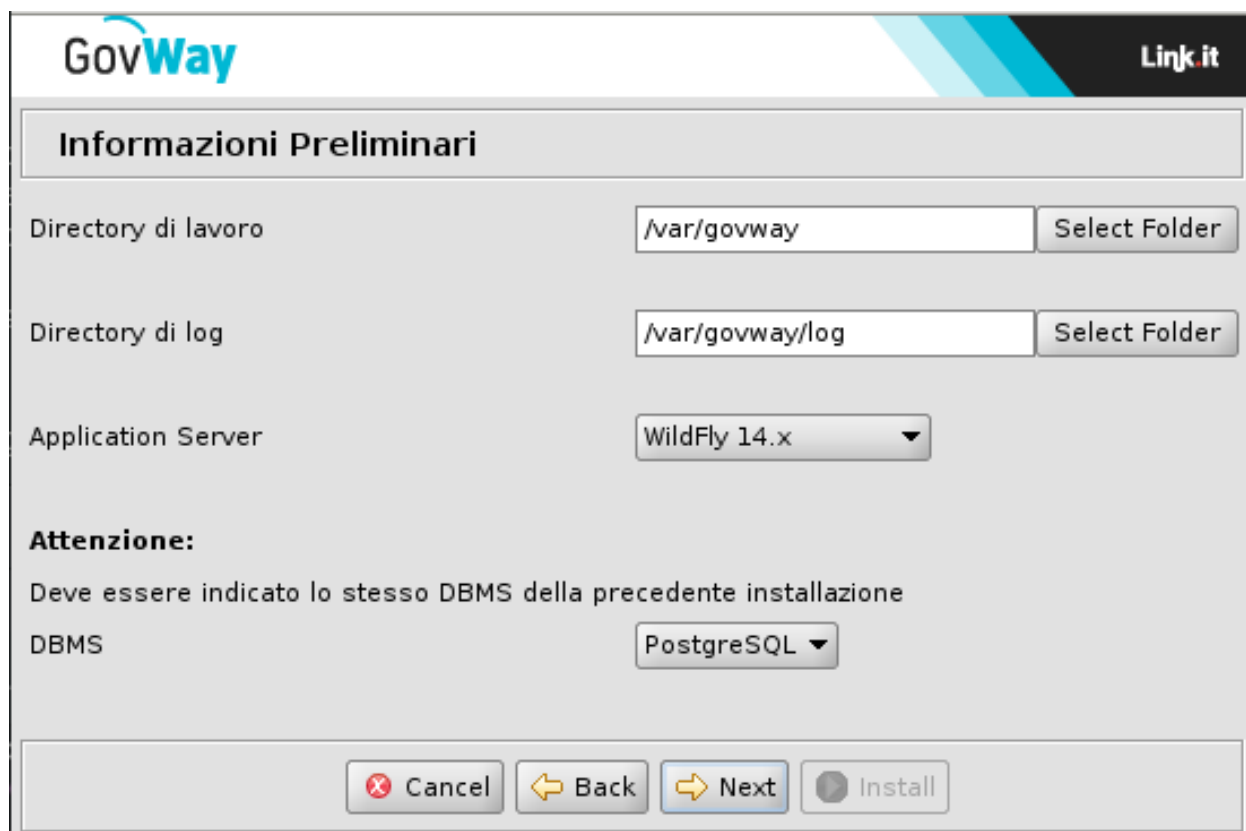
3.2 Aggiornamento

Supponiamo che la scelta sia quella di aggiornare una installazione precedente. Vediamo come si sviluppa il processo per differenza rispetto al caso di una nuova installazione:

1. Il primo passo è quello di indicare la versione di GovWay da cui si parte per l'aggiornamento.
2. Al passo successivo, dove si indicano le informazioni preliminari, vi è il vincolo di indicare la medesima piattaforma database utilizzata per l'installazione che si vuole aggiornare.
3. Nel successivo passo è possibile indicare se tra gli archivi generati devono essere inclusi i servizi che permettono la configurazione ed il monitoraggio di GovWay tramite API REST.
4. Nella maschera che permette la scelta dei profili di interoperabilità, vi è il vincolo di indicare almeno i medesimi profili utilizzati per l'installazione che si vuole aggiornare.
5. I rimanenti passaggi sono uguali al caso della nuova installazione con la differenza che non sarà disponibile la funzione per impostare le credenziali dei cruscotti grafici.



Fig. 3.12: Scelta versione precedente



The screenshot shows the 'Informazioni Preliminari' (Preliminary Information) window of the GovWay installer. The window has a header with the 'GovWay' logo on the left and the 'Link.it' logo on the right. The main area contains several configuration fields:

- Directory di lavoro** (Working Directory): A text box containing '/var/govway' and a 'Select Folder' button.
- Directory di log** (Log Directory): A text box containing '/var/govway/log' and a 'Select Folder' button.
- Application Server**: A dropdown menu currently showing 'WildFly 14.x'.
- Attenzione:** (Attention:) A section with the text 'Deve essere indicato lo stesso DBMS della precedente installazione' (The same DBMS must be indicated as the previous installation).
- DBMS**: A dropdown menu currently showing 'PostgreSQL'.

At the bottom of the window is a bar with four buttons: 'Cancel' (with a red X icon), 'Back' (with a left arrow icon), 'Next' (with a right arrow icon and highlighted in blue), and 'Install' (with a play button icon).

