PROGETTO ADI

SECURITY

Sommario

1 Premessa

In merito al progetto ADI, con il presente documento si vuole illustrare l'architettura dell'infrastruttura cloud e i processi di funzionamento delle applicazioni, in modo di fornire gli elementi di valutazione del livello di protezione e sicurezza dei dati trattati.

Privacy by Design e by Default

"Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" definita anche **Privacy by Design e by Default**. Si tratta di uno dei principi sanciti e chiariti nel **GDPR 2018**, il "**General Data Protection Regulation**", più comunemente definito nuovo **Regolamento Europeo per la Protezione dei Dati Personali**, fortemente voluto da tutti gli Stati Membri dell'Unione Europea, che dovranno recepire la direttiva e allinearsi entro il **25 maggio 2018**. Numerose le novità introdotte dal testo, come il principio di "**responsabilizzazione**" o "**accountability**", che diventerà centrale per aziende e pubbliche amministrazioni, e il "**diritto all'oblio**" ovvero il **diritto alla cancellazione dei propri dati personali**, anche e soprattutto online, da parte del **titolare del trattamento**, se ricorrono una serie di condizioni.

L'**articolo 25 del GDPR 2018**, poi, prevede il principio **Privacy by Design e by Default**, in italiano: "**la protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**". Si tratta di un obbligo generale e prescrive: "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso" il Titolare del trattamento dei dati "mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati".

Nell'ambito del **Privacy by Design e by Default**, dunque, il titolare del trattamento deve assicurarsi di mettere in atto "misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento". In tal senso "tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. Ciò significa che tali "misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica". In questo ambito, il testo prevede infine un meccanismo di certificazione che "può essere utilizzato come elemento per dimostrare la conformità ai requisiti" sopra citati.

2 Sicurezza e protezione dei dati

Al fine di garantire la sicurezza dei dati, secondo quanto richiesto dalla normativa, sono stati presi in esame i seguenti elementi:

- Encryption del disco
- Sicurezza delle comunicazioni
- Controllo degli accessi

In seguito all'analisi sono state effettuate delle scelte sia di progettazione che di prodotto.

2.1 Encryption del disco

La normativa prevede che l'infrastruttura contempli l'encryption dei supporti storage utilizzati. Nel progetto in questione, essendo una soluzione virtualizzata che prevede l'utilizzo di server virtuali, l'encryption dei dischi diventa l'encryption dei volumi. Questa caratteristica garantisce che gli utenti, che hanno accesso agli stessi supporti fisici del cliente ASUR Marche, non abbiamo la possibilità di accedere ai volumi contenenti i dati sensibili del Cliente.

2.2 Sicurezza delle comunicazioni

La normativa richiede che il canale di comunicazione attraverso il quale vengono trasmessi i dati sia sicuro. Nel progetto in esame si possono individuare diversi canali di comunicazione:

- intra datacenter
- internet
- intranet

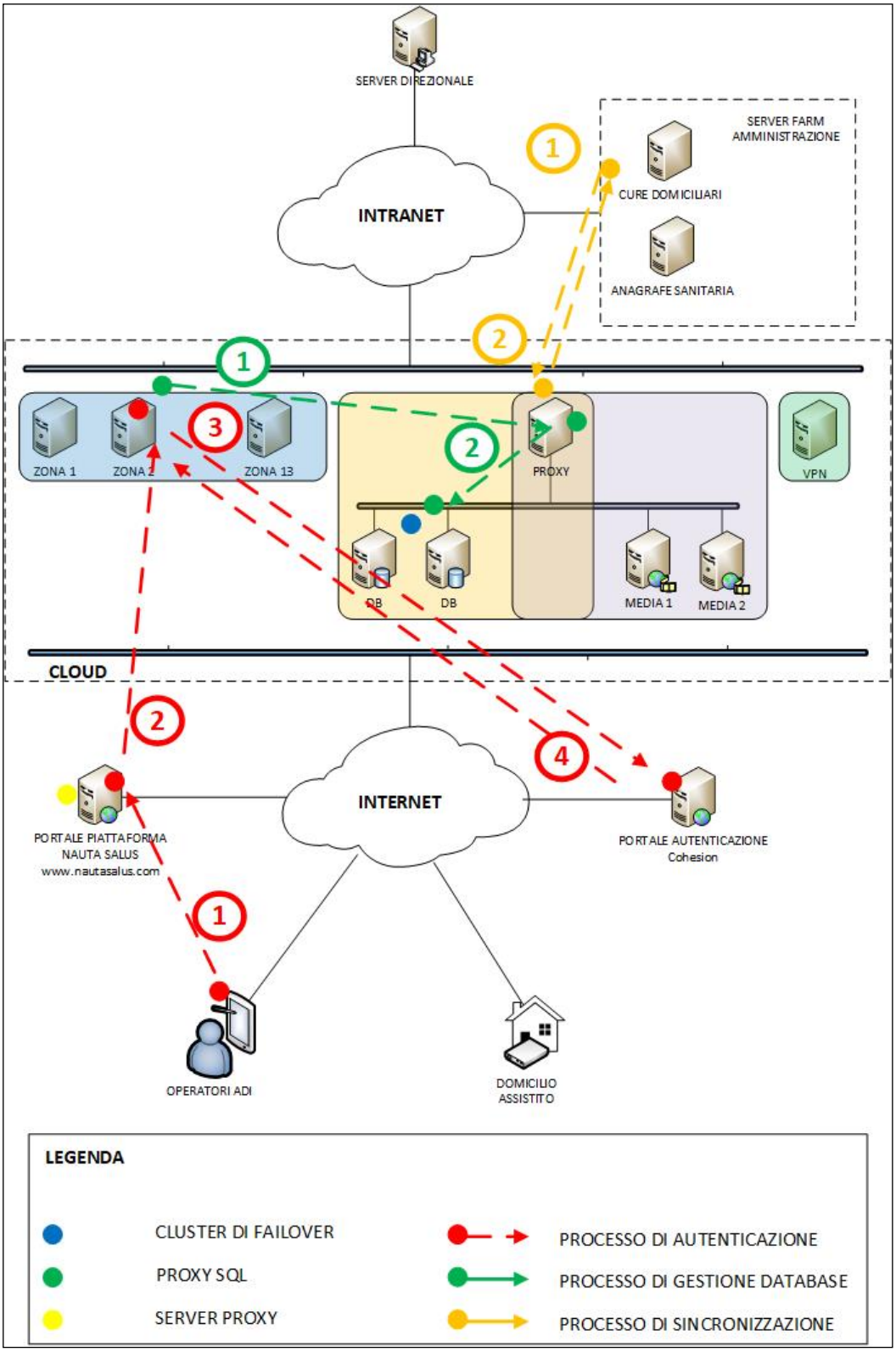
La sicurezza delle informazioni in transito è resa possibile tramite protocolli sicuri, come TLS (Transport Layer Security), che si basa su rete TCP/IP. Al fine di garantire la sicurezza delle comunicazioni sono previsti una serie di certificati per la comunicazione in HTTPS.

2.3 Controllo degli accessi

La normativa richiede che l'accesso ai dati sia controllato e permesso solo dopo aver autenticato l'utente. Nel progetto è previsto l'utilizzo il servizio di autenticazione Cohesion fornito dalla della Regione Marche. Il framework Cohesion permette di verificare la corretta identità degli utenti (persone fisiche munite di codice fiscale) che accedono a servizi online opportunamente integrati, gestendo il processo di autenticazione e demandando il processo di autorizzazione/profilatura utente all'applicazione chiamante.

3 Descrizione della soluzione

Al fine di migliorare la sicurezza e l'affidabilità del servizio, è stata riprogettata l'architettura rispetto a quella descritta nel documento di progetto iniziale.
Di seguito è rappresentata la nuova architettura con indicati i principali flussi operativi.



La miglioria principale è l'Introduzione di un cluster di failover. formato da due server virtuali (DB) e un server proxy per la gestione delle chiamate da parte degli applicativi.

L'obbiettivo di concentrare il data base nel cluster, piuttosto che distribuirlo all'interno dei server di zona (progetto originale) è di poter identificare un solo punto logico dove sono contenuti i dati. Questa modifica consente di proteggere le informazioni in maniera più semplice ed efficace, tramite l'encryption del volume logico (encryption del data base).

Per realizzare questa soluzione sono stati introdotti tre nuovi componenti: Proxy SQL, Percona XtraDB e Percona Xtrabackup. Questa architettura permette la gestione sincrona del database.

