Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Un modello tecnologico per il dispiegamento di servizi di Fascicolo Sanitario Elettronico dell'infrastruttura InFSE su piattaforma Cloud

Angelo Esposito, Mario Sicuranza, Mario Ciampi

RT-ICAR-NA-2013-04 **Novembre 2013**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) – Sede di Napoli, Via P. Castellino 111, I-80131 Napoli, Tel: +39-0816139508, Fax: +39-0816139531, e-mail: napoli@icar.cnr.it, URL: *www.na.icar.cnr.it*

Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Un modello tecnologico per il dispiegamento di servizi di Fascicolo Sanitario Elettronico dell'infrastruttura InFSE su piattaforma Cloud

Angelo Esposito, Mario Sicuranza, Mario Ciampi

Rapporto Tecnico N: **RT-ICAR-NA-2013-04** ***Data:*** **Novembre 2013**

Un modello tecnologico per il dispiegamento di servizi di Fascicolo Sanitario Elettronico dell'infrastruttura InFSE su piattaforma Cloud

Angelo Esposito, Mario Sicuranza, Mario Ciampi

Istituto di Calcolo e Reti ad Alte Prestazioni, Consiglio Nazionale delle Ricerche
Via Pietro Castellino, 111 – 80131 Napoli, Italia
E-mail: {angelo.esposito, mario.sicuranza, mario.ciampi}@na.icar.cnr.it

Abstract

L'uso del Cloud Computing per l'erogazione dei servizi del Fascicolo Sanitario Elettronico (FSE) risulta di particolare interesse per gli enormi benefici portati dall'adozione di tale paradigma.

In questo lavoro, è stato predisposto un ambiente prototipale di testing per l'erogazione dei servizi del FSE in ambiente Cloud.

L'obiettivo di questo lavoro è stato duplice, da una parte dimostrare la fattibilità dell'uso del Cloud nell'erogazione dei servizi FSE, dall'altro aprire alla sperimentazione di tale modello nell'ambito Cloud con benefici concreti sull'interoperabilità tra le diverse soluzioni di FSE nell'ambito nazionale ed internazionale.

Keywords: Cloud, Fascicolo Sanitario Elettronico, Interoperabilità, InFSE.

Introduzione

Dall'analisi svolta nel rapporto tecnico [1], è evidente quanto il Cloud rappresenti una tecnologia particolarmente vantaggiosa da utilizzare nel contesto e-health. Per dimostrare la possibilità concreta dell'uso del Cloud ai fini dell'erogazione dei servizi del Fascicolo sanitario Elettronico (FSE), è stato predisposto un ambiente prototipale dell'Infrastruttura tecnologica del FSE (InFSE) su Cloud. L'infrastruttura InFSE è stata sviluppata nell'ambito di diversi progetti di ricerca condotti dall'Istituto di Calcolo e Reti ad Alte prestazioni del CNR in collaborazione con il Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione Tecnologica della Presidenza del Consiglio dei Ministri.

Il documento si compone di cinque capitoli. Nel primo sono presentate brevemente le componenti dell'infrastruttura tecnologica InFSE. Nel secondo capitolo sono descritte le scelte intraprese per la predisposizione dei servizi di FSE su Cloud. Il terzo capitolo descrive il modello tecnologico proposto per il dispiegamento dei servizi InFSE su piattaforma Cloud, evidenziando in particolare le modalità di installazione delle componenti sulla piattaforma offerta da Amazon. Il quarto capitolo mostra uno scenario di test riguardante il recupero di documenti sanitari disponibili nella piattaforma Cloud. Infine, il quinto capitolo conclude il rapporto tecnico.

1. Componenti del modello InFSE

Per comprendere lo scenario prototipale del FSE predisposto su Cloud è necessaria una breve trattazione delle componenti che costituiscono il modello infrastrutturale InFSE.

Il modello architetturale di InFSE rispecchia, nel suo complesso, un'architettura orientata ai servizi (Service-Oriented Architecture, SOA). Tale architettura è organizzata su tre livelli (three layers) ed è mostrata in Figura 1.

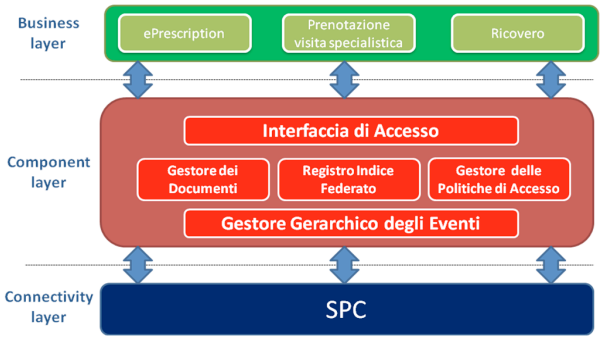

Figura 1 – Architettura multi-layers di InFSE

Il **Connectivity layer** è rappresentato dal Sistema Pubblico di Connettività[1] per la cooperazione applicativa tra le Pubbliche Amministrazioni mediante busta eGov[2]. In particolare, tutte le interazioni interregionali devono avvenire attraverso una Porta di Dominio[3].