Fig. 3.13: Scelta piattaforma database identica all'installazione di provenienza

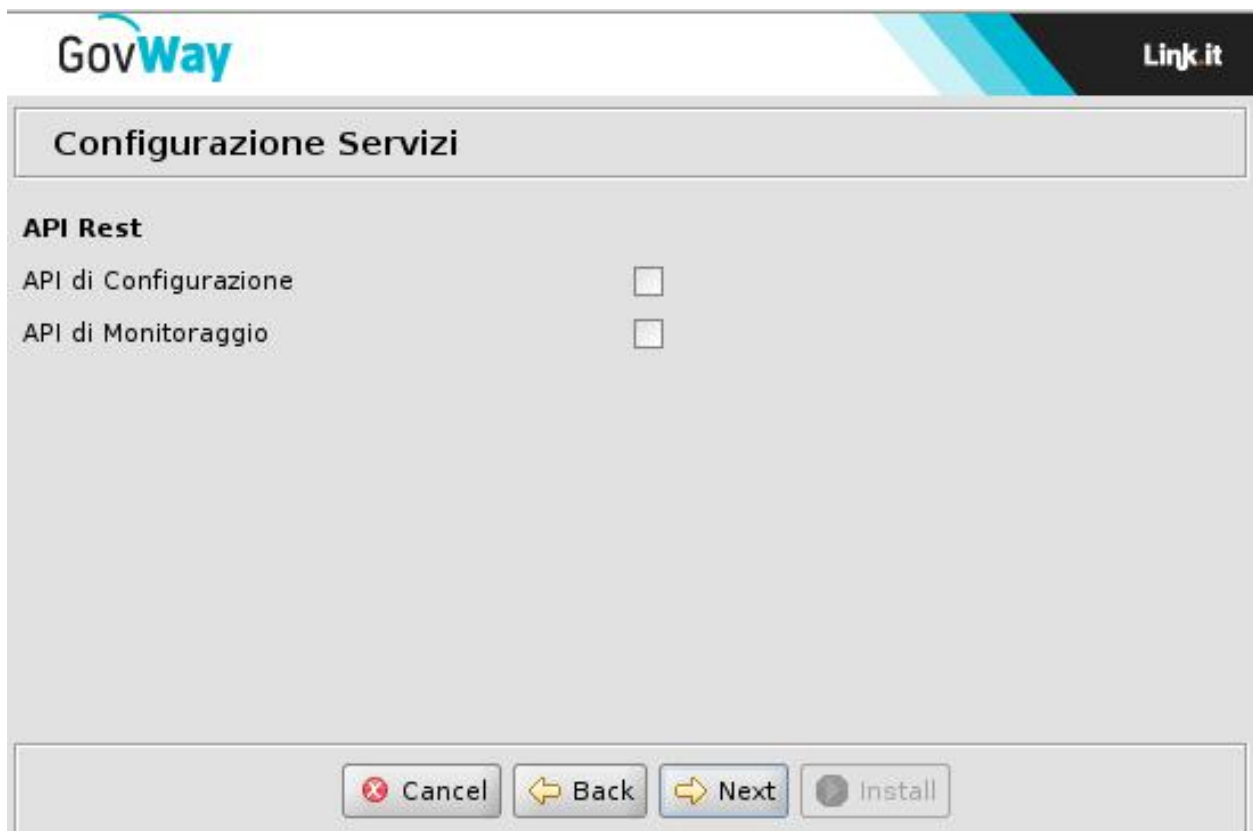
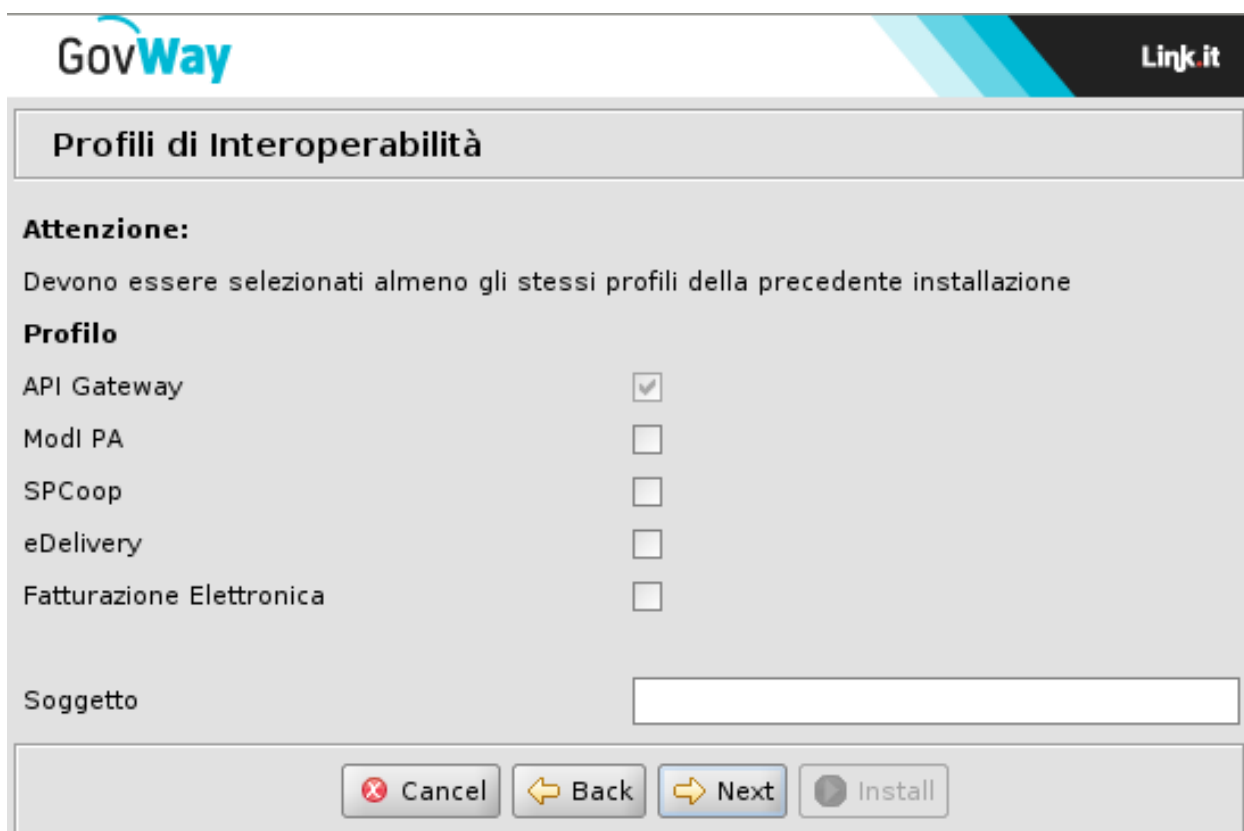


Fig. 3.14: Configurazione Servizi



GovWay **Link.it**

Profili di Interoperabilità

Attenzione:
Devono essere selezionati almeno gli stessi profili della precedente installazione

Profilo

API Gateway	<input checked="" type="checkbox"/>
ModI PA	<input type="checkbox"/>
SPCoop	<input type="checkbox"/>
eDelivery	<input type="checkbox"/>
Fatturazione Elettronica	<input type="checkbox"/>

Soggetto

Fig. 3.15: Scelta Profilo di Interoperabilità

Fase di Dispiegamento

Al termine dell'esecuzione dell'utility di installazione vengono prodotti i files necessari per effettuare il dispiegamento nell'ambiente di esercizio. Tali files sono disponibili nella directory *dist*.

Il processo di dispiegamento del software si distingue nei casi di nuova installazione e aggiornamento. Le sezioni seguenti illustrano i due casi.

4.1 Nuova Installazione

Per completare il processo di installazione si devono effettuare i passi seguenti:

1. Creare un utente sul RDBMS avente i medesimi valori di username e password indicati in fase di setup.
2. Creare un database, per ospitare le tabelle dell'applicazione, avente il nome indicato durante la fase di setup. Il charset da utilizzare è UTF-8.
3. Impostare i permessi di accesso in modo che l'utente creato al passo 1 abbia i diritti di lettura/scrittura sul database creato al *passo 2*. Si può consultare un esempio relativo a questi primi 3 passi, riferito alla piattaforma PostgreSQL, in sezione *Esempio di setup del database PostgreSQL*.

4. Eseguire lo script *sql/GovWay.sql* per la creazione dello schema del database.

Successivamente eseguire lo script *sql/GovWay_init.sql* per inserire i dati di inizializzazione del database.

Ad esempio, nel caso di PostgreSQL, si potranno eseguire i comandi:

- `psql <hostname> <username> -f sql/GovWay.sql`
- `psql <hostname> <username> -f sql/GovWay_init.sql`

5. Installare il DriverJDBC, relativo al tipo di RDBMS indicato in fase di setup, nella directory:

- `<WILDFLY_HOME>/standalone/deployments`, nel caso di Wildfly.
- `<TOMCAT_HOME>/lib`, nel caso di Tomcat.

6. Per le connessioni al database è necessario configurare i seguenti datasource impostati con i parametri forniti durante l'esecuzione dell'utility di installazione:

- Il gateway necessita di un datasource con nome JNDI:
 - *org.govway.datasource*
- Le console grafiche necessitano di un datasource con nome JNDI:
 - *org.govway.datasource.console*
- Nel caso si sia richiesto il supporto al protocollo eDelivery, è necessario un terzo datasource con nome JNDI:
 - *org.govway.datasource.console.domibus*

I datasource, preconfigurati per l'Application Server indicato, sono disponibili nella directory *datasource* e contengono le configurazioni di accesso al database indicate (ip, db_name, utenza, password). Tali files possono essere utilizzati come riferimento per la definizione dei datasource richiesti nelle modalità disponibili per l'Application Server scelto. Tali files possono anche essere utilizzati direttamente per un rapido dispiegamento copiandoli nelle seguenti posizioni nel file system:

- *<WILDFLY_HOME>/standalone/deployments*, nel caso di Wildfly.
- *<TOMCAT_HOME>/conf/Catalina/localhost*, nel caso di Tomcat

Utilizzando i file preconfigurati, su WildFly è necessario sostituire al loro interno il placeholder *NOME_DRIVER_JDBC.jar* con il nome del driver JDBC installato in precedenza.

7. Eseguire il dispiegamento delle applicazioni presenti nella directory *archivi* secondo le modalità disponibili per l'Application Server scelto. Per un rapido dispiegamento è possibile copiare gli archivi nelle seguenti posizioni nel file system:

- *<WILDFLY_HOME>/standalone/deployments*, nel caso di Wildfly.
- *<TOMCAT_HOME>/webapps*, nel caso di Tomcat

8. Verificare che la directory di lavoro di GovWay, fornita con le informazioni preliminari dell'utility di installazione, esista o altrimenti crearla con permessi tali da consentire la scrittura all'utente di esecuzione dell'application server
9. Copiare nella directory di lavoro tutti i files di configurazioni presenti nella directory *cfg*. Ad esempio con il comando:

- *cp cfg/*.properties /etc/govway/*

La directory di destinazione deve essere accessibile in lettura all'utente con cui si esegue l'Application Server.

10. Avviare l'application server con il relativo service oppure utilizzando la linea di comando:

- *<WILDFLY_HOME>/bin/standalone.sh*, nel caso di Wildfly.
- *<TOMCAT_HOME>/bin/startup.sh*, nel caso di Tomcat.

4.2 Aggiornamento

Sulla base delle scelte operate sulle maschere del wizard, nella directory *dist* saranno presenti i file necessari per procedere all'aggiornamento richiesto.

