1. **DESCRIZIONE DELLA SOLUZIONE DI DISASTER RECOVERY**

Sulla base dei requisiti raccolti l’architettura presso il DC di Rozzano per l’ambiente di DR è rappresentata nello schema seguente.



Il sito di DR è connesso con il sito primario (v.Aldo Moro-Bologna) con una coppia di collegamento lambda Wave da 1 GB ciascuno dedicati esclusivamente al servizio.

I due end point sono terminati, nel DC di Rozzano , **su una coppia di switch 3750** on configurazione stack con le 2 porte in port channel tra loro, che ricevono i rilanci in fibra.

Presso la sede cliente di Via Aldo Moro – Bologna, è prevista la predisposizione di una coppia di switch con medesima configurazione.

I collegamenti nel data center di Rozzano sono protetti con una coppia di firewall **Fortinet** **Fortigate** 1000C in configurazione ad alta affidabilità dove il traffico verrà inoltrato verso i server di architettura.

A Bologna presso il cliente è presente il sistema principale, comprendente una serie di application server con software Glassfish realizzati su un middleware VmWare in ambiente RedHat per il software applicativo Sacer[[1]](#footnote-1), application server TOMCAT sempre su VmWare in ambiante RedHat con software applicativo TPI, server di database Oracle DB 12g Enterprise Edition con opzione GRID server di backup/file server con Tivoli TSM per la gestione delle archiviazioni/backup su nastro.

**Ambiente di DR di Rozzano:**

L’infrastruttura di DR è realizzata su 2 server fisici e su ambienti virtuali realizzati su 2 nodi VMWare ESXi distribuiti equamente sui 2 restanti server previsti in fornitura

La consistenza di Host virtuali comprende:

* 2 ApplicationServer **“Sacer**” di **Produzione** con Glassfish in prima fase, poi Jboss
* 1 Application Server “**Sacer**” di **Test**
* 2 Application Server “**TPI”** con **Tomcat** uno di Test ed uno Produzione
* 1 WebServer con funzionalità di **bilanciamento** sugli application server.
* 1 Server dedicato a **Vcenter**.

Tutti gli host virtuali sono realizzati su sistema operativo Red Hat, con licenze:

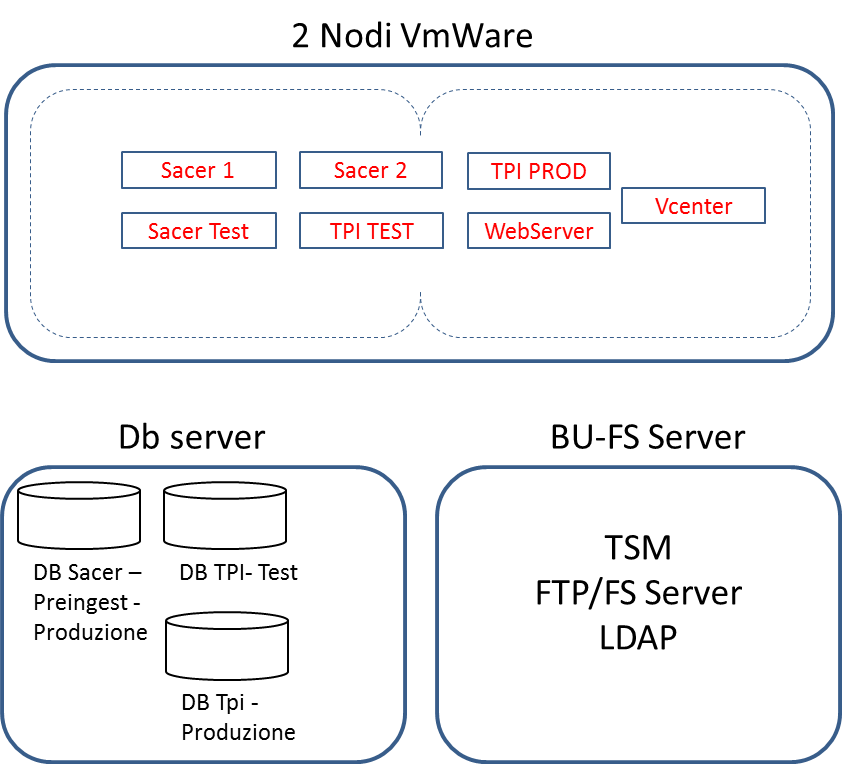
* 1 **VMware essential plus kit**, configurazione per 3 host biprocessori
* 2 **Red Hat Enterprise Linux** for Virtual Datacenters (Disaster Recovery)

I 2 server rimanenti sono dedicati, uno al Database Oracle con:

* Istanza di **Produzione** che include gli schemi dei Database **Sacer** e **Preingest e relativi schemi utilizzati da applicativo Sacer (SIAM, Verso)**
* Istanza di **produzione** di **TPI**
* Istanza di **Test** di **TPI**

L’ultimo server ospita **Tivoli** **TSM** dove saranno definite le configurazioni di Produzione e test; oltre al ruolo principale è utilizzato anche, come nella logica attuale, per la configurazione dei servizi di “sistema” necessari al funzionamento dell’architettura (NFS, NTP).

