Day 6 – Elastic Agents

Introduzione al Problema

Scenario: "Immaginiamo di avere 100 macchine Windows da cui dobbiamo raccogliere i log e inviarli a **Elasticsearch** per poi visualizzarli su **Kibana**.

Tuttavia, alla fine ci dimentichiamo di configurare alcuni agenti, quindi non vediamo nulla su Kibana.

Soluzione:

Fleet Server
Per evitare questi problemi di configurazione, possiamo utilizzare un Fleet Server che centralizza la gestione degli agenti.

Cos'è un Fleet Server?

- Il **Fleet Server** è il componente che connette e gestisce gli **Elastic Agent** da un unico punto centrale.

- Consente di gestire **più agenti** da un singolo server, garantendo la distribuzione e l'aggiornamento degli agenti.

- Facilita l'**aggiornamento delle policy** degli agenti e permette di aggiornare automaticamente gli agenti stessi se sono disponibili nuove versioni.

- Supporta azioni come l'unenroll degli agenti quando necessario(rimuoverlo dal Fleet).

Cos'è un Elastic Agent?

Elastic Agent è un componente centrale dello Stack ELK che semplifica la raccolta e l'invio di dati da vari endpoint verso Elasticsearch. Fornisce un metodo unificato per monitorare, proteggere e gestire i dati provenienti da server, applicazioni e container.

Modalità di Funzionamento:

1. Standalone

- Configurazione Manuale: L'agente è configurato direttamente su ciascun dispositivo.
- Gestione Locale: Ogni macchina gestisce la propria configurazione senza un controllo centralizzato.
- Adatto a: Ambienti con pochi dispositivi o dove la gestione centralizzata non è necessaria.

2. Managed by Fleet

- Gestione Centralizzata: L'agente è controllato tramite Fleet Server.
- Configurazione Automatizzata: Le configurazioni e le policy vengono applicate da una console centralizzata.
- per: Implementazioni su larga scala che richiedono un controllo e una visibilità totali, facilitando aggiornamenti e gestione automatica.

Vantaggi di Elastic Agent rispetto a Beats

Elastic Agent vs. **Beats**:

- **Elastic Agent**:
  - Gestione unificata di log, metriche e dati di sicurezza.
  - Integrazione centralizzata tramite **Fleet Server**.
  - Supporta aggiornamenti automatici e policy centralizzate.
- **Beats**:
  - Agenti separati per diversi tipi di dati (es. Filebeat per log, Metricbeat per metriche).
  - Configurazione e gestione individuali senza supporto centralizzato.

Inputs e Outputs supportati: Beats vs Elastic Agent

Confronto tra Beats e Elastic Agent:

Caratteristica	Beats	Elastic Agent
Input Supportati	Log, Metriche, Traces	Log, Metriche, Traces, Sicurezza
Output Supportati	Elasticsearch, Logstash, File	Elasticsearch, Logstash, Fleet Server
Gestione centralizzata	No	Sì, tramite Fleet Server
Integrazioni	Più Beats separati	Integrazioni unificate tramite policy

Vantaggi del Fleet Server

- Gestione centralizzata degli agenti tramite una singola interfaccia.
- Aggiornamenti automatici degli agenti e delle configurazioni da remoto.
- Possibilità di unenroll degli agent e gestione delle policy in tempo reale.
- Riduce gli errori manuali e garantisce visibilità completa su Kibana.