Il **Component layer** è costituito dalle componenti infrastrutturali di InFSE, che sono:

- **Interfaccia di Accesso:** questa componente funge da interfaccia all'Infrastruttura del Fascicolo Sanitario Elettronico. Essa deve essere presente presso ogni nodo regionale e, opzionalmente, presso i nodi locali. L'interfaccia di accesso di un nodo regionale è la componente che riceve tutte le richieste avanzate dagli attori regionali (es. Medico di Medicina Generale) e dalle Interfacce di Accesso dei nodi delle altre Regioni o Province Autonome. A fronte di una richiesta, l'Interfaccia di Accesso del nodo regionale orchestra una serie di interazioni con le altre componenti dell'Infrastruttura al fine di soddisfare la richiesta.

- **Registro Indice Federato:** il Registro Indice Federato è una componente atta a memorizzare una serie di informazioni (metadati) inerenti i documenti sanitari archiviati nei repository, al fine di facilitarne la ricerca e la localizzazione. Tali informazioni possono riguardare la tipologia del documento, l'identificativo del paziente, l'autore del documento, l'organizzazione incaricata della custodia del documento, l'identificativo del documento, etc. Il Registro Indice Federato è una componente composta da un insieme di interfacce che interagiscono con i registri secondo un modello federato. Gli utenti possono accedere al sistema attraverso qualsiasi registro e, in generale, ognuno di questi mantiene solo le informazioni inerenti al dominio di pertinenza. Pertanto, è possibile ottenere i metadati inerenti ai documenti disponibili presso i domini regionali interrogando i corrispondenti registri regionali mediante apposite interfacce del Registro Indice Federato, eseguendo in tal modo una ricerca federata.

- **Gestore Gerarchico degli Eventi:** il Gestore Gerarchico degli Eventi è una componente opzionale che effettua il routing e la notifica degli eventi sanitari a tutti gli attori interessati (medici di medicina generale, medici specialisti, etc.). Il modello adottato è il publish/subscribe basato su broker.

- **Gestore dei Documenti:** il Gestore dei Documenti deve memorizzare in maniera persistente, affidabile e sicura i documenti creati da un utente autorizzato ad ogni occorrenza di un evento sanitario di un assistito. Tale memorizzazione deve avvenire all'interno di opportuni repository. Questi ultimi sono localizzati presso i nodi locali o regionali. Le principali operazioni che il Gestore dei Documenti deve offrire sono le seguenti:
    - reperimento di uno o più documenti sanitari disponibili in un repository a partire da un riferimento;

[1] Sistema Pubblico di Connettività (SPC): è un insieme di infrastrutture tecnologiche e di regole tecniche che ha lo scopo di "federare" le infrastrutture ICT delle pubbliche amministrazioni al fine di realizzare servizi integrati mediante regole e servizi condivisi.

[2] Busta e-Gov: I messaggi scambiati tra Enti e PA attraverso le Porte di Dominio, sono racchiusi in una Busta (Busta di e-Gov) costituita da un uso della struttura SOAP 1.1 con estensioni. Tale Busta è logicamente suddivisa in due parti, una parte che contiene tipicamente informazioni infrastrutturali, ed una parte di contenuto dipendente dal servizio applicativo oggetto della interazione.

[3] Porta di dominio: è un elemento fondamentale dell'infrastruttura SPCOOP, grazie al quale è possibile effettuare la cooperazione tra enti attraverso la trasmissione di messaggi nel formato della busta e-gov.

- archiviazione di un documento sanitario all'interno di un repository.

Ogni nodo dell'Infrastruttura, sia esso locale o regionale, può interagire con i repository, attraverso le componenti Gestore dei Documenti. Il Gestore dei Documenti può quindi essere installato presso il nodo regionale o presso i nodi locali.

- **Gestore delle Politiche di Accesso: i**l Gestore delle Politiche di Accesso è responsabile degli aspetti generali di sicurezza sia per i servizi infrastrutturali che per quelli di tipo applicativo. L'approccio adottato segue il paradigma *security as a service*, tipico delle architetture orientate ai servizi, per l'implementazione di un Single Sign-On (SSO). L'autorizzazione per l'accesso al servizio sarà richiesta sulla base di particolari attributi quali ad esempio il ruolo dell'operatore, il tipo di documento, il contesto d'uso, la struttura organizzativa che detiene il documento e così via.

Infine, il **Business layer** definisce i servizi di supporto ai processi sanitari quali, ad esempio, l'ePrescription, la prenotazione di una visita specialistica, il recupero del Patient Summary, etc.

2. Scelte progettuali per la predisposizione dei servizi di FSE su Cloud

In questo paragrafo sono illustrate le scelte adottate per la predisposizione dei servizi di FSE su ambiente Cloud.

Piattaforma Cloud: Amazon Web Services (AWS) ElasticBeanstalk[4]. Questo tipo di servizio messo a disposizione da Amazon Web Services consente lo sviluppo e la gestione di applicazioni in ambiente Cloud in modo del tutto trasparente rispetto all'infrastruttura HW/SW sulla quale sono eseguite tali applicazioni. AWS ElasticBeanstalk riduce la complessità di gestione senza restringere le scelte o il controllo dell'ambiente Cloud. Pertanto, ElasticBeanstalk risulta uno dei servizi più adatti alla definizione di prototipi su Cloud.