Di seguito sono descritti gli elementi distintivi della soluzione.

Cluster di failover

Il cluster di failover è costituito da due nodi con XtraDB (engine), dove i dati sono replicati in maniera sincrona tramite replica SST (State Snapshoot Transfer), basata su XtraBackup. Inoltre, grazie al supporto nativo per la criptazione dei dati, Percona XtraDB garantisce un elevato livello di sicurezza delle informazioni.
L'accesso ai dati del cluster è gestito da un nodo Proxy SQL, che funge da load balancing.

Percona XtraDB Cluster è un'alternativa alle soluzioni di Clustering e Replicazione messe a disposizione direttamente da MySQL, in grado di fornire una buona scalabilità e alta disponibilità (High Availability). Percona XtraDB Cluster integra Percona Server, un fork di MySQL che si propone di scalare meglio sui nuovi hardware e fornire prestazioni più stabili. Inoltre attraverso l'utilizzo della libreria Galera di MySQL, XtraDB Cluster fornisce maggiore efficienza nell'utilizzo delle risorse.

XtraDB è il motore per il salvataggio di dati (storage engine) di Percona (flauvor MySql). La sua caratteristica principale è essere un sistema Open Source, ma di tipo Enterprise Grade e compatibile con engine generici, come Mysql e MariaDb. XtraDB utilizza infatti utilizza come schema InnoDB.

Le caratteristiche distintive di Percona Cluster sono:

- Capacità di realizzare replicazione sincrona
- Supporto alla replicazione con più nodi master
- Replicazione parallela
- Aggiornamento/Re-sincronizzazione automatica dei nodi

L'installazione del cluster Percona (PXC) si avvale dei seguenti meccanismi di sicurezza:

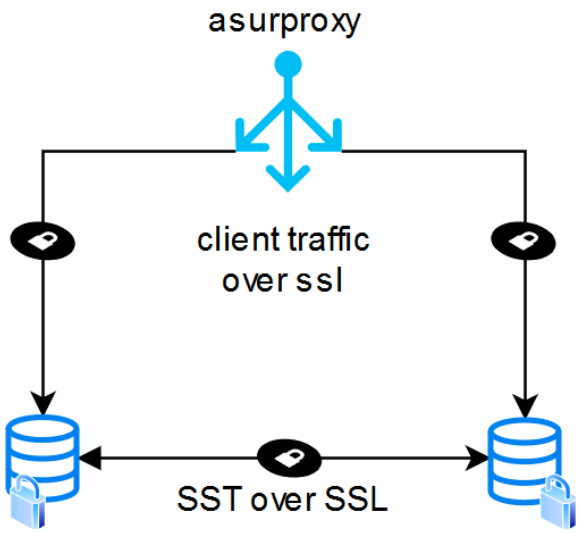
1) I database sono codificati al livello di spazio tabelle (Table space encryption)
2) La replica tra i nodi cluster è codificata (SST encryption)
3) Sono codificati i log binari (Binlog encryption)
4) È implementata la codifica del traffico client con ausilio di SSL.

La encryption dei punti 1,2,3 è una crittografia a doppia chiave (asimmetrica), implementata attraverso una Certification Authority (CA) locale installata nel server asurproxy,

La CA è un soggetto terzo di fiducia (*trusted third part*), pubblico o privato, abilitato ad emettere un certificato digitale tramite una procedura di certificazione che segue standard internazionali e in conformità alla normativa europea e nazionale in materia. La tecnologia per la cifratura è di tipo asimmetrico, cioè la crittografia a doppia chiave. In questa tecnica una delle due chiavi viene resa pubblica all'interno del certificato (chiave pubblica), mentre la seconda, univocamente correlata con la prima, rimane segreta e associata al titolare (chiave privata). Una coppia di chiavi può essere attribuita a un solo titolare. L'autorità dispone di un certificato con il quale sono firmati tutti i certificati emessi agli utenti.

Le chiavi utilizzate sono di tipo RSA da 2048 bits.

Seguendo le best practices per la sicurezza dei dati, la chiave privata della CA è stata rimossa dal server asurproxy in modo da non permettere la generazione di nuovi certificati server.



Al fine di ridurre le vulnerabilità del sistema è stato effettuato una operazione di hardening sulle VM. Questa attività comporta la riduzione delle componenti software allo stretto necessario al funzionamento del servizio.

