REGIONE TOSCANA

Giunta Regionale

Direzione Generale Organizzazione e Risorse

Area di Coordinamento

Organizzazione, Personale, Sistemi Informativi

Settori

INFRASTRUTTURE E TECNOLOGIE PER LO SVILUPPO DELLA SOCIETA' DELL'INFORMAZIONE

SISTEMI INFORMATIVI E TECNOLOGIE DELLA CONOSCENZA

Monitoraggio Specifico Applicativi

DOCUMENTO: Documento illustrativo – Monitoraggio Specifico Applicativi

EMISSIONE - VERIFICA – PUBBLICAZIONE - APPROVAZIONE

	Funzione	Nome	firma
Emissione	Settore	INFRASTRUTTURE E TECNOLOGIE PER LO SVILUPPO DELLA SOCIETA' DELL'INFORMAZIONE	
Emissione	Settore	SISTEMI INFORMATIVI E TECNOLOGIE DELLA CONOSCENZA	
Verifica	Settore	INFRASTRUTTURE E TECNOLOGIE PER LO SVILUPPO DELLA SOCIETA' DELL'INFORMAZIONE	
Verifica	Settore	SISTEMI INFORMATIVI E TECNOLOGIE DELLA CONOSCENZA	
Pubblicazione	Specialisti Tecnici	hostmaster@regione.toscana.it riferimento per chiarimenti sul presente documento	
Approvazione	Responsabile Settore	Laura Castellani	
Approvazione	Responsabile Settore	Leonardo Borselli	

LISTA DI DISTRIBUZIONE : po-progetti-ict@liste.regione.toscana.it ; responsabili tecnici di progetti ICT, allo scopo di inserire riferimenti al documento nei capitolati speciali di appalto nonché diffondere e distribuire lo stesso agli attuali e futuri fornitori di componenti software per Regione Toscana.

AGGIORNAMENTI

Versione	Data	Paragrafi Modificati	Motivo Modifica
1.0	14/07/2014		Prima stesura

Sommario

GENERALITÀ....4

1.1 VALIDITÀ....4
1.2 RIFERIMENTI....4
1.3 DEFINIZIONI E ABBREVIAZIONI....4
1.4 ALLEGATI....4

2.MONITORAGGIO DEGLI APPLICATIVI....5

2.1 APPLICATIVI DA MONITORARE....5
2.2 INTERFACCIAMENTO CON IL SISTEMA DI MONITORAGGIO....5
2.2.1 Applicativi web....5
2.2.2 Servizi....6
2.3 COSA MONITORARE ALL'INTERNO DEL SINGOLO APPLICATIVO....6
2.3.1 Verifica dell'accesso alle basi di dati....7
2.3.2 Raggiungibilità dei servizi esterni utilizzati dall'applicativo....7

3.ANALISI PER L'INTRODUZIONE DEL MONITORAGGIO IN DUE APPLICAZIONI RILEVANTI....7

3.1 SISTEMA DI GESTIONE DEGLI EVENTI DI PRONTO SOCCORSO (IN ODS)....8
3.1.1 Verifica dell'accesso alle basi di dati....8
3.1.2 Raggiungibilità dei servizi esterni utilizzati dall'applicativo....8
3.2 FASCICOLO SANITARIO ELETTRONICO (FSET)....8
3.2.1 Verifica dell'accesso alle basi di dati....8

4.IMPEGNI CHE ASSUME IL FORNITORE CHE SVILUPPA L'APPLICAZIONE....9

GENERALITÀ

Obiettivo del documento è la definizione delle strategie da adottare per consentire l'integrazione degli applicativi dei sistemi informativi con il sistema di monitoraggio di RT.

Nel documento è riportata la descrizione dei seguenti aspetti:

- Tipologie degli applicativi da monitorare.
- Modalità di interfacciamento con il sistema di monitoraggio.
- Funzionalità monitorate.

1.1 Validità

Il presente documento è valido a partire dalla data di emissione riportata in copertina.

1.2 Riferimenti

- [1] "Monitoraggio degli applicativi del SIS", verbale della riunione del 01/09/2010.
- [2] http://www.regione.toscana.it/-/standard-tecnici-e-ambienti-di-sviluppo-e-produzione#architetture

  url alla quale è prelevabile il documento
  - [3] RT_CSA_Standard_tecnologici_v3.0.pdf
- https://www.tix.it/doctecnica

  url alla quale è prelevabile il documento
  - Modalità di consegna applicativi su ambiente multi-tier RT

1.3 Definizioni e abbreviazioni

SIS	Sistema Informativo Sanitario - SIS_ARCHITETTURA
118	Emergenza 118 - SIS_RFC_134 Gest. Emergenza Urgenza 118
FSET	Fascicolo Sanitario Elettronico - SIS_FSE

1.4 Allegati

- N.A.