Componenti InFSE: Interfaccia di Accesso, Registro Indice Federato, Gestore dei Documenti, Gestore delle Politiche di Accesso: Il dispiegamento delle componenti in ambiente cloud è del tutto simile per ogni componente del modello InFSE, pertanto a titolo esemplificativo in questo lavoro si descrive l'installazione in ambiente Cloud solo di una delle componenti del modello: il "Gestore dei Documenti".

Modello di servizio: IAAS[5]. Considerando la soluzione InFSE, che fornisce servizi a livello infrastrutturale in maniera modulare e flessibile, la scelta del modello di servizio di tipo IAAS ha permesso un deployment senza alterare le potenzialità offerte dalla infrastruttura InFSE e allo stesso tempo con impatto minimo sulle modifiche alle componenti deployate in ambiente Cloud.

Tipologia di Cloud: Public Cloud[6]. Per una prototipazione del modello InFSE in ambiente cloud si è scelto di adottare un Public Cloud che offrisse servizi avanzati per il deployment delle applicazioni. È importante comunque menzionare che è possibile adottare la tipologia di Cloud che si ritiene più opportuna e vicina alle proprie esigenze in maniera analoga.

3. Approccio per il deployment del modello InFSE su Cloud

L'infrastruttura InFSE prevede un dispiegamento delle componenti del modello su due livelli, il primo è relativo ai nodi locali che possono essere assistiti o completi e che rappresentano le Aziende Sanitarie Locali o le Aziende Ospedaliere (ASL/AO), il secondo relativo ai nodi regionali che essendo nodi completi prevedono il deployment di tutte le componenti del modello InFSE.

[4] **AWS Elastic Beanstalk:** è uno dei sevizi web Services messi a disposizione da Amazon per la gestione automatizzata e il caricamento diretto mediante interfaccia Web dell'applicazioni realizzate.

[5] **IAAS:** è un modello di servizio offre una infrastruttura tecnologica (Hardware) con capacità computazionale, di memorizzazione e di rete, sulla quale l'utente può installare ed eseguire il software a lui necessario (dal sistema operativo alle applicazioni).

[6] **Public Cloud**: è uno dei modelli di dispiegamento dei servizi su cloud. I servizi Cloud Pubblici sono offerti da fornitori che mettono a disposizione degli utenti/clienti (che ne fanno richiesta) le risorse hardware e software dei loro data center.

L'interazione tra le componenti per la ricerca e il recupero di un documento nel Repository in uno dei nodi locali è rappresentato in Figura 2.

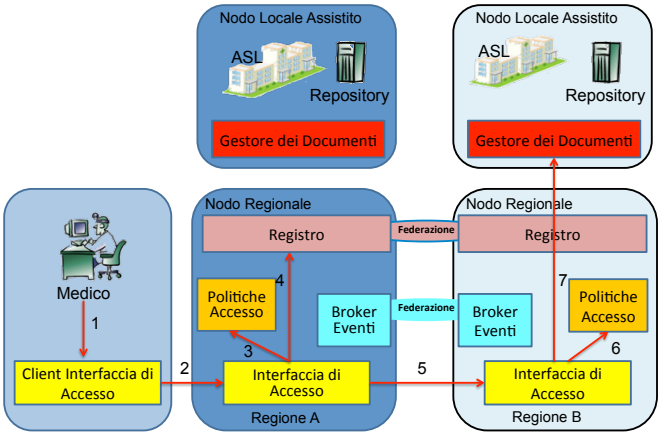

Figura 2 – Interazione delle componenti InFSE sulla funzione di ricerca e recupero di un documento

Il dispiegamento dell'architettura prototipale InFSE su Cloud, realizzata in questo lavoro e l'interazione tra le componenti del modello, nel contesto Cloud, ai fini della ricerca e recupero di un documento sanitario registrato nel repository di un nodo locale, è rappresentato in Figura 3.

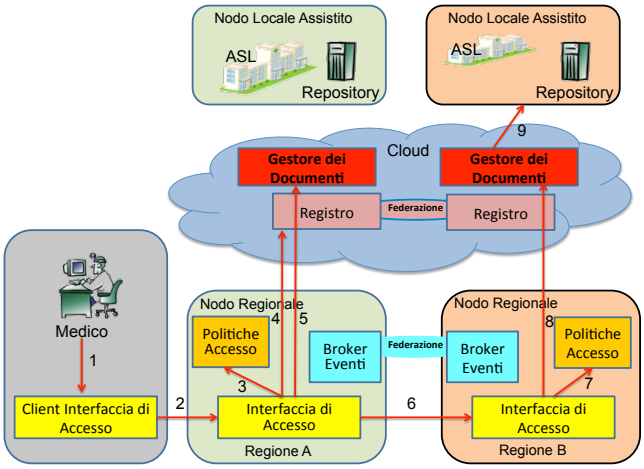

Figura 3 – Interazione delle componenti InFSE sulla funzione di recupero di un documento su Cloud

3.1 Installazione delle componenti del FSE su Amazon ElasticBeanStalk

In questo paragrafo è illustrata la configurazione dell'ambiente ElasticBeanStalk per l'installazione della componente "Gestore dei Documenti" di InFSE. Il dispiegamento delle altre componenti del modello InFSE è del tutto simile a quello trattato in questo lavoro.
Prima del deployment del "Gestore dei Documenti" sono necessari dei passaggi di pre-configurazione dell'ambiente di ElasticBeanStalk. Questi ultimi sono descritti nel prossimo paragrafo.