L'aggiornamento richiede i seguenti step:

- Fermo dell'Application Server
- *Aggiornamento del database*
- *Aggiornamento dei datasource*

- *Aggiornamento degli archivi applicativi*
- *Aggiornamento dei file di properties*
- Riavvio dell'Application Server

4.2.1 Aggiornamento del database

Nella sottodirectory *sql* si trovano gli script SQL da eseguire sul database attualmente utilizzato per adeguarlo alla nuova versione:

1. Eseguire lo script *sql/GovWay_upgrade_<new-version>.sql* per aggiornare lo schema del database.
2. Se sono stati selezionati nuovi profili di interoperabilità rispetto alla precedente installazione, devono essere eseguiti anche gli script:
 - *sql/profilo/GovWay_upgrade_initialize-profilo-<new-profile>.sql*
3. Se si è modificata la tipologia di Application Server rispetto a quella utilizzata nell'installazione precedente (es. da jboss a tomcat), deve anche essere eseguito lo script:
 - *sql/utilities/as/upgradeAS_to<new-type>.sql*

4.2.2 Aggiornamento dei datasource

Nella sottodirectory *datasource* si trovano le configurazioni dei datasource automaticamente generate in base ai dati di connessione al database forniti e all'Application Server indicato. Se non è stato modificato l'Application Server, rispetto a quello utilizzato nell'attuale installazione, un aggiornamento dei datasource non è necessario. Eventualmente confrontare i dati di configurazione dei datasource generati dall'installer con i dati degli attuali datasource presenti nell'Application Server per verificare che non esistano differenze. Se necessario aggiornare questi elementi, procedere come indicato per questa attività nella Sezione *Nuova Installazione*.

4.2.3 Aggiornamento degli archivi applicativi

Eseguire il dispiegamento delle applicazioni presenti nella sottodirectory *archivi* secondo le modalità disponibili per l'Application Server scelto. Per un rapido dispiegamento è possibile copiare gli archivi nelle seguenti posizioni del file system:

- wildfly: WILDFLY_HOME/standalone/deployments/
- tomcat: TOMCAT_HOME/webapps/

4.2.4 Aggiornamento dei file di properties

Nella sottodirectory *cfg* si trovano i template dei file di properties esterni. Questi file, durante l'installazione del prodotto, sono già stati copiati nella directory di lavoro di GovWay. Tali file di properties hanno lo scopo di fornire all'utente dei file pre-confezionati, con proprietà commentate, da utilizzare rapidamente secondo quanto descritto nei manuali d'utilizzo del prodotto, per modificare eventuali configurazioni built-in. Non è quindi indispensabile che tali file vengano riportati sull'installazione precedente e soprattutto occorre fare attenzione a non sovrascrivere eventualmente i precedenti, se erano stati modificati rispetto al template iniziale (generato dall'installer).

Nota: Nella sottodirectory *cfg/utilities/diff* vengono riportate solamente le modifiche attuate sui file, rispetto alla versione precedente, nel formalismo «diff» (estensione .diff) o il file intero (estensione .properties) se si tratta di un file che non esisteva nella precedente versione

Verifica dell'Installazione

Appena conclusa la fase di dispiegamento si può procedere con l'avvio dell'application server, quindi:

1. Verificare che la *govwayConsole*, l'applicazione web per la gestione di GovWay, sia accessibile tramite browser all'indirizzo: *http://<hostname-pdd>/govwayConsole*. In caso di corretto funzionamento verrà visualizzata la schermata seguente:



The screenshot shows a web browser window displaying the 'GovWay - Console di Gestione' login page. The page has a dark blue header with the title 'GovWay - Console di Gestione'. Below the header is a white login form with a 'Login' label, two input fields for 'Login' and 'Password', and a 'Login' button. At the bottom of the page is the 'Link.it' logo.

Fig. 5.1: Verifica Installazione: govwayConsole

2. Accedere alla govwayConsole utilizzando le credenziali fornite durante l'esecuzione dell'installer.

3. Verificare che la *govwayMonitor*, l'applicazione web per il monitoraggio di GovWay, sia accessibile tramite browser all'indirizzo: `http://<hostname-pdd>/govwayMonitor`. In caso di corretto funzionamento verrà visualizzata la schermata seguente:



Fig. 5.2: Verifica Installazione: govwayMonitor

4. Accedere alla *govwayMonitor* utilizzando le credenziali fornite durante l'esecuzione dell'installer.
5. Se durante l'esecuzione dell'Installer è stato indicato di generare il servizio che consente la configurazione tramite API REST, in caso di corretto funzionamento sarà possibile scaricare l'interfaccia OpenAPI v3. L'interfaccia nel formato yaml sarà disponibile all'indirizzo:
 - `http://<hostname-pdd>/govwayAPIConfig/openapi.yaml`L'interfaccia nel formato json sarà disponibile all'indirizzo:
 - `http://<hostname-pdd>/govwayAPIConfig/openapi.json`
6. Se durante l'esecuzione dell'Installer è stato indicato di generare il servizio che consente il monitoraggio tramite API REST, in caso di corretto funzionamento sarà possibile scaricare l'interfaccia OpenAPI v3. L'interfaccia nel formato yaml sarà disponibile all'indirizzo:
 - `http://<hostname-pdd>/govwayAPIMonitor/openapi.yaml`L'interfaccia nel formato json sarà disponibile all'indirizzo:
 - `http://<hostname-pdd>/govwayAPIMonitor/openapi.json`

Finalizzazione dell'Installazione

Terminati i passi descritti nelle precedenti sezioni, GovWay è pienamente operativo e può essere utilizzato per proteggere le proprie API. Il prodotto viene dispiegato con dei parametri di configurazione che possiedono dei valori di default relativamente alle seguenti tematiche:

1. *URL di Invocazione*

Per conoscere l'url di invocazione di una API protetta da GovWay è possibile accedere al dettaglio di una erogazione o fruizione tramite la `govwayConsole`. L'url fornita avrà un prefisso `http://localhost:8080/govway`.

Se il gateway è stato dispiegato in modo da essere raggiungibile tramite un host, porta o contesto differente è possibile configurare tale prefisso seguendo le indicazioni descritte nella sezione *Url di Invocazione*.

2. *Multi-Tenant*

I processi di configurazione e monitoraggio attuabili tramite le console sono ottimizzati nell'ottica di gestire sempre un unico dominio rappresentato da un soggetto interno il cui nome è stato fornito durante l'esecuzione dell'installer (Fig. 3.7).

Per estendere l'ambito delle configurazioni e del monitoraggio tramite console a più di un soggetto interno al dominio seguire le indicazioni presenti nella sezione *Multi-Tenant*.

3. *Gestione CORS*

Nella configurazione di default di GovWay è abilitata la gestione del *cross-origin HTTP request (CORS)*; è possibile modificarne la configurazione seguendo le indicazioni presenti nella sezione *Gestione CORS*.

4. *Rate Limiting - Numero Complessivo Richieste Simultanee*

GovWay permette definire un rate limiting sulle singole erogazioni o fruizioni di API. Le metriche utilizzabili riguardano il numero di richieste all'interno di un intervallo temporale, l'occupazione di banda, il tempo di risposta etc.

Oltre al rate limiting GovWay consente di fissare un numero limite complessivo, indipendente dalle APIs, riguardo alle richieste gestibili simultaneamente dal gateway, bloccando le richieste in eccesso.

Per default GovWay è configurato per gestire simultaneamente al massimo 200 richieste. Per modificare tale configurazione seguire le indicazioni presenti nella sezione *Rate Limiting - Numero Complessivo Richieste Simultanee*.

5. *Tempi Risposta*

GovWay è preconfigurato con dei parametri di timeout per quanto concerne la gestione delle connessioni verso gli applicativi interni (erogazioni) o esterni (fruizioni) dal dominio di gestione. Per effettuare un tuning di tali parametri seguire le indicazioni descritte nella sezione [Tempi Risposta](#).

6. *Caching della Risposta - Disk Cache*

In GovWay è possibile abilitare il salvataggio delle risposte in una cache sia globalmente, in modo che sia attivo per tutte le APIs, che singolarmente sulla singola erogazione o fruizione. Questa funzionalità permette ad un backend server di non dover riprocessare le stesse richieste più volte.

La configurazione di default prevede di salvare in una cache, che risiede in memoria RAM, fino a 5.000 risposte (ogni risposta comporta il salvataggio di due elementi in cache). In caso venga superato il numero massimo di elementi che possano risiedere in cache, vengono eliminate le risposte meno recenti secondo una politica *LRU*.

GovWay consente di personalizzare la configurazione della cache in modo da aggiungere una memoria secondaria dove salvare gli elementi in eccesso. Per abilitare la memoria secondaria seguire le indicazioni descritte nella sezione [Caching della Risposta - Disk Cache](#).

7. *Configurazione e Monitoraggio*

GovWay fornisce sia una console che dei servizi che espongono API REST per la sua configurazione e per il monitoraggio. L'installer genera per default le console mentre i servizi devono essere selezionati puntualmente dall'utente ([Fig. 3.6](#)).

