Il 15 novembre 2016 è stato pubblicato all'interno dell'area Azure Documents il documento "What is Log Analytics?". L'Auditing applicato ai servizi ICT non è cosa nuova, la lettura è sempre contrastante, chi lo interpreta come una importante misura di tracciabilità, chi come un male necessario. Microsoft Operations Management Suite – Log Analytics (LA) è una soluzione completamente cloud based che promette di rispondere a tutte le caratteristiche necessarie ad implementare un moderno sistema di auditing e molto più. LA è componibile tramite singole soluzioni che definiscano sorgenti dati e "intelligenza" nell'interpretazione dei dati raccolti, in questo articolo sarà affrontata unicamente la solution di Security (https://opbuildstorageprod.blob.core.windows.net/output-pdf-files/en-us/Azure.azure-documents/live/log-analytics.pdf).

di Carlo Mauceli

IT SECURITY AUDITING: MICROSOFT LOG ANALYTICS

Carlo MAUCELI *è National Digital Officer della filiale italiana di Microsoft, con la responsabilità di promuovere l'innovazione del Paese, gestendo i rapporti con le government élites, i leader accademici e i decisori pubblici e contribuendo alla definizione di una politica tecnologica funzionale alla digitalizzazione del territorio.*

1. Introduzione

Il tema dell'auditing applicato ai servizi ICT non è cosa nuova, la lettura è sempre contrastante, chi lo interpreta come una importante misura di tracciabilità, chi come un male necessario. Chi cerca di implementarlo coprendo tutti gli ambiti amministrativi di un moderno sistema ICT, chi prova a limitarlo alle misure minime di sicurezza imposte dalla legge.

Quale che sia l'approccio scelto, e per inciso si ritiene che sia quanto mai necessario oggi avere una strategia di sicurezza del dato che comprenda un auditing completo, tutte le soluzioni implementate *on-premises* (presso i datacenter di proprietà) soffrono di limiti tecnologici che è difficile gestire:

- Il volume dei dati raccolti è importante, in molti casi diventa la base dati più voluminosa in azienda. La dimensione è direttamente proporzionale ai costi di gestione e dei servizi accessori, in primis le politiche di protezione in termini di Recovery Point Objective e Recovery Time Objective. Anche se esistono soluzioni che tentano di ridurre le dimensioni del dato raccolto queste vanno o a discapito delle performance, oppure causano un data loss mantenendo solo alcune proprietà dell'evento originale.
- La dimensione della base dati implica che è molto costoso ottenere performance accettabili in fase di ricerca del dato.
- È possibile garantire la non modificabilità del dato una volta raccolto solo tramite un processo organizzativo, ovvero tramite nomina di un auditor o Data Protection Officer che abbia esclusivo accesso al vault dei dati e che non detenga alcun diritto amministrativo sui servizi soggetti ad audit. Nelle piccole e medie aziende questo processo organizzativo ha sfide quasi insormontabili. L'unico modo tecnico per garantire la non modificabilità del dato sarebbe un meccanismo di signature con time stamping pubblico sia a livello di riga sia a livello di intero stream in modo progressivo. In passato ho valutato una soluzione con queste caratteristiche, ma non era in grado di garantire scalabilità quando gli eventi iniziavano ad essere nelle migliaia per secondo, non conosco una soluzione sul mercato che faccia questo.

La risposta a questi vincoli è una soluzione che:

- catturi il dato in *real time* (o *near real time*);
- trasferisca il dato in un *vault* esterno al perimetro dell'auditing, tramite un protocollo mutuamente autenticato e crittografato, dove diventa non più modificabile sia per caratteristica tecnologica sia per impossibilità di accesso in scrittura (write once, read many);
- garantisca un processo di *ingestion* senza perdita di informazioni, anche inc aso di trasformazione è fondamentale che nessuna delle proprietà native venga perduta (l'indicizzazione è ovviamente necessaria per garantire tempi di risposta idonei)
- garantisca tempi di estrazione nell'ordine dei secondi o delle decine di secondi;
- permetta di esportare le interrogazioni verso sistemi di analisi *on-premises* (esempio in Excel);
- permetta di creare *dashboard* di controllo nativamente o tramite *feeding* di sistemi di business intelligence (esempio PowerBI);
- sia facilmente estensibile e permetta di raccogliere dati da qualsiasi piattaforma.