3.1.1 Pre-configurazione dell'ambiente di Amazon ElasticBeanStalk

Il servizio AWS mette a disposizione una dashboard chiamata Amazon Elastic Compute Cloud (EC2), tramite la quale è possibile svolgere tutte le principali funzioni per la gestione degli strumenti forniti.
Per avere accesso alle macchine in ambiente Cloud è necessario:

- creare una coppia di chiavi (privata e pubblica) per stabilire una connessione sicura da remoto con le macchine disponibili in ambiente Cloud. La coppia di chiavi può essere creata dal pannello di gestione *EC2* selezionando la voce *Key Pairs*.
- creare un Security Group e aggiungere l'indirizzo ip della macchina dalla quale si effettua l'accesso alle macchine in Cloud. Infatti, per accedere alle macchine in ambiente Cloud è necessario che tale indirizzo della macchina dalla quale ci si collega deve appartenere ad un Security Group associato all'ambiente Cloud. Il Security Group può essere creato dal pannello *Security Group* in *EC2*.

Una volta creato il Security Group è sufficiente aggiungere il proprio indirizzo IP e il tipo di protocollo utilizzato per il collegamento con le macchine in Cloud (Figura 4).

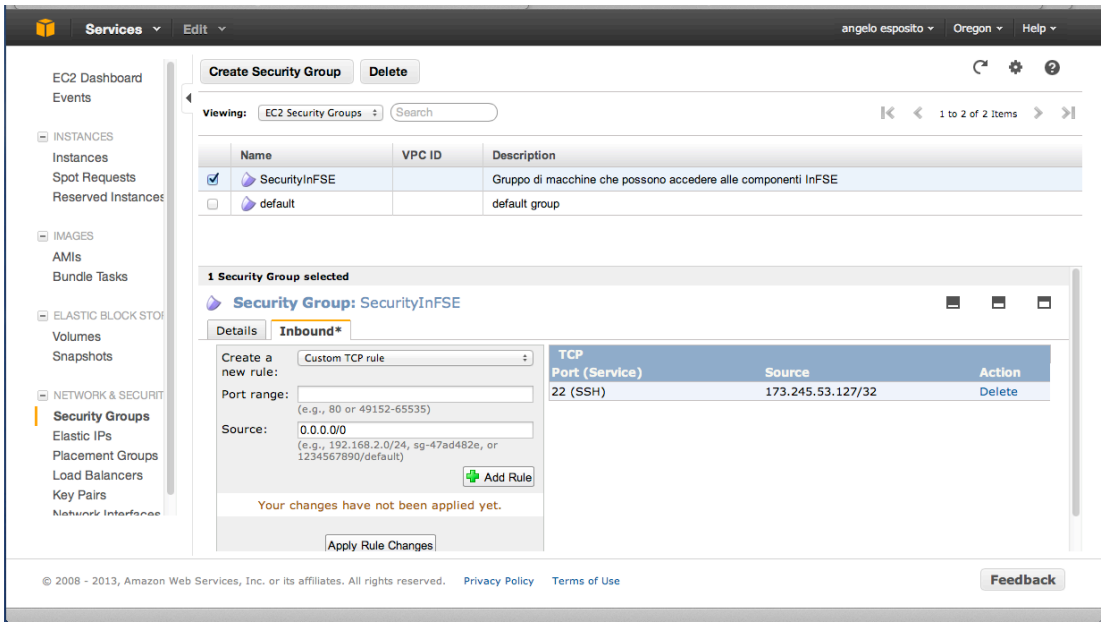

Figura 4 – Dettaglio di configurazione del Security Group

3.1.2 Installazione della componente Gestore dei Documenti su Cloud

Una volta svolte le attività di pre-configurazione dell'ambiente Cloud di Amazon, è possibile creare un nuovo "ambiente" in ElasticBeanStalk pre-caricando la componente InFSE in formato WAR. Per la creazione dell'ambiente, selezionare la voce *Customizer* (Figura 5).