Gli indirizzi per accedere alle console sono già stati forniti nella fase di [Verifica dell'Installazione](#).

Nel caso invece siano stati generati i servizi, gli indirizzi base per utilizzarli sono:

- <http://<hostname-pdd>/govway/ENTE/api-config/v1/>
- <http://<hostname-pdd>/govway/ENTE/api-monitor/v1/>

ma deve essere completata la configurazione del Controllo degli Accessi per poterli invocare correttamente seguendo le indicazioni descritte nella sezione [Configurazione e Monitoraggio](#).

8. *Load Balancing*

Il prodotto è preconfigurato per funzionare su di una singola istanza. Per realizzare un'installazione in load balancing seguire le indicazioni descritte nella sezione [Configurazione in Load Balancing](#).

9. *Configurazione HTTPS*

GovWay processa ogni richiesta in una duplice veste agendo sia da server al momento della ricezione della richiesta che da client al momento di inoltrare la richiesta verso i backend applicativi.

In entrambi i ruoli la configurazione varia a seconda dell'architettura in cui è stato dispiegato GovWay (es. presenza di un Web Server). Indicazioni sulla configurazione vengono fornite nella sezione [Configurazione HTTPS](#).

6.1 Url di Invocazione

Per scoprire quale sia la url di una API protetta da GovWay da fornire ai client esterni, il gestore può utilizzare la `govwayConsole`, la quale fornisce nella visualizzazione del dettaglio di una erogazione o fruizione di API la url di invocazione (es. [Fig. 6.1](#)).

L'url fornita ha per default un prefisso `http://localhost:8080/govway` che può non andar bene se il gateway è stato dispiegato in modo da essere raggiungibile tramite un host, porta o contesto differente.

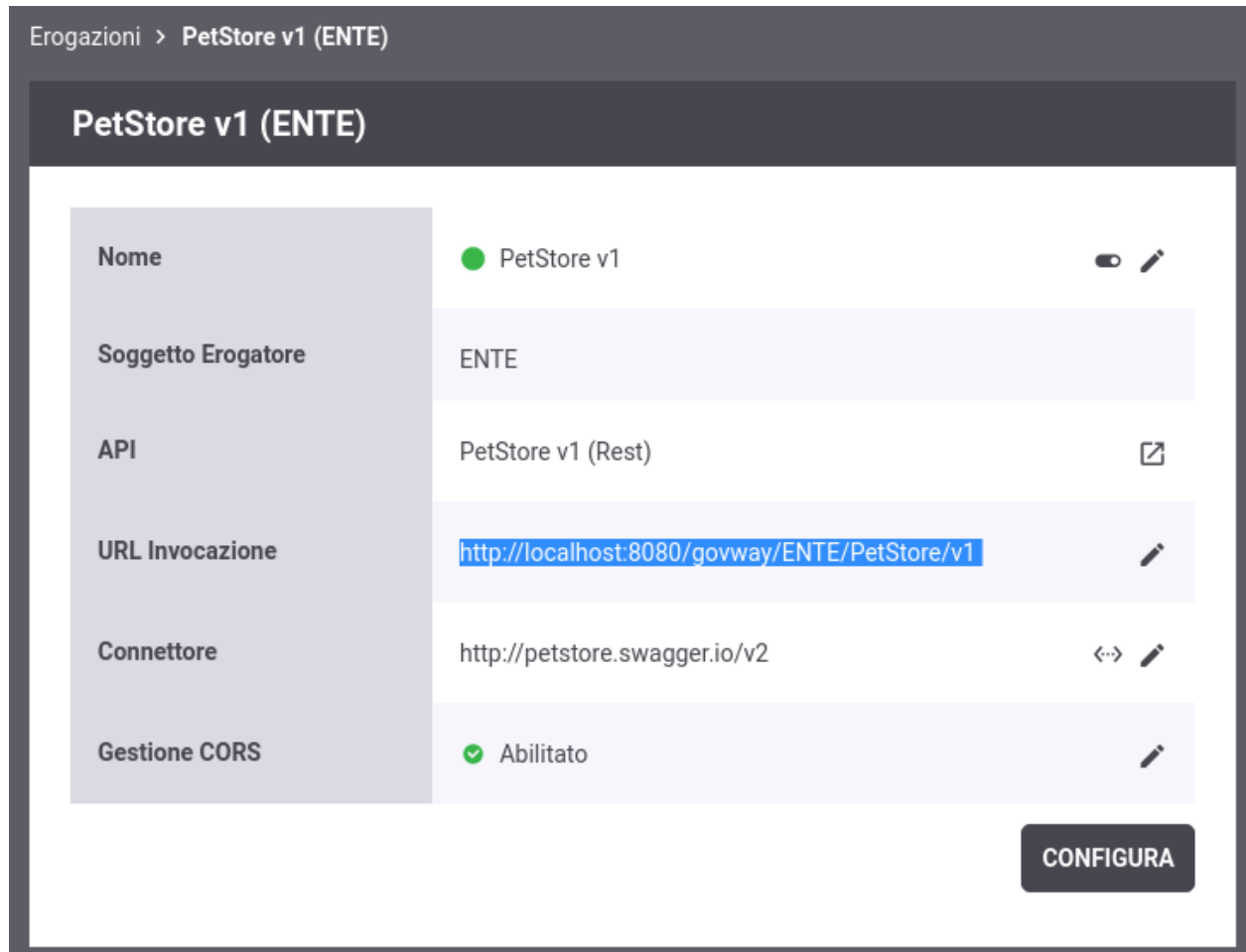
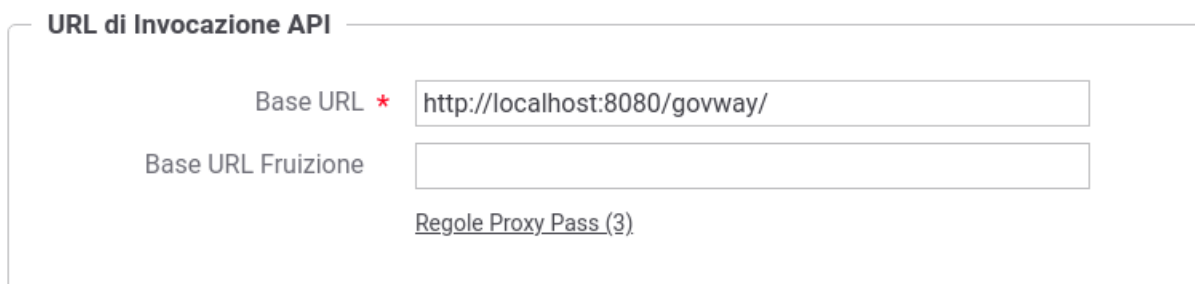


Fig. 6.1: Url di Invocazione di una Erogazione

Per modificare i prefissi delle url di invocazioni accedere alla voce “*Configurazione - Generale*” del menù (sezione *configGenerale_urlInvocazione*). Nella sezione “*URL di Invocazione API*” è possibile configurare i prefissi di una erogazione e di una fruizione. Inoltre in presenza di un reverse proxy che media le comunicazioni http con GovWay, è anche possibile configurare opportunamente le url di invocazione delle API esposte da GovWay allineandole con le eventuali configurazioni specifiche realizzate sul reverse proxy.



URL di Invocazione API

Base URL *

Base URL Fruizione

[Regole Proxy Pass \(3\)](#)

Fig. 6.2: Configurazione prefissi per le Url di Invocazione

6.2 Multi-Tenant

I processi di configurazione e monitoraggio attuabili tramite le console sono ottimizzati nell’ottica di gestire sempre un unico dominio rappresentato da un soggetto interno il cui nome è stato fornito durante l’esecuzione dell’installer (Fig. 3.7). In tal senso, le fruizioni e le erogazioni si intendono sempre in soggettiva riguardo un singolo soggetto interno amministrato dall’utente in sessione.

La funzionalità Multi-Tenant è un’opzione che consente di estendere l’ambito delle configurazioni prodotte dalla govwayConsole a più di un soggetto interno al dominio. Tale opzione si attiva accedendo alla voce “*Configurazione - Generale*” del menù, sezione “*Multi-Tenant*”.