Microsoft Operations Management Suite – Log Analytics (LA) è una soluzione completamente *cloud based* che promette di rispondere a tutte le caratteristiche necessarie ad implementare un moderno sistema di auditing e molto più. LA infatti è un sistema di *data ingestion* e *analysis general purpose* che permette di applicare sui dati raccolti interrogazioni su cui basare *alerting*, *reporting*, *dashboard*, export in locale o verso account PowerBI.

LA è componibile tramite singole soluzioni che definiscano sorgenti dati e "intelligenza" nell'interpretazione dei dati raccolti, in questo articolo sarà affrontata unicamente la solution di Security. La solution di Security permette infatti di fare molto più che mero auditing:

- Aggrega diverse fonti dati in "Security Domains", non solo eventi di security, ma anche informazioni su antimalware, patching, traffico di rete e molto altro
- Estrae situazioni di attenzione in "Notable Issues" e permette di integrarle con propri allarmi
- Incrocia i dati raccolti dalle varie fonti con l'engine di intelligenza artificiale alimentato dal security team di Microsoft "Threat Intelligence".

2. L'Auditing secondo la legislazione italiana

Se pensiamo alla situazione italiana, la legge 196/03 e più specificatamente l'allegato B con tutte le sue integrazioni, richiede l'auditing dell'accesso amministrativo ai dati "protetti". I dati protetti sono tutti quelli definiti "sensibili", ma comprendono anche quelli definiti "personali" in base alle indicazioni dell'ufficio legale dell'azienda. **Occorre aggiungere che l'elenco completo delle attività previste per l'"amministratore di sistema" può essere delegata, pertanto tale figura può non essere limitata al solo "root", "sudoable", "administrator" o "domain admins": chiunque acceda ai sistemi con le relative deleghe previste per tale figura è nei fatti un "amministratore di sistema"**. Quindi il caldo consiglio è di collezionare l'accesso e le operazioni di tutti gli utenti.

Esistono altre normative a livello europeo ed italiano che richiedono un sistema di tracciabilità. Non sono un legale e quindi non mi addentro oltre, ma conto presto di integrare questo intervento con un'interpretazione legale qualificata. Tornando alla 196/03 che ho avuto modo di affrontare in maggiore dettaglio e che sicuramente interessa in modo orizzontale chiunque abbia dati protetti, la normativa richiede alcune caratteristiche tecniche, che vengono indirizzate da Log Analytics come segue:

- **Completezza**: garantita dal fatto che la soluzione colleziona i dati direttamente dalla sorgente (Security log windows, audit trail linux, log di Office 365 e così via) e dal fatto che i log vengono immediatamente collezionati dall'agente. Se l'amministratore decidesse di cancellare il security log, questo evento sarebbe comunque collezionato evidenziando l'operazione.
- **Inalterabilità**: dal punto di vista della proposta per inalterabilità del dato si intende l'impossibilità per gli amministratori oggetto di auditing di modificare il dato raccolto. L'inalterabilità si ottiene prima di tutto grazie alla raccolta "near real time" delle informazioni dai security log e dalla loro trasmissione in modo cifrato sulla rete fino a raggiungere il workspace sulla cloud. Una volta sulla cloud il dato non sarà più modificabile.
- **Integrità**: l'integrità del dato è garantita dal cloud provider e dalla implementazione tecnologica della soluzione
- **Mantenimento per almeno 6 mesi**, ma la soluzione permette di mantenere il dato per 12 mesi.