2. MONITORAGGIO DEGLI APPLICATIVI

2.1 Applicativi da monitorare

Come riportato in [1], sono oggetto di monitoraggio tutti gli applicativi del SIS. Tra questi in particolare:

- Tutti i servizi (es. Pronto Soccorso, Laboratorio, 118, RIS, RIC, PASU, DSH, servizi anagrafici HL7 e DBSIS).
- Tutti gli applicativi web tra cui anche FSET.

2.2 Interfacciamento con il sistema di monitoraggio

L'interfacciamento con il sistema di monitoraggio è effettuato diversamente a seconda della tipologia di applicativo (applicazione web o servizi). In questa sezione vengono riportati i dettagli per ciascuna tipologia.

2.2.1 Applicativi web

L'applicativo web da monitorare dovrà esporre una pagina JSP che sarà invocata dal sistema di monitoraggio di Regione Toscana. La pagina dovrà essere prodotta ed esposta seguendo le specifiche riportate di seguito.

Se l'applicazione risponde a http(s)://nomehost/nomeapplicazione occorre che sia aggiunta una risorsa con nome http(s)://nomehost/nomeapplicazione/monitor.jsp) che risponda con un testo tipo:

```
<prima riga> BEGIN
<seconda riga> STATUS : OK|WARN|ERROR (quest'ultimo ritenuto il peggiore tra gli stati riportati nelle righe successive)
<successive n righe> misura : valore (OK|WARN|ERROR) + messaggio
<ultima riga> END
```

Requisiti della pagina monitor.jsp

- La pagina non dovrà restituire html ma solo testo.
- La pagina dovrà inoltre rispondere in un tempo massimo di 15 secondi superati i quali sarà considerata non operante nei range prestabiliti.

  Nel caso i test necessitino di un tempo superiore ai 15 secondi questi dovranno essere effettuati ad intervalli periodici e non al momento della chiamata alla pagina monitor.jsp. Al momento della chiamata saranno visualizzati i risultati dell'ultima esecuzione.

- La pagina non dovrà restituire un errore http 500. Ogni eventuale eccezione interna dovrà essere catturata e dovrà essere restituito un messaggio del tipo:

  ```
  BEGIN
  STATUS : ERROR messaggio esplicativo del problema occorso.
  END
  ```

- Nel caso di applicativi web che utilizzano ARPA, occorre che la pagina sia mappata ad una URL non intercettata dai filtri ARPA. Nel caso in cui questo non sia possibile (come ad es. in FSET) il filtro dovrà essere modificato per escludere la url della pagina *monitor.jsp*.

  Per evitare che la pagina di monitoraggio sia accessibile a chiunque, si introduce all'interno della pagina monitor.jsp la gestione di una "white-list" con cui verificare l'indirizzo IP del chiamante.
  La pagina di monitoraggio dovrà verificare se l'IP del chiamante appartiene al range di indirizzi della white-list e dovrà restituire i risultati del monitoraggio solo se il controllo ha esito positivo.

Nel caso in cui l'IP del chiamante non appartenga al range di indirizzi indicato, verrà restituito un errore.

La white-list sarà una lista di indirizzi di rete del tipo "**`XXX.YYY.WWW.ZZZ/N`**" separati dal carattere '|' ;
alla data gli unici IP autorizzati alle chiamate verso gli applicativi sono::

```
159.213.224.190/32|159.213.225.5/32
```

La white list, se concordato con il capoprogetto a cui il fornitore fa riferimento, può essere reperibile dall'applicativo tramite una lookup JNDI. Il nome JNDI sarà indicato da Regione Toscana.

2.2.2 Servizi

Nel caso di servizi, al posto della pagina *monitor.jsp* sarà creato un nuovo servizio *"Monitor Service"* dedicato al monitoraggio. Il servizio sarà invocato dal sistema di monitoraggio di RT con una richiesta SOAP e risponderà con un messaggio SOAP i cui contenuti sono analoghi a quelli della pagina *monitor.jsp*.