Multi-Tenant

Stato **abilitato**

Fruizioni

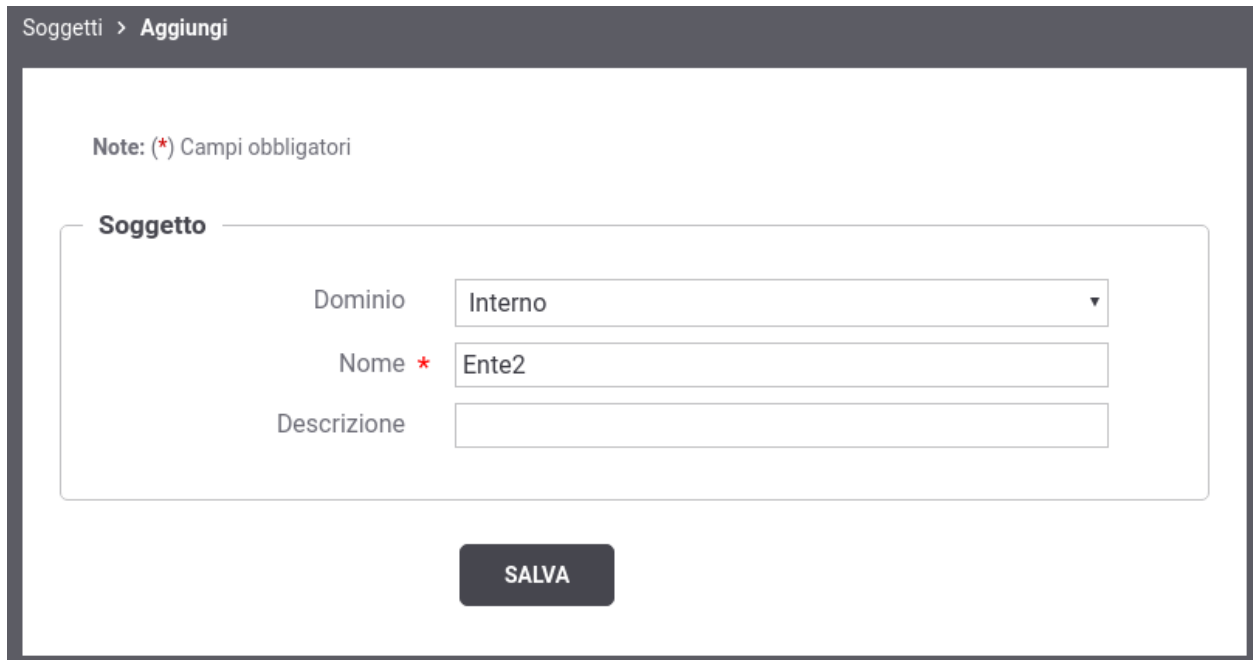
Soggetto Erogatore

Erogazioni

Soggetti Fruttori

Fig. 6.3: Abilitazione Multi-Tenant

Una volta abilitato accedere alla voce “*Soggetti*” del menù e selezionare il pulsante “*Aggiungi*” per registrare un nuovo soggetto interno (nuovo dominio).



The screenshot shows a web interface for adding a new subject. At the top, there is a breadcrumb 'Soggetti > Aggiungi'. Below it, a note states 'Note: (*) Campi obbligatori'. The main form is titled 'Soggetto' and contains three input fields: 'Dominio' with a dropdown menu currently showing 'Interno', 'Nome' with a red asterisk and the value 'Ente2', and 'Descrizione' which is empty. A dark 'SALVA' button is positioned at the bottom center of the form.

Fig. 6.4: Registrazione nuovo Soggetto

Terminata la registrazione del nuovo soggetto sia nella console di gestione (*govwayConsole*) che nella console di monitoraggio (*govwayMonitor*) prima di procedere con qualsiasi operazione è adesso possibile selezionare il soggetto per cui si intende gestire il dominio attraverso l'apposito menù situato in alto a destra nell'intestazione delle console.

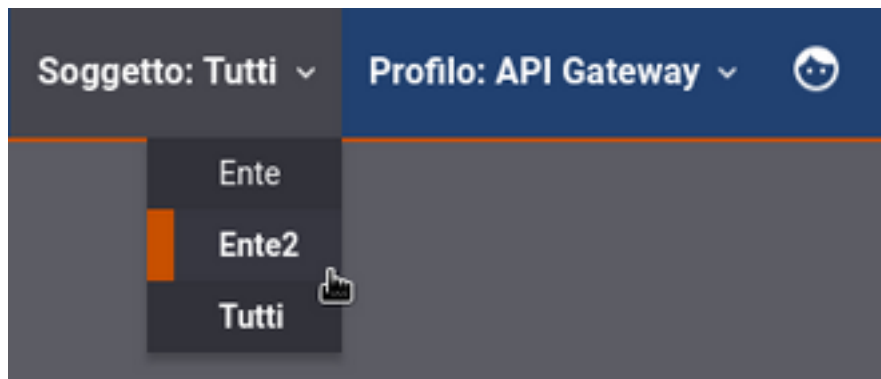


Fig. 6.5: Selezione del Soggetto

6.3 Gestione CORS

In GovWay è possibile abilitare la gestione del *cross-origin HTTP request (CORS)* sia globalmente, in modo che sia valida per tutte le APIs, che singolarmente sulla singola erogazione o fruizione.

Nell'installazione di default è abilitata la gestione del CORS globalmente per tutte le API. Tale configurazione è modificabile accedendo alla voce “*Configurazione - Generale*” del menù, sezione “*Gestione CORS*”.

Gestione CORS

Stato: abilitato

Tipo: Gestito dal Gateway

Access Control

All Allow Origins: ☒

Allow Headers *: SOAPAction x Content-Type x

Allow Methods *: POST x PUT x GET x DELETE x

Allow Credentials: ☐

Fig. 6.6: Gestione CORS

6.4 Rate Limiting - Numero Complessivo Richieste Simultanee

GovWay consente di fissare un numero limite complessivo, indipendente dalle singole APIs, riguardo alle richieste gestibili simultaneamente dal gateway, bloccando le richieste in eccesso. Nell'installazione di default tale limite è fissato a 200 richieste simultanee.

Il limite deve essere allineato rispetto al numero di connessioni simultanee consentite dal frontend web e/o dall'applicazione server. Ad esempio su tomcat tale parametro è configurabile all'interno del file *conf/server.xml* nell'attributo *maxThreads* degli elementi *connector*.

Per modificare la configurazione sul numero limite di richieste simultanee accedere alla voce “*Configurazione - Controllo Traffico*” del menù, sezione “*Limitazione Numero di Richieste Complessive*”.

6.5 Tempi Risposta

GovWay è preconfigurato con dei valori di timeout riguardanti i tempi di risposta dei servizi con cui il gateway interagisce durante l'elaborazione delle richieste. Nel caso delle erogazioni, si tratta dei tempi di risposta dei servizi interni al dominio, successivamente ad una richiesta di erogazione dall'esterno. Nel caso delle fruizioni, si tratta dei tempi di risposta dei servizi esterni, successivamente ad una richiesta di fruizione da parte di un client interno al dominio. I tempi configurabili sono:

Limitazione Numero di Richieste Complessive

Stato

Max Richieste Simultanee *

[Visualizza Informazioni Runtime](#)

Fig. 6.7: Numero Richieste Simultanee

- *Connection Timeout (ms)*: Intervallo di tempo atteso, sulle comunicazioni in uscita, prima di sollevare l'errore Connection Timeout (scadenza del tempo di attesa per stabilire una connessione).
- *Read Timeout (ms)*: Intervallo di tempo atteso, dopo aver stabilito una connessione in uscita, prima di sollevare l'errore di Read Timeout (scadenza del tempo di attesa per ricevere il payload dall'interlocutore).
- *Tempo Medio di Risposta (ms)*: Valore di soglia del tempo medio di risposta al fine di valutare la situazione di *Degrado Prestazionale*, condizione per l'applicabilità di eventuali politiche restrittive di rate limiting (per ulteriori dettagli si rimanda alla guida utente).

6.6 Caching della Risposta - Disk Cache

In GovWay è possibile abilitare il salvataggio delle risposte in una cache. Questa funzionalità permette ad un backend server di non dover riprocessare le stesse richieste più volte.

La configurazione di default prevede di salvare in una cache, che risiede in memoria RAM, fino a 5.000 risposte (ogni risposta comporta il salvataggio di due elementi in cache). In caso venga superato il numero massimo di elementi che possano risiedere in cache, vengono eliminate le risposte meno recenti secondo una politica *LRU*.

Per modificare la configurazione della cache in modo da aggiungere una memoria secondaria dove salvare gli elementi in eccesso è possibile agire sul file `<directory-lavoro>/govway_local.jcs.properties` scommentando le seguenti:

```
jcs.region.responseCaching=responseCachingDiskCache
jcs.region.responseCaching.elementattributes.IsSpool=true
```

Per ulteriori dettagli sui parametri di configurazione della memoria secondaria si rimanda alla documentazione della cache <http://commons.apache.org/proper/commons-jcs/IndexedDiskCacheProperties.html>.