3. Come funziona

LA, come detto, è un sistema completamente operato da Microsoft dalla *cloud*, mette a disposizione ad oggi due livelli di mantenimento del dato: 1 mese ed 1 anno (390 giorni in realtà). Come tutte le indicazioni di capacity qui indicate, queste sono soggette a modifiche migliorative, tipiche dei sistemi operati dalla cloud. Può raccogliere i propri dati in diversi modi:

- Tramite agenti per i sistemi operativi (Windows o Linux che siano)
- Tramite interfaccia con le diagnostiche memorizzate negli storage account di Azure, questo permette in taluni casi di evitare l'installazione dell'agente all'interno del sistema operativo
- Tramite interfaccia diretta ad altri sistemi (ad esempio Office 365 o Application Insights)

Una volta che le varie sorgenti dati sono state connesse al workspace LA, gli eventi e in generale le informazioni raccolte iniziano ad alimentare il vault in modo sicuro (TSL) e mutuamente autenticato. Appena indicizzate le informazioni vengono messe a disposizione del linguaggio di ricerca della soluzione e possono essere consultate tramite interfaccia web o tramite *web service* REST.

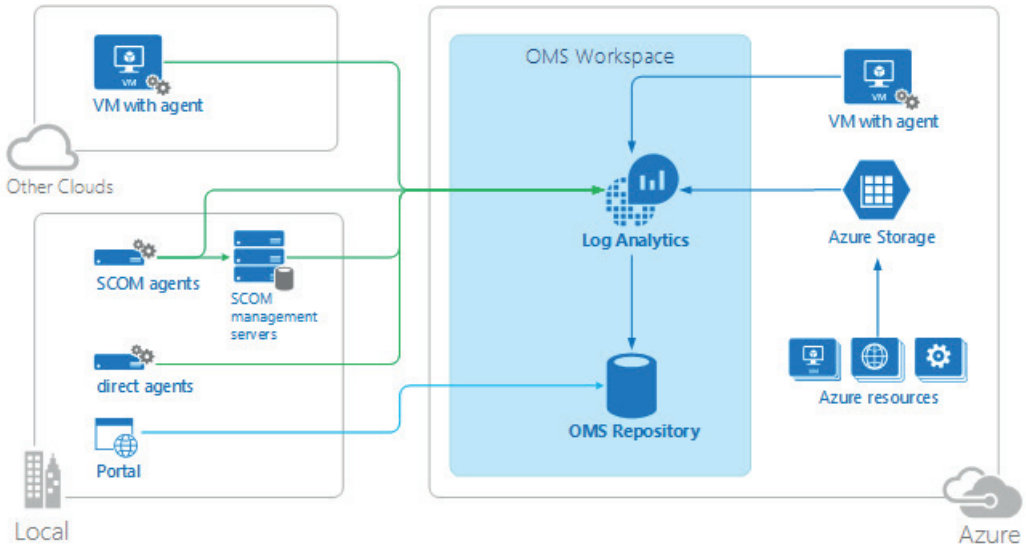

Figura 1 - Log Analytics Architecture
(fonte "What is Log Analytics?" del 15 novembre 2016 disponibile su Azure Documents)

È garantita la *durability* del dato e la sua congruenza, questo permette di delegare completamente tutti i temi che riguardano la protezione del dato raccolto. In caso di assenza di connettività l'agente sui sistemi è autonomo per 2 ore, accodando il dato ed effettuando tentativi di trasmissione ogni 8 minuti.

4. Dove sono i miei dati e quali garanzie ?

Alcune aziende classificano anche i dati di auditing come dati protetti, ma in generale tutte considerano questi dati come un patrimonio importante su cui esercitare le opportune misure di controllo. Come per tutti i servizi implementati su Microsoft Azure è possibile scegliere la region dove memorizzare i dati, il numero di datacenter dove è implementato LA è in costante aumento. Al momento è possibile memorizzare i propri dati presso il data center "West Europe" e avere quindi garanzia che i dati rimangano sul territorio della comunità europea.
Essendo un servizio basato sui datacenter Azure eredita da questi tutte le caratteristiche di sicurezza fisica e logica, in particolare Log Analytics è al momento è certificato: ISO/IEC 27001 , Service Organization Controls (SOC) 1 Type 1 and SOC 2 Type 1 .

