DRS-SLR

Secure long term repository

RDSlab
data retention systems

RDSLab srl a DRSLab company

RDSlab
data retention systems

INDEX


Data Protecti

Cosa significa Data Retention

La Data Retention è la tecnologia che consente di:

- acquisire e archiviare enormi quantità di dati elementari rappresentanti eventi di varia natura;
- conservare questi dati per lunghi periodi di tempo;
- garantire l'inalterabilità , la consistenza del dato e la sua validità nel tempo;
- ricercare e restituire i dati rilevanti al cliente ed all'eventuali richieste dell' Autorità giudiziaria in tempi brevi, fornendo evidenza incontestabile sulla loro attendibilità, affinché possano essere utilizzati anche in procedimenti penali .

La Data Retention è uno dei principali strumenti di indagine per le agenzie investigative, con applicazioni che richiedono enorme scalabilità, lunghi periodi di archiviazione e veloci capacità di risposta.

Caratteristiche DRS-SLR

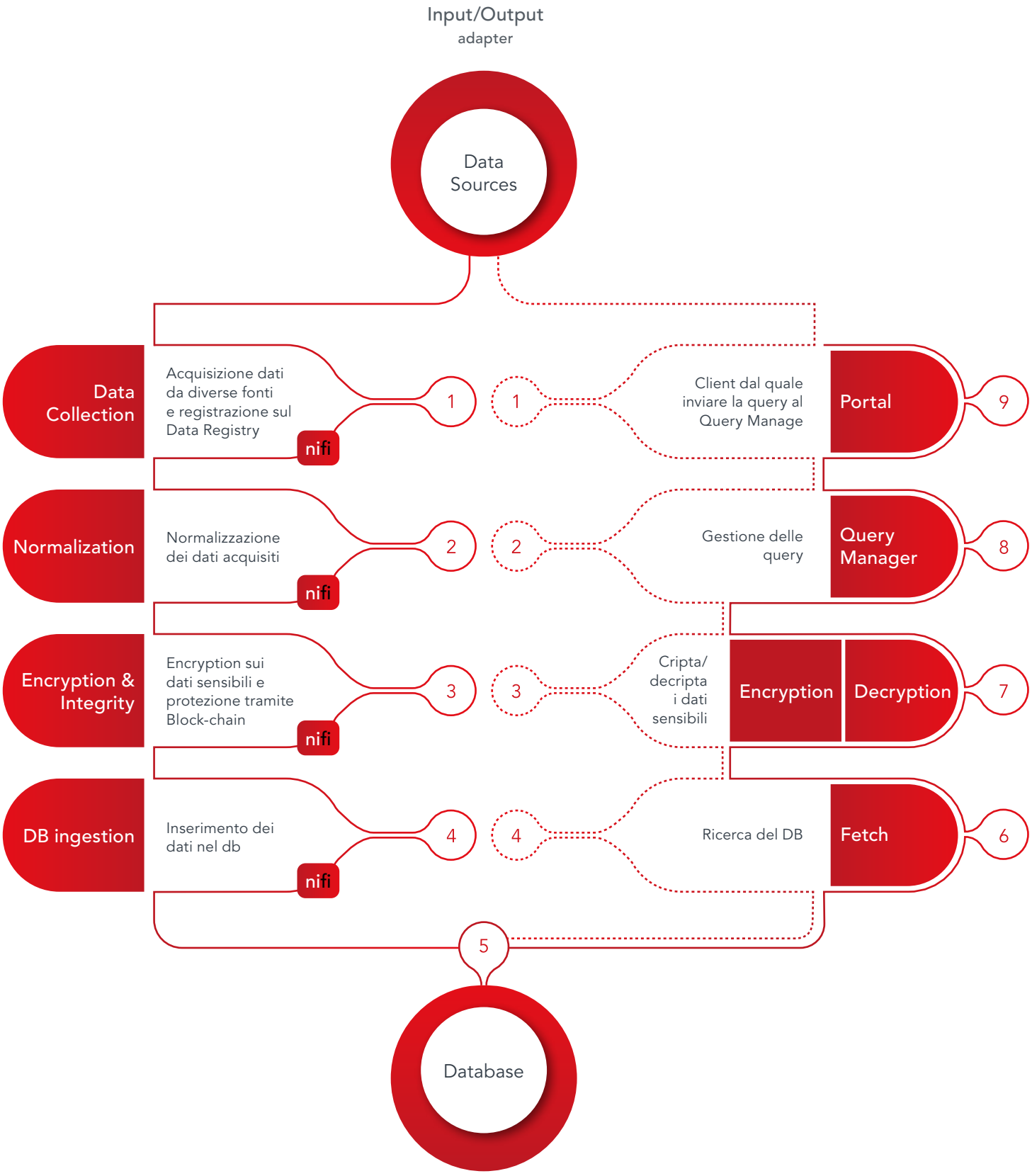
Acquisizione:
- Integrazione di fonti eterogenee.
- Filtri in ingresso per i dati da acquisire.