La libreria di caching utilizzata da GovWay, (*JCS*: <http://commons.apache.org/proper/commons-jcs/>) consente di definire diversi tipi di memoria secondaria. Per ulteriori dettagli su come abilitare i vari tipi di memoria si rimanda alla documentazione: <http://commons.apache.org/proper/commons-jcs/JCSPlugins.html>.

Nota: Accedendo alla sezione “Configurazione - Generale”, tramite l'utilizzo della *govwayConsole* in modalità *avanzata*, è possibile modificare i parametri di configurazione (numero di elementi e politica di svecchiamento) della cache che risiede in memoria RAM tramite la sezione “Cache (Risposte)”.

Tempi Risposta

Fruizioni

Connection Timeout *
Indicazione in millisecondi (ms)

Read Timeout *
Indicazione in millisecondi (ms)

Tempo Medio di Risposta *
Indicazione in millisecondi (ms)

Erogazioni

Connection Timeout *
Indicazione in millisecondi (ms)

Read Timeout *
Indicazione in millisecondi (ms)

Tempo Medio di Risposta *
Indicazione in millisecondi (ms)

Fig. 6.8: Tempi Risposta

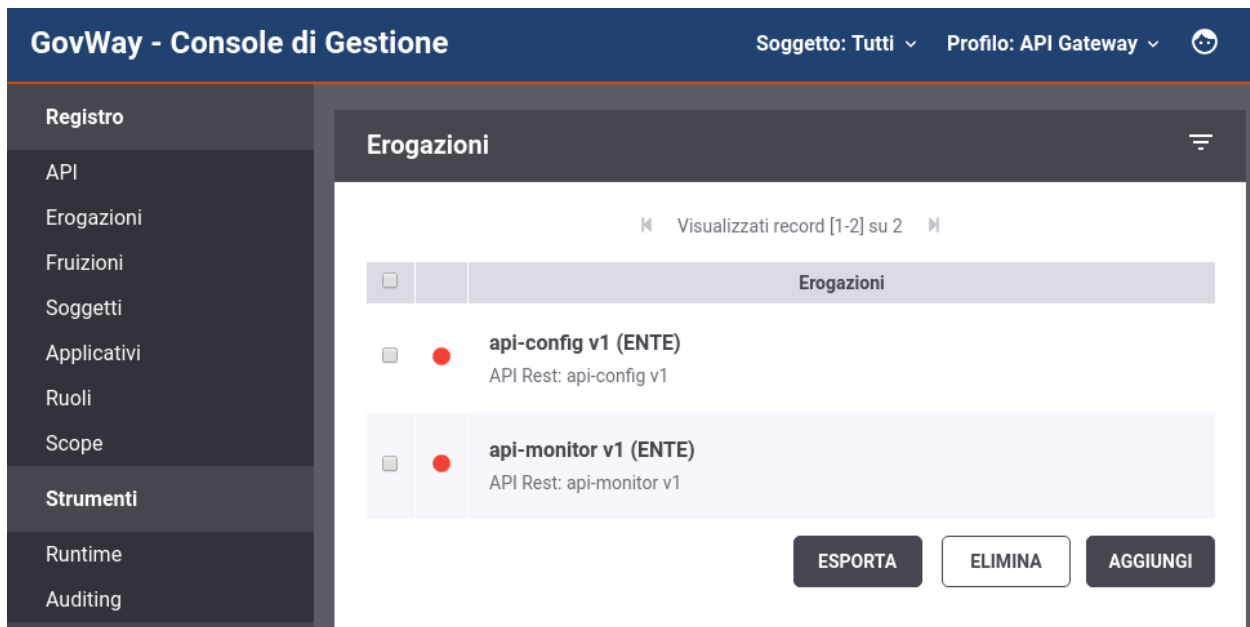
6.7 Configurazione e Monitoraggio

Se nell'installer sono stati selezionati i servizi che espongono API REST per la configurazione e il monitoraggio di GovWay (Fig. 3.6) gli indirizzi base per utilizzarli sono:

- `http://<hostname-pdd>/govway/ENTE/api-config/v1/`
- `http://<hostname-pdd>/govway/ENTE/api-monitor/v1/`

Per poterli invocare deve prima essere completata la configurazione del Controllo degli Accessi accedendo alla console di gestione tramite browser all'indirizzo `http://<hostname-pdd>/govwayConsole` utilizzando le credenziali fornite durante l'esecuzione dell'installer.

Accendendo alla lista delle Erogazioni si può notare come le API relative alla configurazione ed al monitoraggio riportano uno "stato rosso" che evidenzia una configurazione incompleta.



Procedere con la configurazione del `apiGwControlloAccessi` di ogni API al fine di renderla invocabile dall'esterno secondo le modalità di autenticazione ed autorizzazione desiderate. Per maggiori informazioni sul *Controllo degli Accessi* si rimanda alla Guida della Console di Gestione.

6.8 Configurazione in Load Balancing

Per realizzare un'installazione in load balancing è necessario predisporre più istanze dell'Application Server, ognuna con una propria installazione del software. Sarà inoltre necessario:

1. Che tutte le istanze di GovWay siano configurate per condividere lo stesso DB.
2. Che esista un Load Balancer in grado di bilanciare il flusso di richieste in arrivo sulle varie istanze di AS ospitanti il software GovWay.
3. Che GovWay sia opportunamente configurato con un identificatore unico che contraddistingua lo specifico nodo.

In particolare per realizzare la configurazione descritta al punto 3, è necessario:

1. Editare il file <directory-lavoro>/govway_local.properties aggiungendo la seguente riga:

```
# Identificativo univoco della macchina
org.openspcoop2.pdd.cluster_id=#IDGW#
```

inserendo al posto di #IDGW# l'identificatore unico associato alla specifica istanza che si sta configurando. Scegliere un identificativo con cui si possa facilmente riconoscere la macchina, ad esempio l'hostname.

2. Nel caso del protocollo SPCoop, editare il file <directory-lavoro>/spcoop_local.properties aggiungendo le seguenti righe:

```
# Tipo di generazione dell'identificativo
org.openspcoop2.protocol.spcoop.id.tipo=static
# Prefisso dell'identificativo (opzionale)
org.openspcoop2.protocol.spcoop.id.prefix=#NUMERO#
```

inserendo al posto di #NUMERO# l'identificatore unico associato a quella istanza (da 0 a 99). Scegliere un identificativo numerico progressivo, a partire da 0, per ciascuna istanza del software GovWay nel cluster.

3. Effettuata la modifica dei files è necessario un riavvio dell'Application Server per rendere operative le modifiche.

NOTA: La directory "<directory-lavoro>" è la directory contenente tutti i files di configurazione. Verificare quale directory è stata indicata durante l'esecuzione del setup (vedi Esecuzione dell'Installer).

6.8.1 Configurazione delle Console

La configurazione del Load Balancing si completa fornendo ulteriori dati di configurazione alle console grafiche. Queste configurazioni consentono alle console di avere i corretti riferimenti ai nodi presenti in modo da poter dettagliare questo aspetto nelle proprie maschere ed inoltre poter propagare eventuali modifiche su ogni nodo senza attendere il timeout della cache o richiedere riavvii dell'AS.

A tale scopo sarà necessario:

1. Editare il file <directory-lavoro>/govway_local.properties aggiungendo le seguenti righe su ogni PdD in Load Balancing:

```
# JMX Resources
org.openspcoop2.pdd.check.readJMXResources.enabled=true
org.openspcoop2.pdd.check.readJMXResources.username=#USERNAME#
org.openspcoop2.pdd.check.readJMXResources.password=#PASSWORD#
```

inserendo al posto di #USERNAME# e #PASSWORD# le credenziali che dovranno essere utilizzate dalle console e che dovranno essere configurate nei punti successivi di questo paragrafo.