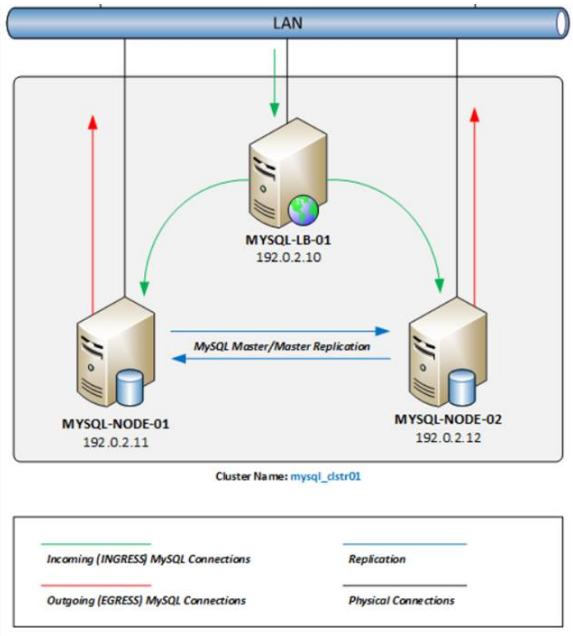
Sui sistemi sono state effettuate le seguenti operazioni di hardening:

1) Ogni database è vincolato ad un solo utente specifico per ogni server di zona
2) Accesso ai db è garantito solo al server asurproxy
3) ProxyDB è stato configurato con policy di sicurezza che consentono l'accesso solo agli specifici database da specifici server di zona

Proxy SQL

Il nodo Proxy SQL è un Load Balancing (bilanciatore di carico), ovvero è un software che permette di smistare le connessioni in ingresso verso più server.
I vantaggi principali della soluzione sono:

- Bilanciamento del carico sui nodi di back end, al fine di garantire sempre le migliori prestazioni
- Alta disponibilità e affidabilità del servizio in quanto, in caso di fault di uno dei due server di backend (DB o Media), le richieste vengono indirizzate sul nodo attivo.



Portale piattaforma Nauta Salus

L'accesso al servizio da parte degli utenti avviene tramite il portale www.nautasalus.com, dove viene richiesto un codice identificativo di verifica della validità della licenza di utilizzo.
Il portale effettua un controllo sullo stato amministrativo del codice utenza immesso e a questo punto instrada l'utente verso il server di zona agganciato al codice utenza richiesto, attivando delle sessioni direttamente su quel server. L'interfaccia mostrerà un menu con i servizi ai quali può accedere l'utente.

Lo stato delle sessioni è gestito dai singoli server di zona.
Ogni volta che un'istanza di server riceve una richiesta da parte di un client, prima di gestire la richiesta stessa, carica lo stato della sessione salvate in locale.
Ogni volta che avviene questa operazione viene aggiornato il registro delle sessioni.

3.1 Flussi operativi

3.1.1 Percorso di autenticazione

Al fine di utilizzare un metodo di autenticazione sicuro, tutti gli applicativi comunicheranno con il sistema di autenticazione Cohesion della Regione Marche.

Di seguito il flusso di autenticazione:

1. Autenticazione alla piattaforma NautaSalus
    a. L'operatore si collega al portale www.nautasalus.com e si autentica con le proprie credenziali
    b. La piattaforma NautaSalus verifica che il servizio sia attivo e riconosce a che zona territoriale è associato il richiedente
2. Indirizzamento al server di Zona
    a. L'operatore viene indirizzato al server di zona sul cloud TIM
3. Autenticazione dell'operatore
    a. L'operatore viene rindirizzato sul portale Cohesion per l'autenticazione
4. Accesso al servizio
    a. Il portale Cohesion autentica l'operatore e invia il codice fiscale al server di zona
    b. Il server di zona abilita l'operatore al servizio richiesto

3.1.2 Percorso di gestione database

L'accesso ai dati della piattaforma Nauta Salus avviene tramite richieste gestite dalla macchina proxy SQL. I diversi applicativi, che risiedono nei diversi server di zona, inviano la richiesta di accesso al database alla VM Proxy SQL, che a sua volta comunica con il cluster DB.
Come specificato nei precedenti paragrafi l'architettura proxy SQL, assieme al cluster DB, assicura la costante disponibilità dei dati e sicurezza.