Normalizzazione:
- Semplificazione delle attività di ricerca.
- Integrazione con script esterni (Python, Perl, Ruby), funzioni Java.

Integrità e Criptazione:
- Utilizzo di algoritmi proprietari (DRS-Encryption), o standard attualmente in uso.
- Integrità dei dati acquisiti tramite uno schema hash di tipo block-chain.

Search:
- Ricerca dei dati nel rispetto dei differenti SLA.

Workflow


Input/Output
adapter
Data
Sources
Data
Collection
Acquisizione dati
da diverse fonti
e registrazione sul
Data Registry
nifi
1
1
Client dal quale
inviare la query al
Query Manage
Portal
9
Normalization
Normalizzazione
dei dati acquisiti
nifi
2
2
Gestione delle
query
Query
Manager
8
Encryption &
Integrity
Encryption sui
dati sensibili e
protezione tramite
Block-chain
nifi
3
3
Cripta/
decripta
i dati
sensibili
Encryption
Decryption
7
DB ingestion
Inserimento dei
dati nel db
nifi
4
4
Ricerca del DB
Fetch
6
5
Database

Data Collection

NiFi acquisisce i dati da diverse sorgenti (DB, FTP, HTTPS o da locale), per ogni file acquisito crea un FlowFile che sarà successivamente registrato all'interno del Data Registry.
L'acquisizione dei dati di traffico dalle fonti avviene attraverso un canale cifrato con mutua autenticazione e successivo controllo sul codice hash del file. Se il controllo è negativo viene richiesto un nuovo invio.

Normalization

Una volta che il FlowFile è stato creato e registrato nel Data Registry viene invocato il modulo proprietario java DRSHNormalizeEncrypt che normalizza il contenuto di quest'ultimo.

Encryption & Integrity

DRS-H utilizza uno schema di encryption di tipo pseudo omomorfico. Infatti, seppur non permettendo operazioni sui dati cifrati, si comporta come tale offrendo la possibilità di effettuare ricerche di uguaglianza e match parziali sugli stessi.

Questa flessibilità nella fase di ricerca dei dati è resa possibile grazie all'implementazione proprietaria dello schema di encryption, basato su Spritz Stream Cipher, 3DES, AES.

DB Ingestion

Il contenuto del FlowFile viene inserito all'interno del db attraverso un apposito modulo di NiFi

DB

I file verranno conservati all'interno del db scelto durante la fase di installazione. Non esiste alcun vincolo sul tipo di database che può essere utilizzato durante questa fase

Query Manager

E' il modulo che esegue la cifratura/decifratura per eseguire le richieste di ricerca dati proveniente dal portale.

A fronte di richieste di estrazione da parte dell'autorità giudiziaria, per garantire l'integrità dei dati che l'AG archivia nel procedimento penale, viene posta la firma digitale dell'operatore che ne garantisce l'autenticità. In alcuni casi questo metodo comunque non viene gestito dalla AG in quanto crea un problema di conservazione della chiave. In questi casi si ricorre alla fornitura del file nei due formati TX e PDF con allegato l'hash del file TX.

Fetch

Terminata la preparazione della query da parte del Query Manager, in questa fase avviene l'interrogazione del db per estrarre i dati richiesti

Apache NiFi

Apache NiFi nasce originariamente come un progetto interno della NSA. Scopo principale è la gestione e l'automazione di flussi di dati fra sistemi.

Caratteristiche principali:

- alta configurabilità: applicazioni a bassa latenza vs applicazioni ad alta portata, prioritizzazione dinamica dei file in coda, loss tolerant vs guaranteed delivery;

- data provenance: tracciamento completo delle trasformazioni e dello sviluppo dell'output all'interno del flusso;

- estensibilità: compatibilità con i maggiori prodotti di storage e i tool in ambito Big Data e non.