2. Editare il file <directory-lavoro>/console_local.properties aggiungendo le seguenti righe al fine di configurare la govwayConsole:

```
# Configurazione gateway in Load Balancing
risorseJmxPdd.tipoAccesso=openspcoop
risorseJmxPdd.alias=#IDGW1#, ..., #IDGWN#
```

Devono essere elencati tutti gli identificativi, di ogni nodo gateway in Load Balancing, descritti in precedenza e registrati nella proprietà:

```
org.openspcoop2.pdd.cluster_id del file govway_local.properties
```

Per ogni identificativo devono inoltre essere fornite le seguenti informazioni:


```
# Configurazione IDGW1
#IDGW1#.risorseJmxPdd.descrizione=#DESCRIZIONEGW1#
#IDGW1#.risorseJmxPdd.remoteAccess.url=http://#HOSTGW1#:#PORTGW1#/govway/check
#IDGW1#.risorseJmxPdd.remoteAccess.username=#USERNAMEGW1#
#IDGW1#.risorseJmxPdd.remoteAccess.password=#PASSWORDGW1#
...
# Configurazione IDGWN
#IDGWN#.risorseJmxPdd.descrizione=#DESCRIZIONEGWN#
#IDGWN#.risorseJmxPdd.remoteAccess.url=http://#HOSTGWN#:#PORTGWN#/govway/check
#IDGWN#.risorseJmxPdd.remoteAccess.username=#USERNAMEGWN#
#IDGWN#.risorseJmxPdd.remoteAccess.password=#PASSWORDGWN#
```

Devono essere elencati inserendo al posto di #USERNAMEGW# e #PASSWORDGW# le credenziali utilizzate in precedenza nel file:

```
govway_local.properties, proprietà
org.openspcoop2.pdd.check.readJMXResources.username e
org.openspcoop2.pdd.check.readJMXResources.password
```

Indicare inoltre al posto di #HOSTGW# e #PORTGW# l'hostname e la porta con cui è raggiungibile GovWay. Infine deve anche essere fornita una descrizione per ogni nodo in Load Balancing al posto di #DESCRIZIONEGW#.

3. Editare il file <directory-lavoro>/monitor_local.properties Disabilitare la configurazione per la singola istanza commentando la proprietà "statoPdD.sonde.standard.Gateway.url":

```
# Configurazione PdD in Singola Istanza
#statoPdD.sonde.standard.Gateway.url=http://127.0.0.1:8080/govway/check
```

Aggiungere le seguenti righe al fine di configurare la govwayMonitor per il Load Balancing:

```
# Configurazione PdD in Load Balancing
configurazioni.risorseJmxPdd.tipoAccesso=openspcoop
configurazioni.risorseJmxPdd.alias=IDGW1, .., IDGWN
statoPdD.sonde.standard.nodi=IDGW1, .., IDGWN
transazioni.idCluster.useSondaPdDList=true
```

Devono essere elencati tutti gli identificativi, di ogni PdD in Load Balancing, registrati nel file govway_local.properties nella proprietà "org.openspcoop2.pdd.cluster_id" come descritto in precedenza. Per ogni identificativo devono inoltre essere fornite le seguenti informazioni:

```
# Configurazione IDGW1
statoPdD.sonde.standard.#IDGW1#.url=http://#HOSTGW1#:#PORTGW1#/govway/check
#IDGW1#.configurazioni.risorseJmxPdd.remoteAccess.url=http://#HOSTGW1#:#PORTGW1/
↪govway/check
#IDGW1#.configurazioni.risorseJmxPdd.remoteAccess.username=#USERNAMEGW1#
#IDGW1#.configurazioni.risorseJmxPdd.remoteAccess.password=#PASSWORDGW1#
...
# Configurazione IDGWN
statoPdD.sonde.standard.#IDGWN#.url=http://#HOSTGWN#:#PORTGWN#/govway/check
#IDGWN#.configurazioni.risorseJmxPdd.tipoAccesso=openspcoop
#IDGWN#.configurazioni.risorseJmxPdd.remoteAccess.url=http://#HOSTGWN#:#PORTGWN/
↪govway/check
#IDGWN#.configurazioni.risorseJmxPdd.remoteAccess.username=#USERNAMEGWN#
#IDGWN#.configurazioni.risorseJmxPdd.remoteAccess.password=#PASSWORDGWN#
```

Devono essere elencati inserendo al posto di #USERNAMEGW# e #PASSWORDGW# le credenziali utilizzate in precedenza nel file:

```
govway_local.properties, proprietà  
org.openspcoop2.pdd.check.readJMXResources.username e  
org.openspcoop2.pdd.check.readJMXResources.password
```

Indicare inoltre al posto di #HOSTGW# e #PORTGW# l'hostname e la porta con cui è raggiungibile GovWay.

6.9 Configurazione HTTPS

GovWay processa ogni richiesta in una duplice veste agendo sia da server al momento della ricezione della richiesta che da client al momento di inoltrare la richiesta verso i backend applicativi.

In entrambi i ruoli la configurazione varia a seconda dell'architettura in cui è stato dispiegato GovWay (es. presenza di un Web Server). Nelle sezioni successive vengono forniti dettagli su come è possibile attuare la configurazione sia quando GovWay agisce da server che quando agisce da client.

6.9.1 Comunicazioni in Ingresso

La configurazione varia a seconda se la terminazione ssl è gestita direttamente sull'application server (wildfly o tomcat) o viene gestita da un frontend http (Apache httpd, IIS, etc).

Wildfly

Nota: La seguente sezione fornisce degli esempi utili ad attuare la configurazione https. Per conoscere maggiori dettagli e modalità di configurazioni differenti fare riferimento a quanto indicato nella documentazione ufficiale dell'Application Server Wildfly (<http://wildfly.org>).

La configurazione può essere attuata nel file standalone.xml che si trova all'interno della cartella "WILD-FLY_HOME/standalone/configuration/".

- Deve prima essere definito un security realm contenente il certificato che il server deve esporre, aggiungendolo ai security realms esistenti.

```
<security-realms>  
  <security-realm name="mySecurityRealm">  
    <server-identities>  
      <ssl>  
        <keystore path="/etc/govway/keys/govway_server.  
↪jks" keystore-password="changeit"  
        alias="aliasInKeystore" key-password=  
↪"changeit" />  
      </ssl>  
    </server-identities>  
  </security-realm>  
  ...  
</security-realms>
```

se oltre ad esporre un certificato server, si deve autenticare il certificato client del chiamante, la configurazione del security realm deve essere estesa con la definizione di un trustStore che contenga i certificati necessari a validarli.

```

<security-realms>
  <security-realm name="mySecurityRealmClientAuth">
    <server-identities>
      <ssl>
        <keystore path="/etc/govway/keys/govway_https_
↪server.jks" keystore-password="changeit"
                                alias="aliasInKeystore" key-password=
↪"changeit" />
      </ssl>
    </server-identities>
    <authentication>
      <truststore path="/etc/govway/keys/govway_https_
↪truststore.jks" keystore-password="changeit"/>
    </authentication>
  </security-realm>
  ...
</security-realms>

```

- Il security realm creato deve essere associato ad un “https-listener”.

```

<https-listener name="httpsGovWay" socket-binding="httpsGovWay" security-
↪realm="mySecurityRealm"/>

```

Per rendere obbligatorio che il chiamante debba fornire un proprio certificato client deve essere aggiunto l’attributo “verify-client” valorizzato con il valore “REQUIRED”. Se tale attributo viene valorizzato invece con il valore “REQUESTED” il certificato client non è obbligatorio ma verrà comunque validato, se presente.

```

<https-listener name="httpsGovWayClientAuth" socket-binding=
↪"httpsGovWayClientAuth" security-realm="mySecurityRealmClientAuth"
↪verify-client="REQUIRED"/>

```

- Si deve infine associare al socket-binding indicato nell’https listener una porta su cui l’application server gestisce le richieste https.

```

<socket-binding name="httpsGovWayClientAuth" port="${jboss.https.
↪port:8445}"/>

```

Tomcat

Nota: La seguente sezione fornisce degli esempi utili ad attuare la configurazione https. Per conoscere maggiori dettagli e modalità di configurazioni differenti fare riferimento a quanto indicato nella documentazione ufficiale dell’Application Server Apache Tomcat (<http://tomcat.apache.org>).

La configurazione può essere attuata nel file server.xml che si trova all’interno della cartella “TOMCAT_HOME/conf”.

Deve essere definito un connettore contenente il certificato che il server deve esporre e la porta su cui deve gestire le richieste https.

```

<Connector port="8445" protocol="HTTP/1.1" SSLEnabled="true"
  strategy="ms" maxHttpHeaderSize="8192"
  emptySessionPath="true"
  scheme="https" secure="true" clientAuth="false" sslProtocol = "TLS"
  keyAlias="aliasInKeystore"
  keystoreFile="/etc/govway/keys/govway_https_server.jks"
  keystorePass="changeit"/>

```

Nota: Nell'esempio fornito la password della chiave privata del certificato server deve coincidere con la password del keystore.