Di seguito un esempio di un possibile messaggio[1]:

```
<MonitorResponse>
      <Status code="KO">Impossibile raggiungere i servizi.</Status>
      <Result name="Connessione al database" code="OK" Value="1">
            La connessione al database e' stabilita correttamente</Result>
      <Result name="Raggiungibilità servizio anagrafico" code="KO" Value="0">
            Il servizio non può essere raggiunto.</Result>
      <Result name="numero eventi in attesa" code="WARN" Value="20003">
            Il numero eventi in attesa ha raggiunto la soglia di
      attenzione.</Result>
</MonitorResponse>
```

Requisiti del servizio

- Di norma il servizio non effettuerà il controllo della white list. Trattandosi di un servizio questo sarà accessibile solo dal back end e quindi non necessita di un controllo degli accessi. Nel caso in cui il controllo della whitelist si rendesse comunque necessario, sarà implementato secondo le specifiche dichiarate al punto 2.2.1

- Nel caso di errore il servizio risponderà con un messaggio apposito, ad esempio:

```
<MonitorResponse>
      <Status code="ERROR">Messaggio esplicativo del problema</Status>
</MonitorResponse>
```

2.3 Cosa monitorare all'interno del singolo applicativo

Per ogni applicativo dovranno essere effettuate le verifiche seguenti:

- verifica dell'accesso al database;
- raggiungibilità dei servizi esterni utilizzati dall'applicativo.

Obiettivo della verifica è quindi la valutazione della disponibilità delle risorse da cui dipende l'applicazione

[1] Il messaggio fornito è solo un esempio, l'effettivo formato sarà documentato con un WSDL. Nel messaggio di esempio manca inoltre la busta SOAP: viene mostrato solo il contenuto.

tramite un set di test attivi che simulano/emulano/utilizzano componenti dell'applicazione stessa.

Nelle sezioni seguenti si riporta un esempio sul modo in cui queste verifiche saranno effettuate all'interno dei singoli applicativi con riferimento particolare all'applicativo del fascicolo sanitario FSET e al sistema erogatore di Pronto Soccorso.

2.3.1 Verifica dell'accesso alle basi di dati

La raggiungibilità del database viene verificata effettuando una o più query che saranno definite applicativo per applicativo in relazione alla struttura della base di dati e alle tabelle sulle quali si ritiene significativo svolgere la verifica.
In particolare, verrà effettuata una query per ogni datasource utilizzato dall'applicativo.

Le query dovranno essere effettuate utilizzando la stessa API (ad esempio Hibernate o JPA) e gli stessi componenti (ad es. le classi DAO) che l'applicativo utilizza per interrogare il database.
Analogamente dovrà essere utilizzata la stessa "Configuration" Hibernate / "Persistence Unit" JPA utilizzata dall'applicativo.
Questa strategia consente di verificare l'accesso al database utilizzando le stesse modalità di accesso dell'applicativo. In questo modo il risultato della verifica dà evidenza dei seguenti aspetti:

- raggiungibilità del database;
- corretta configurazione del datasource;
- disponibilità di connessioni nel datasource;
- corretta configurazione del contesto di persistenza dell'applicativo in relazione al database e (parziale) verifica della coerenza della struttura del database con quanto atteso dall'applicativo.

Per la verifica potranno essere effettuate una o più query, a seconda del numero dei datasource. Sarà quindi riportato l'esito (OK | WARN | ERROR) all'interno della pagina / messaggio SOAP di monitoraggio.

Se l'applicativo utilizza più schema (come ad esempio nel caso di FSET) attraverso uno stesso datasource, la query dovrà essere effettuata in modo casuale su schema diversi ad ogni invocazione del servizio di monitoraggio.

2.3.2 Raggiungibilità dei servizi esterni utilizzati dall'applicativo

La raggiungibilità dei servizi da cui l'applicativo dipende viene verificata effettuando il recupero del WSDL del servizio (o altra risorsa statica equivalente).
Se questi servizi sono esposti da una porta di dominio, verrà effettuato il recupero del WSDL del servizio esposto dalla porta di dominio.

Per ogni servizio su cui viene effettuata la verifica, viene riportato l'esito (OK | WARN | ERROR) all'interno della pagina / messaggio SOAP di monitoraggio.

3. ANALISI PER L'INTRODUZIONE DEL MONITORAGGIO IN DUE APPLICAZIONI RILEVANTI

In questa sezione si riporta una descrizione dell'intervento necessario per interfacciare con il sistema di monitoraggio due applicativi del SIS che sono presi come rappresentativi di due categorie di applicazioni differenti:

- il sistema di gestione degli eventi di pronto soccorso in ODS;
- l'applicazione web per la consultazione del fascicolo sanitario FSET.

Di seguito la descrizione delle funzionalità, dei componenti monitorati e degli interventi necessari.

3.1 Sistema di gestione degli eventi di pronto soccorso (in ODS)

Il sistema ha il compito di ricevere gli eventi di pronto soccorso dall'infrastruttura CART, interrogare l'anagrafe DBSIS per identificare il soggetto cui la prestazione è associata, archiviare l'informazione sulla base di dati e infine inviare un acknowledge che dà evidenza all'inviante sull'esito dell'operazione.

Il sistema di pronto soccorso interagisce quindi con i seguenti sistemi esterni:

- base di dati in cui sono archiviate le prestazioni;
- servizi anagrafici DBSIS:
- servizi di acknowledge esposti dalla porta di dominio.