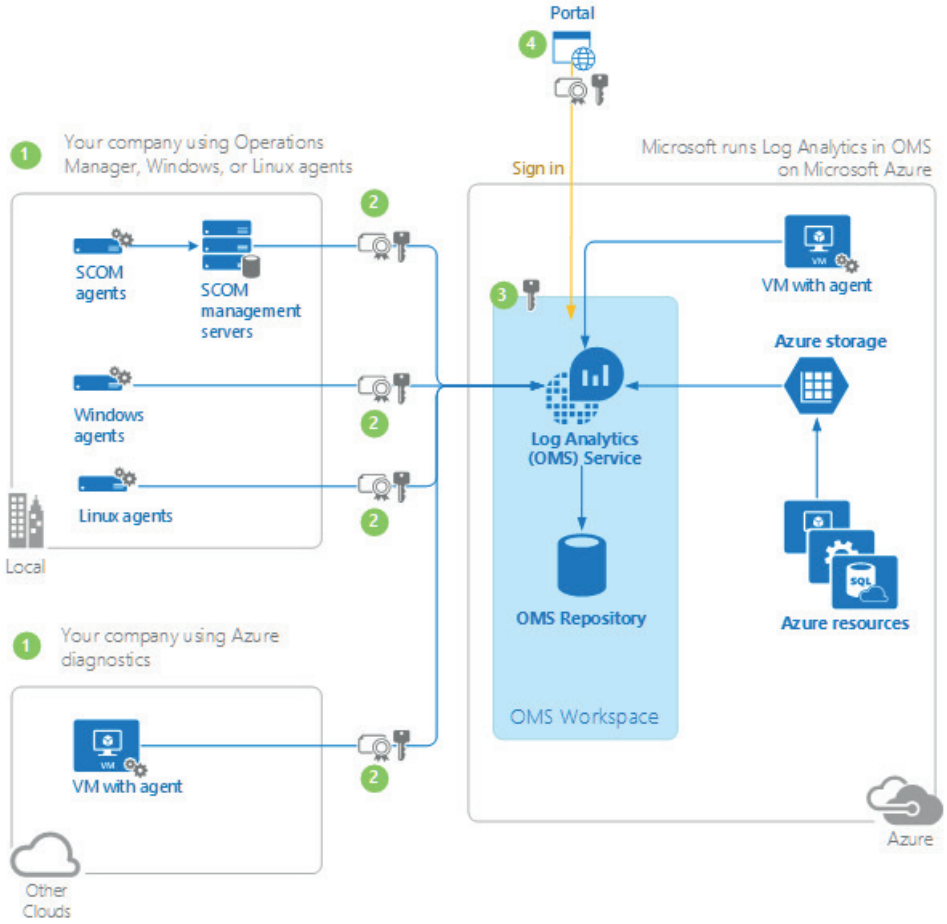

Figura 2 - Cloud Security Architecture: flusso delle informazioni dall'Azienda al servizio Log Analytics
(fonte "What is Log Analytics?" del 15 novembre 2016 su Azure Documents)

5. Quali dati posso collezionare ?

LA è una soluzione che permette di collezionare qualsiasi tipo di *log*, in base al tipo e alla sorgente possono cambiare tempi e modalità di inclusione, di seguito una sintesi delle tipologie e delle sorgenti più comuni: Windows security event logs, Windows firewall logs, Windows event logs, Linux audit trail, Network / syslog, Office 365, Other custom logs.
Il Progel Security Log Gateway è una soluzione che può essere utilizzata per completare LA. Sebbene molte delle fonti dati gestite possano essere incluse tramite meccanismi diversi in LA, il Progel Security Log Gateway trasforma queste sorgenti in eventi di security in modo che possano essere processati con le stesse modalità di *near real time* e di sicurezza.
Al momento il Progel Security Log Gateway permette di processare eventi per i seguenti sistemi:

- Oracle 10i+;
- Exchange 2007+ on premises;
- SQL Server 2005+;
- Custom eventlog transformation.

6. Conclusioni

Microsoft Operations Management Suite Log Analytics è una soluzione *cloud based* che permette di implementare un moderno sistema di audit e monitor della sicurezza senza l'onere di un'infrastruttura *on-premises*, con il valore aggiunto di garantire il mantenimento e l'inalterabilità del dato per 1 anno. ©