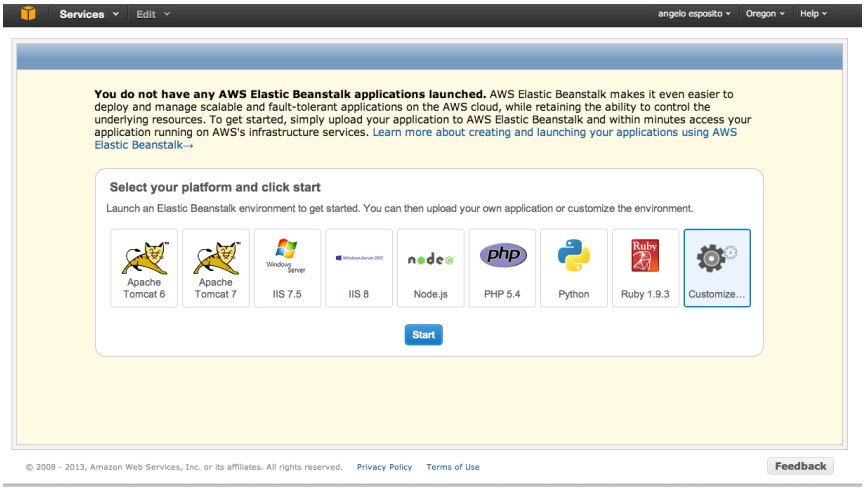

Figura 5 – Creazione dell'ambiente di esecuzione della componenti InFSE in ElasticBeanStalk

La prima schermata di configurazione consente di scegliere il nome dell'applicazione, una breve descrizione ed infine il tipo di *Container* (Figura 6).

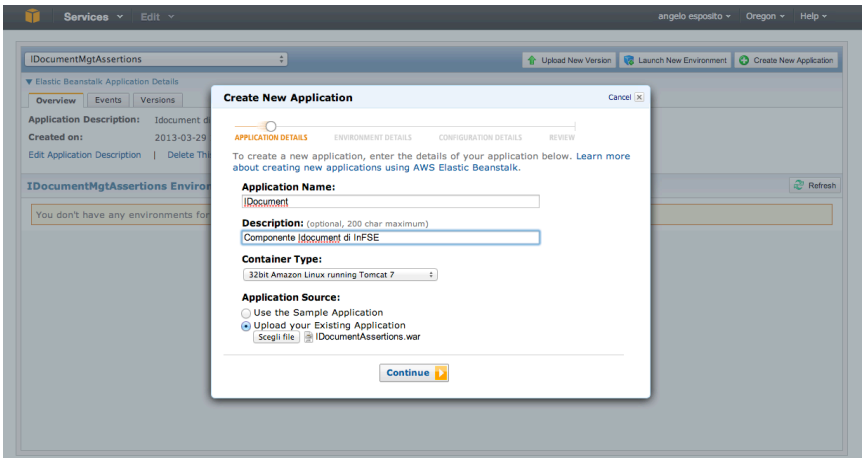

Figura 6 – Creazione Ambiente Cloud con il precaricamento della componente di InFSE

Il settaggio dell'ambiente di esecuzione della componete InFSE prevede la possibilità di:

- lanciare il nuovo ambiente in esecuzione con la componente di InFSE precaricata;
- creare una nuova istanza del Relational Database Service (RDS DB) collegato all'ambiente Elastic che si sta per lanciare (non necessaria per il funzionamento delle componenti di InFSE).

Figura 7 – Parametri di configurazione di creazione dell'ambiente Cloud

Il passo successivo è indicare la Key Pairs da utilizzare in fase di connessione. La Key Pairs che bisogna utilizzare è quella creata in fase di pre-configurazione dell'ambiente (come esposto nel paragrafo 3.1). Inoltre, è possibile specificare su che tipo di architettura HW viene lanciata l'applicazione.

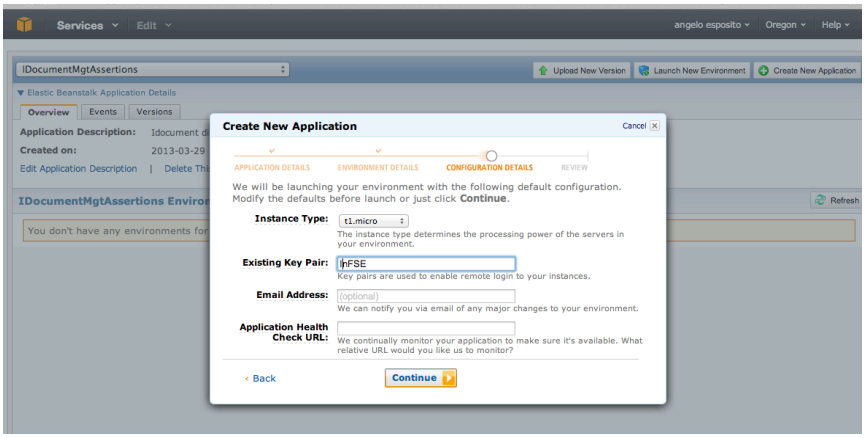

Figura 8 – Dettagli di configurazione dell'ambiente Cloud

ElasticBeanStalk crea automaticamente i livelli di astrazione necessari all'esecuzione della componente applicativa in ambiente Cloud. Una volta terminata l'installazione della componente in ElasticBeanStalk, la schermata che si ottiene è la seguente (Figura 9).