3.1.1 Verifica dell'accesso alle basi di dati

Per la verifica dell'accesso alla base di dati sarà tentato il recupero di un codice id_prestazione di una prestazione di Pronto Soccorso esistente.

L'operazione precedente è svolta introducendo un nuovo servizio (MonitoringService) che utilizzerà Hibernate, gli oggetti di dominio e i DAO presenti all'interno dell'applicativo.

Per la versione TIX la query verrà effettuata, ad ogni invocazione del servizio di monitoraggio, su uno dei 21 schema di PS presenti nel database prestazionale. La scelta dello schema è casuale.
Inoltre occorre effettuare una verifica anche sul database indice (SISINDEX).

3.1.2 Raggiungibilità dei servizi esterni utilizzati dall'applicativo

Per la verifica dei servizi utilizzati dall'applicativo saranno effettuate le seguenti operazioni[2]:

1. recupero del wsdl del servizio DBSIS "RicercaSoggetto";
2. recupero del wsdl dei servizi "EsitoNotificaEventoClinico". In questo caso, abbiamo un servizio per ogni Azienda erogante[3]. La scelta del wsdl da recuperare sarà effettuata casualmente ad ogni invocazione del servizio di monitoraggio.

3.2 Fascicolo sanitario elettronico (FSET)

L'applicazione del fascicolo sanitario elettronico FSET accede alle basi di dati del TIX per mostrare ai cittadini le informazioni anagrafiche, di consenso e prestazionali che costituiscono il proprio fascicolo sanitario. A causa della separazione esistente tra dati anagrafici e prestazionali e anche tra dati prestazionali appartenenti ad Aziende diverse, l'applicazione FSET utilizza database e schema separati, descritti in dettaglio nella sezione successiva. FSET non è invece dipendente da servizi esterni.

FSET si interfaccia con l'infrastruttura ARPA per la gestione dell'accesso. La pagina di monitoraggio *monitor.jsp* deve essere esposta ad una URL accessibile anche senza aver effettuato autenticazione su ARPA.
Per questo occorrerà effettuare una modifica al filtro ARPA per escludere la pagina *monitor.jsp* e dovrà essere introdotta una "white-list" per consentire l'accesso alla pagina solo da parte indirizzi IP appartenenti a sottoreti configurate (come riportato in dettaglio in sez. 2.2.1).

3.2.1 Verifica dell'accesso alle basi di dati

I database utilizzati dall'applicativo FSET sono i seguenti:

- Database contenente i dati anagrafici dagli assistiti: SISANAG;
- Database indice delle prestazioni: SISINDEX;
- Database prestazionale: il database prestazionale contiene schema differenti, uno per ogni Azienda e per ogni dominio applicativo.

[2] Si osserva che la strategia cambia con l'introduzione dei proxy applicativi. In presenza dei proxy, l'anonimizzazione del soggetto non viene effettuata dal sistema di pronto soccorso ma dal proxy presente sul NAL aziendale.
[3] Si osserva che la strategia cambia con l'introduzione dei proxy applicativi. Con i proxy infatti avremo una unica URL da invocare per la spedizione dell'esito alle differenti Aziende. E' compito del proxy indirizzare il messaggio di Ack all'Azienda a partire dai dati forniti dall'inviante.

Per la verifica della disponibilità della base di dati si prevede l'esecuzione delle query seguenti:

- esecuzione di una query sulla anagrafe (SISANAG) per recuperare i dati di una persona fisica a partire da un codice fiscale configurato.
- esecuzione di una query predefinita sull'indice SISINDEX.
- esecuzione di una query su uno schema prestazionale scelto casualmente ad ogni invocazione della pagina monitor.jsp;

Nota importante: l'applicativo FSET è dislocato su più istanze di JBoss diverse che lavorano in load balancing. La pagina di monitoraggio dovrà essere invocata quindi su ogni istanza di JBoss per dare evidenza dello stato di funzionamento e delle prestazioni dell'applicativo che si trova su ciascun nodo.

4. IMPEGNI CHE ASSUME IL FORNITORE CHE SVILUPPA L'APPLICAZIONE

Il fornitore::

- definisce il WSDL del servizio di monitoraggio "MonitoringService";
- realizza la porzione di codice applicativo che espone il servizio di monitoraggio;
- integra le necessarie definizioni se l'applicazione è una applicazione ARPA
- realizza la pagina monitor.jsp
- implementa il controllo sulla white list
- collabora durante i test di integrazione nel sistema di monitoraggio.
- eventualmente propone a RT il nome JNDI della risorsa che contiene la white list;
- verifica con la collaborazione del fornitore l'interfacciamento del sistema di monitoraggio di RT con la pagina monitoring.jsp e con il servizio "MonitoringService".