Per rendere obbligatorio che il chiamante debba fornire un proprio certificato client:

- deve essere abilitato l'attributo "clientAuth".

```
<Connector port="8445" ... clientAuth="true" .../>
```

- deve essere fornito un trustStore che contenga i certificati necessari a validarli i certificati client ricevuti. Il trustStore deve essere fornito attraverso le proprietà java "javax.net.ssl.trustStore" e "javax.net.ssl.trustStorePassword". Per farlo è possibile ad esempio aggiungere la seguente riga al file "TOMCAT_HOME/bin/setenv.sh" (creare il file se non esiste):

```
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore=/etc/govway/keys/govway_
↪https_truststore.jks -Djavax.net.ssl.trustStorePassword=changeit"
```

Frontend HTTP

Nel caso in cui la terminazione ssl viene gestita su un frontend http (Apache httpd, IIS, etc) GovWay necessita di ricevere i certificati client per attuare il processo di autenticazione https.

Nel caso di utilizzo di una integrazione "mod_jk" tra frontend e application server, GovWay riceve i certificati gestiti sul frontend http in maniera trasparente e non sono richieste ulteriori configurazioni.

Negli altri casi invece deve essere configurato opportunamente il frontend http per inoltrare i certificati client o il DN attraverso header HTTP a GovWay. Si rimanda alla documentazione ufficiale del frontend utilizzato su come attivare tale funzionalità. Di seguito invece vengono fornite indicazioni su come configurare GovWay per recepire le informazioni dagli header inoltrati dal frontend.

Integrazione Frontend - GovWay

Nota: Gli esempi forniti descrivono una configurazione valida per le erogazioni. È sufficiente utilizzare il prefisso "org.openspcoop2.pdd.services.pd." invece di "org.openspcoop2.pdd.services.pa." per adeguare la configurazione alle fruizioni.

Per abilitare il processamento degli header inoltrati dal frontend è necessario editare il file <directory-lavoro>/govway_local.properties .

1. Abilitare la proprietà "org.openspcoop2.pdd.services.pa.gestoreCredenziali.enabled"

```
# Mediazione tramite WebServer (Erogazioni)
org.openspcoop2.pdd.services.pa.gestoreCredenziali.enabled=true
# Nome del WebServer che media le comunicazioni https con GovWay
org.openspcoop2.pdd.services.pa.gestoreCredenziali.nome=#FRONTEND-NAME#
```

inserendo al posto di #FRONTEND-NAME# il nome associato al frontend che verrà utilizzato nella diagnostica di GovWay.

2. Se il frontend inserisce in header http il DN del Subject e/o dell'Issuer relativo ai certificati client autenticati, deve essere indicato il nome di tali header tramite la seguente configurazione:

```
# DN del Subject e dell'Issuer tramite gli header:
org.openspcoop2.pdd.services.pa.gestoreCredenziali.header.ssl.subject=#SUBJECT_
↳HEADER-NAME#
org.openspcoop2.pdd.services.pa.gestoreCredenziali.header.ssl.issuer=#ISSUER_
↳HEADER-NAME#
```

inserendo al posto di #SUBJECT_HEADER-NAME# il nome dell'header http utilizzato per propagare il DN del Subject (es. "SSL_CLIENT_S_DN") e al posto di #ISSUER_HEADER-NAME# il nome dell'header http utilizzato per propagare il DN dell'Issuer (es. SSL_CLIENT_I_DN). È possibile anche attuare una configurazione dove viene processato solamente il Subject, lasciando commentata la proprietà relativa all'Issuer.

3. Nel caso il frontend inserisce in un header http il certificato x.509 del client autenticato, deve essere indicato il nome di tale header tramite la seguente configurazione:

```
# Certificato tramite l'header:
org.openspcoop2.pdd.services.pa.gestoreCredenziali.header.ssl.certificate=#CLIENT-
↳CERT_HEADER-NAME#
# Indicazione se l'header valorizzato con il certificato è url encoded:
org.openspcoop2.pdd.services.pa.gestoreCredenziali.header.ssl.certificate.url_
↳decode=false
# Indicazione se l'header valorizzato con il certificato è base64 encoded:
org.openspcoop2.pdd.services.pa.gestoreCredenziali.header.ssl.certificate.base64_
↳decode=false
```

inserendo al posto di #CLIENT-CERT_HEADER-NAME# il nome dell'header http utilizzato per propagare il certificato x.509 (es. "SSL_CLIENT_CERT"). Il certificato inserito nell'header http dal frontend può essere stato codificato in base64 e/o tramite url encoding. È possibile effettuare la decodifica abilitando la proprietà "org.openspcoop2.pdd.services.pa.gestoreCredenziali.header.ssl.certificate.base64_decode" e/o la proprietà org.openspcoop2.pdd.services.pa.gestoreCredenziali.header.ssl.certificate.url_decode.

4. Se il frontend inserisce in header http il principal dell'identità relativa al chiamante, deve essere indicato il nome di tale header tramite la seguente configurazione:

```
# L'identità del chiamante può essere fornita dal WebServer anche come_
↳informazione 'principal' tramite il seguente header:
org.openspcoop2.pdd.services.pa.gestoreCredenziali.header.principal=#PRINCIPAL_
↳HEADER-NAME#
```

inserendo al posto di #PRINCIPAL_HEADER-NAME# il nome dell'header http utilizzato dal frontend.

6.9.2 Comunicazioni in Uscita

Le comunicazioni in uscita utilizzano una configurazione ssl differente a seconda dell'impostazione utilizzata nei connettori configurati per ogni API.

GovWay consente di indicare esplicitamente, nella configurazione di un connettore, i keystore e truststore da utilizzare. Per questa modalità seguire le indicazioni riportate nella Guida alla Console di Gestione, nella sezione "Funzionalità Avanzate - Connettori" al paragrafo avanzate_connettori_https.

In alternativa, se viene solamente indicato un endpoint https senza fornire keystore specifici per l'API, GovWay eredita la configurazione https impostata nella JVM dell'Application Server per la quale viene fornito un esempio di configurazione.

Configurazione HTTPS della JVM

Nota: La seguente sezione fornisce degli esempi utili ad attuare la configurazione https. Per conoscere maggiori dettagli e modalità di configurazioni differenti fare riferimento a quanto indicato nella documentazione ufficiale della JVM e dell'Application Server utilizzato.

- Deve essere fornito un trustStore che contenga i certificati necessari a validare i certificati server ricevuti. Il trustStore deve essere fornito attraverso le proprietà java “javax.net.ssl.trustStore”, “javax.net.ssl.trustStorePassword” e “javax.net.ssl.trustStoreType”. Per farlo è possibile ad esempio aggiungere la seguente riga al file “TOMCAT_HOME/bin/setenv.sh” per Tomcat o al file “WILDFLY_HOME/bin/standalone.conf” per Wildfly:

```
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStore=/etc/govway/keys/govway_
↪https_truststore.jks -Djavax.net.ssl.trustStorePassword=changeit -
↪Djavax.net.ssl.trustStoreType=jks"
```

- Deve essere fornito un keyStore che contenga il certificato client utilizzato da GovWay. Il keyStore deve essere fornito attraverso le proprietà java “javax.net.ssl.keyStore”, “javax.net.ssl.keyStorePassword” e “javax.net.ssl.keyStoreType”. Per farlo è possibile ad esempio aggiungere la seguente riga al file “TOMCAT_HOME/bin/setenv.sh” per Tomcat o al file “WILDFLY_HOME/bin/standalone.conf” per Wildfly:

```
JAVA_OPTS="$JAVA_OPTS -Djavax.net.ssl.keyStore=/etc/govway/keys/govway_
↪https_keystore.p12 -Djavax.net.ssl.keyStorePassword=changeit -Djavax.
↪net.ssl.keyStoreType=pkcs12"
```

Nota: La password della chiave privata del certificato client deve coincidere con la password del keystore.

Esempio di setup del database PostgreSQL

Procedura indicativa, applicabile alla piattaforma RDBMS PostgreSQL, per la redistribuzione del database di GovWay:

1. Creazione Utente

```
[user@localhost]$ su
Parola d'ordine: XXX
[root@localhost]# su - postgres
-bash-3.1$ createuser -P
Enter name of role to add: govway
Enter password for new role: govway
Conferma password: govway
Shall the new role be a superuser? (y/n) n
Shall the new role be allowed to create databases? (y/n) n
Shall the new role be allowed to create more new roles? (y/n) n
CREATE ROLE
```

2. Creazione Database

```
[user@localhost]$ su
Parola d'ordine: XXX
[root@localhost]# su - postgres
-bash-3.1$ createdb -E UTF8 -O govway govway
CREATE DATABASE
```

3. Abilitazione accesso dell'utente al Database, è possibile abilitare l'accesso editando il file */var/lib/pgsql/data/pg_hba.conf* (come super utente). Abilitiamo quindi l'utente govway ad accedere al db govway, aggiungendo le seguenti righe al file:

```
local govway govway md5
host govway govway 127.0.0.1 255.255.255.255 md5
```