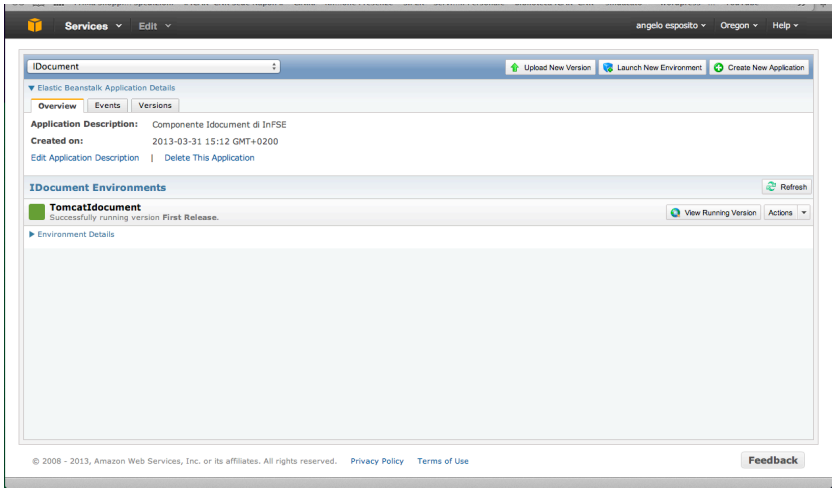

Figura 9 – Schermata principale di gestione dell'ambiente ElastiBeanStalk

Per la configurazione e la personalizzazione di Tomcat e della Amazon Machine Image (AMI) è necessario utilizzare la dashboard messa a disposizione da EC2 (come in Figura 10).

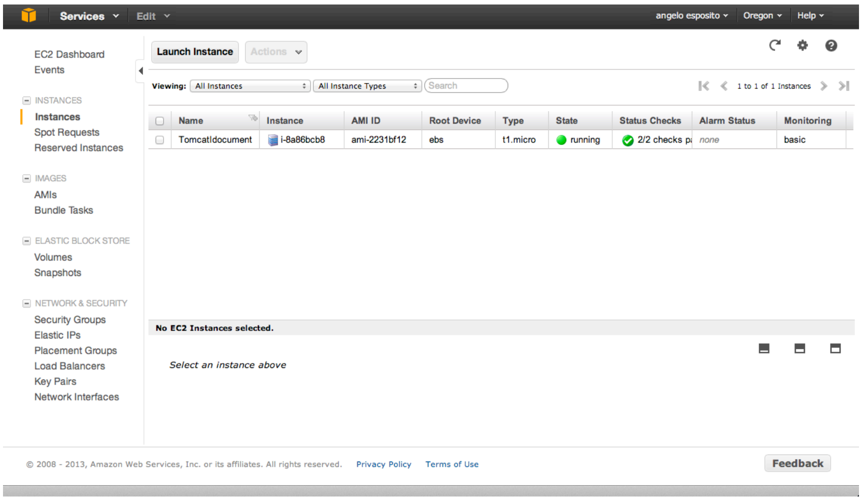

Figura 10 – Schermata di configurazione EC2

Per accedere da remoto al servizio è sufficiente recuperare l'informazione del Public DNS. L'accesso alle macchine del Cloud è consentito solo se l'indirizzo della macchina dalla quale ci si collega è inserito in uno dei Security Group collegato all'ambiente di esecuzione delle macchine del Cloud.

Per l'accesso è possibile utilizzare diversi client SFTP e la Kay Payrs creata in fase di pre-configurazione dell'ambiente (ad esempio WinSPC, Cyberduck, etc).

Per modificare i permessi di accesso alle cartelle di sistema delle macchine su Cloud è possibile accedere da shell via SSH ed impartire il comando chmod.

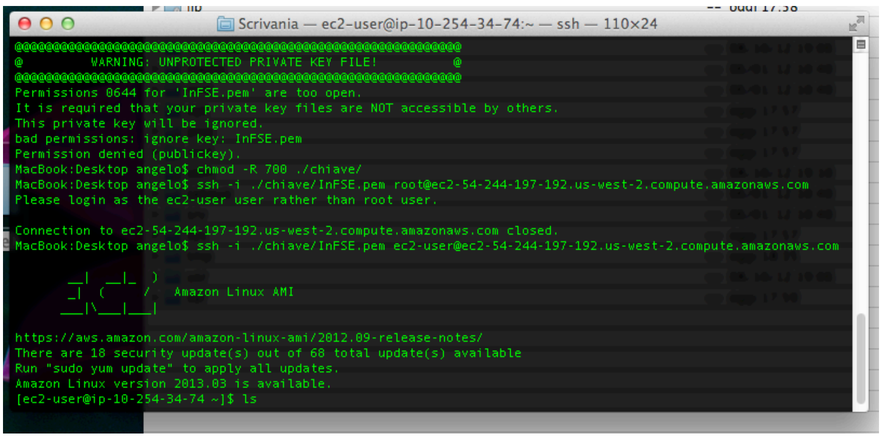

Figura 11 – Collegamento da console via SSH

Una volta create le opportune cartelle per l'esecuzione della componente dell'infrastruttura InFSE è stato effettuato il test per il recupero di un documento nel repository dell'ambiente di test ICAR-NA.

4. Test di recupero documento

La configurazione prototipale testata è mostrata nella figura seguente.