DRS-SLR Data Integrity

- Protezione dei dati archiviati e degli audit logs.
- I dati sono garantiti attraverso il sistema di BlockChain.
- Tale sistema consiste nel generare un HASH del record con l'aggiunta dell'HASH del record precedente.
- Si crea così una catena dove non è più possibile alterare un singolo record senza dover alterare tutti i record successivi.
- Esiste Inoltre un registro di tutti i file processati con i numeri dei record ed un elenco di tutti i file presenti nel db in modo da non poter aggiungere o rimuovere file (anche avendo i necessari privilegi).

Viene Generato l'HASH (SHA-128-256-384-512) del primo record

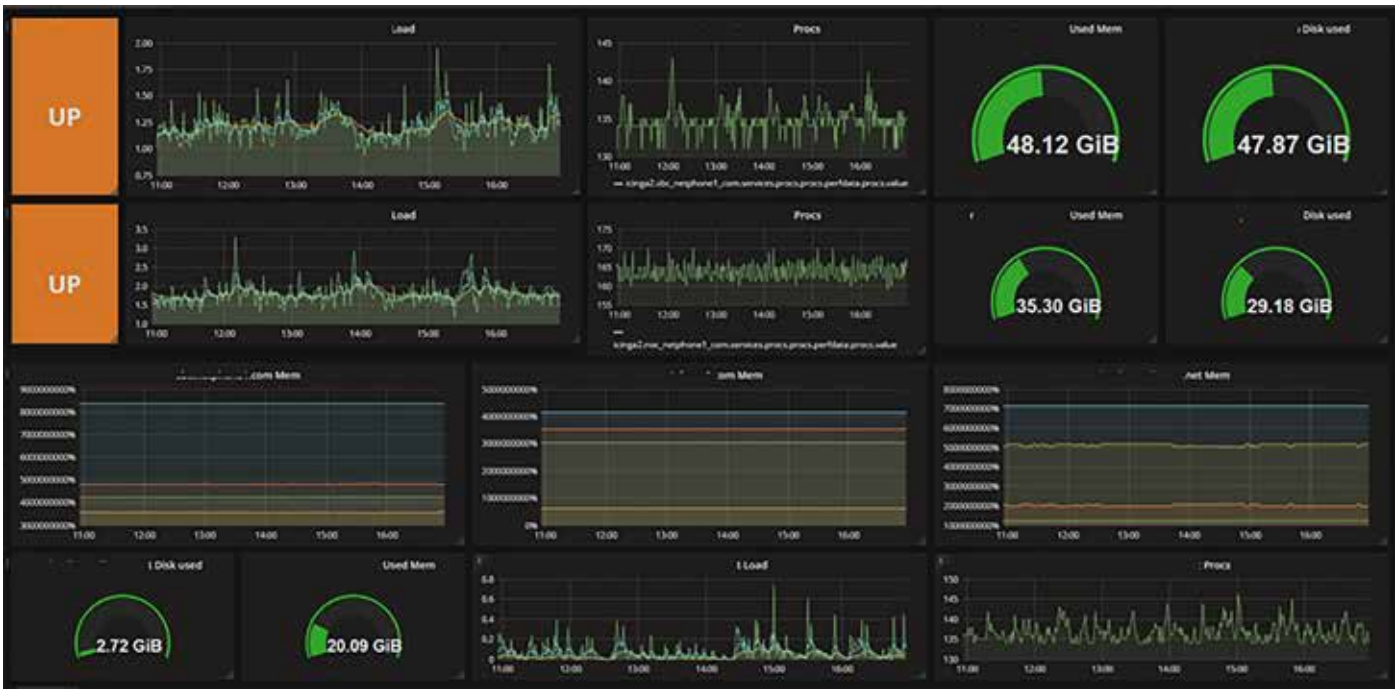
Viene Generato l'HASH (SHA-128-256-384-512) del Secondo record aggiungendo l'HASH del primo

...

Viene inserita la digital signature dell'hash dell'ultimo record con external time stamp

RDSlab
data retention systems

DRS-SLR DashBoard



RDSLab srl

Address
Viale Europa, 55 - 00144 Roma (Italy)

Tel. (+39) 06-45438922
Fax (+39) 06-45438139
info@rdslab.com

RDSLab srl a DRSLab company

Address
Drslab inc.
533 Airport Blvd.
Ste#400
Burlingame , CA, 94010
Tel. +1-650-373-2083