Nell’immagine seguente si schematizza la distribuzione dei server e ruoli sulle macchine fisiche in piattaforma



Nella tabella seguente si elencano gli host virtuali e fisici che compongono l’architettura, indicando layer di appartenenza ed una breve sintesi del ruolo e dell’operatività degli applicativi.

Trattandosi di Sito di Disaster Recovery alcuni componenti vengono attivati solo in caso di dichiarazione di Disastro, mentre altri, come database o Tsm, devono essere mantenuti costantemente attivi per gestire il sincronismo dei dati con il sito primario.

Come descritto nella risposta al capitolato tecnico di gara, le componenti principali sono comunque mantenute sempre in stato attivo al fine di garantire un più efficace controllo dello stato e dell’allineamento delle versioni e componenti installati.

**Tabella 1 Ruoli server**

| **Server** | **Layer** | **Tipologia** | **Middleware** | **Ruolo - Stato** |
| --- | --- | --- | --- | --- |
| **WebServer** | 1 | Virtual | Apache + mod per effettuare bilanciamento e mod ssl | Server **operativo solo in caso di dichiarazione di Disastro**; gestisce il bilanciamento delle connessioni dagli enti versanti verso i 2 application server SACER e verso l’FTP Server.  Dispone di IP Pubblico, visibile solo dall’esterno.  In caso di DR, a seguito della dichiarazione di DR si procede all’attivazione del web server Apache per consentirne l’accesso. |
| **Sacer 1-2** | 2 | Virtual | Glassfish – Jboss (in seconda fase) | Server operativo **solo in caso di dichiarazione di Disastro**; processano i versamenti dei documenti. Si mantengono attivi i virtual host per mantenere un repository delle versioni versioni degli applicativi. I servizi Glassfish (e quindi Jboss) si attivano solo in fase di test di DR  Inizialmente si mantiene application server Glassfish, a seguito del completamento degli sviluppi c/o Regione si procederà a migrazione su Jboss. |
| **Sacer Test** | 2 | Virtual | Glassfish – Jboss (in seconda fase) | **Server sempre attivo**. Utilizzato per test di funzionalità e nuovi rilasci. Disponibile all’accesso da parte dei riferimenti Parer. |
| **TPI Prod** | 2 | Virtual | Tomcat | **Server sempre attivo ed operativo**. Interagisce con le rispettive istanze del sito primario per la gestione delle archiviazioni su nastro dei pacchetti DICOM.  E’ necessario sia sempre attivo e sottoposto a monitoring. |
| **TPI Test** | 2 | Virtual | Tomcat | **Server sempre attivo ed operativo**. Interagisce con le rispettive istanze del sito primario di TEST per la gestione delle archiviazioni su nastro dei pacchetti DICOM. |
| **DB Server** | 3 | Fisico | Oracle 12G | **DB Server**, mantiene l’istanza secondaria dei database Sacer, Preingest e TPI di Produzione e test allineate tramite Dataguard con le rispettive istanze del sito Primario.  E’ necessario sia sempre attivo e sottoposto a monitoring. |
| **BU-FS Server** | 3 | Fisico | Tivoli TSM  Ftp Server | **Server sempre attivo ed operativo**; tramite TSM gestisce backup ed archiviazioni su nastro, sia per l’ambiente di test che di produzione; oltre al ruolo di backup server, espone il servizio ftp da attivare in caso di DR, funge da File server esponendo l’area Storage tramite NFS agli application server , nonché LDAP ed NTP  E’ necessario sia sempre attivo e sottoposto a monitoring. |

* 1. **Replica dei Dati**

La replica dei dati tra sito primario e sito di DR avviene in 2 modalità:

* Allineamento Database: tramite Oracle DataGuard si mantiene una replica dei database Sacer e Preingest del sito Primario; questa funzionalità implica che il database secondario sia mantenuto in modalità Read Only e non possa subire alcuna modifica di configurazione se non derivante da attività definite sul sito Primario.
* Allineamento files Dicom: La trasmissione dei files è gestita da una componente dell’applicativo TPI attiva sul sito primario; a fronte della ricezione di un documento, il modulo tpi provvede, tramite la chiamata di web service e la copia diretta di file tramite il protocollo SFTP sulla directory chiamata “/TPI”, alla replica sul sito di DR dove, i rispettivi moduli TPI procedono alla gestione dell’archiviazione dei dati e quindi all’invio di un messaggio di conferma verso il primario. L’invio dei files avviene tramite trasferimento sftp, tramite l’installazione di un certificato SSL e della relativa chiave pubblica. Questa modalità di allineamento dei dati richiede oltre alla connettività verso il sito di primario, il mantenimento degli application server Tomcat in stato attivo.

1. In una seconda fase del progetto è previsto il rilascio da parte di Parer di una nuova release applicativa SACER disegnata su un infrastruttura Jboss. In conseguenza si procederà ad un aggiornamento di tutti gli application server, primari e di dr con introduzione di Jboss. Le release e tempistiche, alla data di entrata in esercizio dell’infrastruttura non sono ancora definite. [↑](#footnote-ref-1)