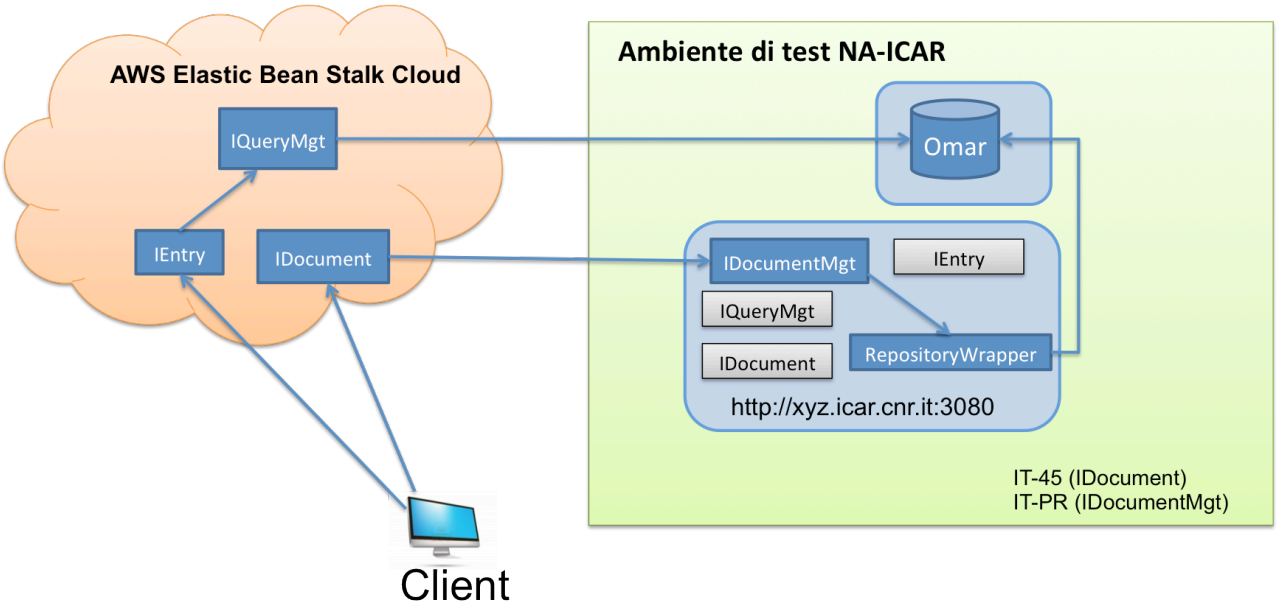

Figura 12 – Ambiente di test del FSE sul Cloud Amazon

Il client è stato configurato in modo che puntasse al servizio Gestore dei Documenti dispeigato sul Cloud all'indirizzo `http://infse.elasticbeanstalk.com:80/IDocumentImpl`.

Il servizio IDocument è stato configurato in modo da puntare al servizio IDocumentMgt sull'ambiente di test NA-ICAR, come mostrato in Figura 12. Per effettuare il test è stato utilizzato un client per la consultazione dei documenti presenti nel FSE (come in Figura 13 e 14).