Al fine di garantire un elevato livello di sicurezza sono state implementate le seguenti tecniche:

- Accesso ai dati dei DB esclusivamente da parte della VM ProxySQL
- Comunicazione cifrata tra la VM ProxySQL e il cluster DB
- Comunicazione con il ProxySQL limitata, attraverso policy, alle sole Apps dei server di zona

3.1.3 Percorso di sincronizzazione

Al fine di sincronizzare i dati sulla piattaforma di INSIEL (dove sono residenti l'archivio delle prestazioni sanitarie, degli assistiti, dei PAI e degli operatori), sono previsti due flussi di dati da e verso la stessa piattaforma.

2. La piattaforma di INSIEL espone dei web services con i dati riguardanti:
    - Anagrafica Operatori
    - Anagrafica Assistiti
    - Elenco delle Prestazioni
    - PAI (Piano Assistenziale Integrato)

    Questo aggiornamento avviene 3 volte al giorno.

3. La piattaforma Nauta Salus invia, tramite web services, alla piattaforma di INSIEL i dati riguardanti:
    - Il rapporto delle prestazioni erogate dagli operatori agli assistiti

    Questo aggiornamento avviene 3 volte al giorno.

Il livello di sicurezza della comunicazione è quello fornito dai web services messi a disposizione da INSIEL. In particolare, è implementata una sicurezza a livello di messaggio tramite SOAP, un protocollo per lo scambio di messaggi tra software.

Nello scambio di messaggi è utilizzato un header SOAP fisso ed in chiaro per verificare l'autenticazione.

Nonostante il canale di comunicazione non utilizza un meccanismo di crittazione dei dati, il livello di sicurezza è garantito dalla rete MPLS su cui avviene il trasferimento dei dati.

3.2 Back up e Recovery

Al fine di gestire il recupero dei dati e il ripristino del servizio, è attivo su ogni VM il servizio di backup offerto da SPC Cloud.

Le policy di backup del servizio SPC Cloud sono:

- Full BackUp settimanale
- Backup incrementale: giornaliero
- Retention: 30 giorni

Oltre a questa protezione, l'architettura è stata progettata per garantire protezione ai dati contenuti all'interno del database (VMs DB). In particolare, è prevista la suite Percona che, come descritto in precedenza, replica i dati sulle due VM DB. In questo modo in caso di down di una delle due VM DB il servizio non subisce interruzioni.

Di seguito le caratteristiche che sono state prese in esame per la scelta della soluzione di back up:

- Procedure operative
- Modalità Agent
- Encryption del data base di back up
- Tempi di retention: RPO (quanta parte dei dati contenuti all'interno di questi sistemi e applicazioni l'azienda possa permettersi di perdere) e RTO (in quanto tempo può essere completato il ripristino)

Di seguito la valutazione sui singoli nodi dell'infrastruttura:

- Server di zona: le caratteristiche della VM rimangono invariate nel normale funzionamento del servizio, quindi in caso di down, il backup del servizio SPC Cloud è immediatamente disponibile per il ripristino.
- Proxy SQL: le caratteristiche della VM rimangono invariate nel normale funzionamento del servizio, quindi in caso di down, il backup del servizio SPC Cloud è immediatamente disponibile per il ripristino.
- DB: è configurato in alta affidabilità e i dati sono allineati grazie alla replica SST, quindi in caso di down di una VM del cluster non c'è disservizio. Mentre, in caso di down di entrambe le VM DB è immediatamente disponibile il backup del servizio SPC Cloud.
- Media: I dati sono duplicati, quindi in caso di down ci sarà continuità del servizio con un eventuale degrado delle prestazioni, visto che tutto il carico sarà gestito da una singola macchina. Mentre, in caso di down di entrambe le VM Media è immediatamente disponibile il backup del servizio SPC Cloud
- VPN: le caratteristiche della VM rimangono invariate nel normale funzionamento del servizio, quindi in caso di down, il backup del servizio SPC Cloud è immediatamente disponibile per il ripristino.

In seguito a queste considerazioni è possibile dichiarare i seguenti SLA per il ripristino del servizio:

- RPO = 0

4 Organizzazione secondo normativa GDPR

L'azienda ASUR Marche nomina TIM spa responsabile del trattamento. TIM nomina a sua volta La società Dinets srl responsabile del trattamento in quanto cloud enabler del progetto