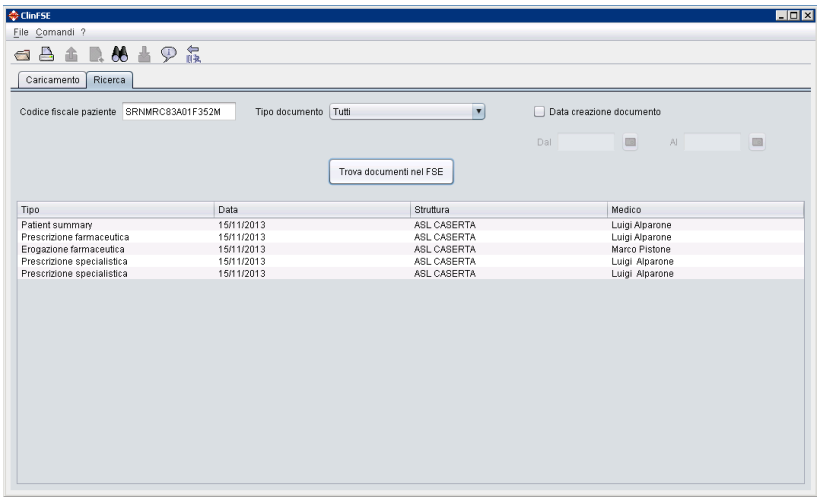

Figura 13 – Interfaccia di consultazione del FSE

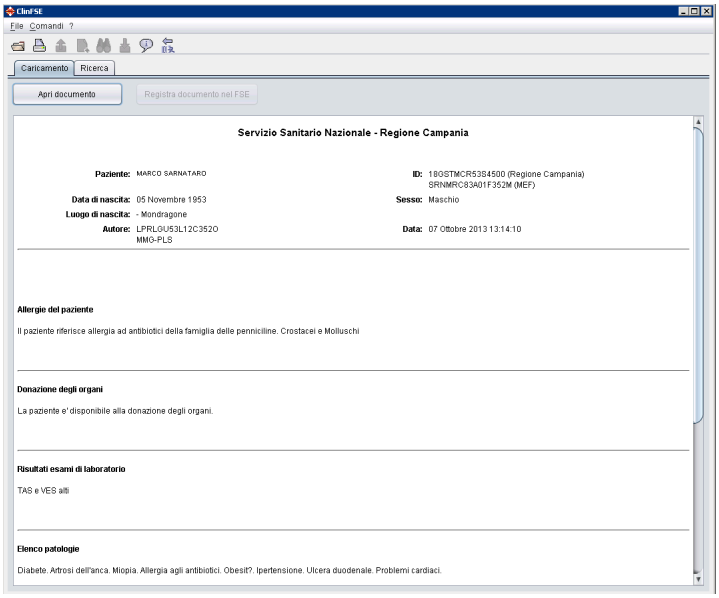

Figura 14 – Visualizzazione di uno specifico documento presente nel FSE

5. Conclusioni

Partendo dall'analisi svolta nel rapporto tecnico [1], in questo lavoro si è dimostrata la fattibilità dell'uso del paradigma Cloud per l'erogazione dei servizi FSE. A tale scopo è stato creato un ambiente prototipale dove sono stati effettuati una serie di test per la verifica del funzionamento e della corretta interazione tra le componenti "in ambiente Cloud" e quelle in ambiente "locale". Questo lavoro consentirà di testare in termini di performance le componenti di InFSE in ambiente Cloud con importanti risultati sulla concretezza nell'adozione di tale paradigma per l'erogazione dei servizi di FSE. Un altro importante sviluppo di questo lavoro riguarda il deployment delle componenti InFSE in due ambienti Cloud "differenti" per la verifica dell'interoperabilità delle componenti di InFSE predisposte in ambienti Cloud differenti.

Riferimenti bibliografici

[1] A. Esposito, “Analisi valutativa dell’adozione del Cloud per il Fascicolo Sanitario Elettronico”, RT-ICAR-NA-2013-1

[2] Raccomandazioni e proposte sull’utilizzo del Cloud Computing nella pubblica amministrazione, DigitPA, 28 giugno 2012.

[3] Infrastruttura tecnologica del Fascicolo Sanitario Elettronico - Linee guida, CNR, Luglio 2012.

[4] Infrastruttura tecnologica del Fascicolo Sanitario Elettronico -Fotografia commentata sperimentazioni esistenti su FSE, CNR, Dicembre 2010.

[5] Cloud Computing Security Risk Assessment, ENISA, November 2009.

[6] Cloud Computing - Benefits, risk and recommendations for information security, ENISA, Novembre 2009.

[7] NIST Cloud Computing Reference Architecture, September 2011.

[8] US Government Cloud Computing Technology Roadmap Volume I Release 1.00 (Draft). High- Priority Requirements to Further USG Agency Cloud Computing Adoption. NIST Cloud Computing Program Information Technology Laboratory, L. Badger, D. Bernstein, R. Bohn, F. de Vaulx, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside and D. Leaf, November 2011.

[9] M. Ciampi, G. De Pietro, C. Esposito, M. Sicuranza, and P. Donzelli, “On Federating Health Information Systems”, in GUT 2012: Proceedings of the International Conference in Green and Ubiquitous Technology, pp. 139-143, 2012, IEEE Press.

[10] C. Esposito, M. Ciampi, G. De Pietro, and P. Donzelli, “Notifying Medical Data in Health Information Systems”, in DEBS 2012: Proceedings of the 6th ACM International Conference on Distributed Event-Based Systems, pp. 373-374, 2012, ACM New York, NY, USA, ISBN: 978-1-4503-1315-5, DOI: 10.1145/2335484.233552.

[11] M. Ciampi, G. De Pietro, C. Esposito, M. Sicuranza, P. Mori, A. Gebrehiwot, and P. Donzelli, "On Securing Communications among Federated Health Information Systems", in SAFECOMP 2012 Workshops: Proceedings of the 31st International Conference on Computer Safety, Reliability and Security, Lecture Notes in Computer Science, vol. 7613, pp. 235-246, 2012, Springer-Verlag Berlin Heidelberg.

[12] G. De Pietro, A. Coronato, M. Ciampi, A. M. Urso, M. Cossentino, R. Rizzo, P. Storniolo, F. Folino, M. C. Buzzi, A. Gebrehiwot, “L’infrastruttura tecnologica del Fascicolo Sanitario Elettronico”, I. Florio, M. T. Guaglianone (Eds.), Il Fascicolo Sanitario Elettronico: Infrastruttura tecnologica e codifica dei dati, pp. 85-127, 2012, CNR – SeGID, Collana Documentalia, ISBN: 978-88-906334-1-6, ISSN: 2239-8414.

[13] G. De Pietro, R. Guarasci, M. Ciampi, A. M. Urso, M.C. Buzzi, C. Pizzuti, “L’interoperabilità nazionale del Fascicolo Sanitario Elettronico: il progetto InFSE”, P. Tarallo (Ed.), Verso e-Health 2020, Il Sole 24 Ore Sanità, 2012, ISBN: 978-88-324-8172-3.

[14] P. Donzelli, G. De Pietro, R. Guarasci, M. Ciampi, and M. T. Chiaravalloti, "Infrastruttura del Fascicolo Sanitario Elettronico: dalle regole alla realizzazione", e-HealthCare, Anno 4, Numero 20, Settembre – Ottobre 2012, pp. 16-22, Edisef, ISSN: 2038-4238.