Installazione di Splunk

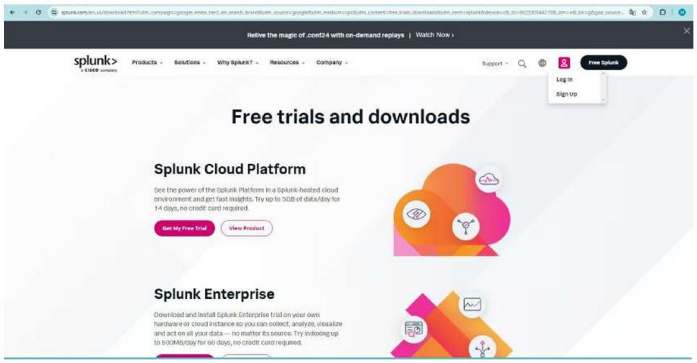
Sommario

Traccia esercizio

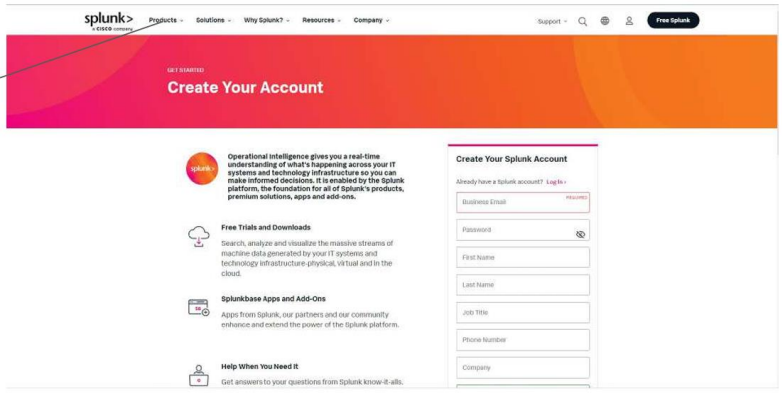
Per installare Splunk andiamo su questo sito.

https://www.splunk.com/en_us/download.html?utm_campaign=google_emea_tier2_en_search_brand&utm_source=google&utm_medium=cpc&utm_content=free_trials_downloads&utm_term=splunk&device=c&_bt=662330344219&_bm=e&_bn=g&gad_source=1&gclid=CjwKCAjw1K-zBhBIEiwAWeCOF3KZmLGB6OREpx_8xYXW6B7a2ESi16-K-9qWnD4walfPdtBef3NVKRoCaX4QAvD_BwE

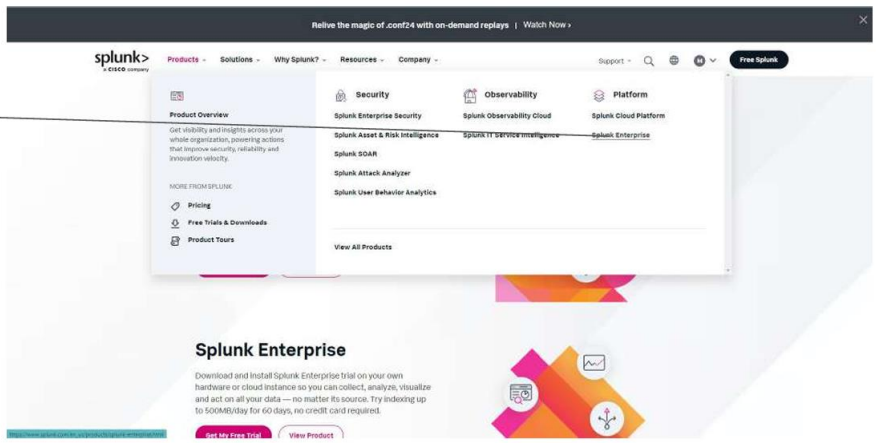
Prima di scaricare Splunk ci dobbiamo registrare.



Una volta compilati i vari campi possiamo fare clic su Products.



Andiamo su Splunk Enterprise.

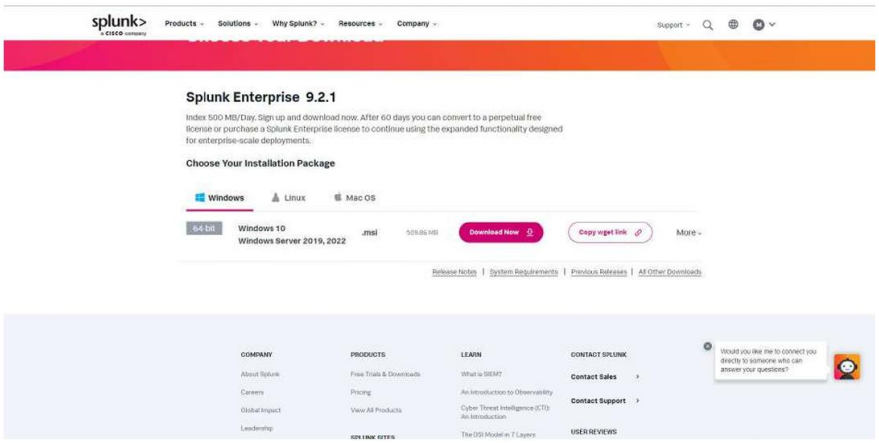


Versione Free Trial

Selezioniamo il sistema operativo e l'architettura.

ATTENZIONE!!!!!

LA VERSIONE FREE durerà 60 giorni o 500MB di dati. Superati questi parametri dovremmo passare ad una versione a pagamento.



Creare l'account.

Finalmente, dopo aver completato l'intera fase di installazione, possiamo esaminare in pratica come analizzare un file di log. Utilizzeremo un file di log fornito da Splunk come esercizio, chiamato "tutorialdata". Questo file di log contiene dati dettagliati sulle richieste HTTP effettuate al server web, come richieste GET e POST, codici di stato HTTP, dimensioni delle risposte, e altri dettagli pertinenti per l'analisi del traffico web e del comportamento degli utenti sul sito del negozio online fittizio "Buttercup Games".

Riassunto dei Contenuti del Tutorial Data

- access.log: Contiene dati di accesso al server web Apache, utili per analizzare il traffico e le interazioni degli utenti con il sito.
- secure.log: Contiene eventi di sicurezza, come tentativi di accesso e altre attività rilevanti per la sicurezza del sistema.
- vendor_sales.log: Contiene informazioni sulle vendite dei prodotti, utilizzato per analisi commerciali e di transazioni.

1. File di Log:
   - access.log: Contiene dati di accesso ai server web, utili per analizzare il traffico web e le richieste fatte ai server.
   - secure.log: Contiene dati relativi alla sicurezza, come i tentativi di accesso e altri eventi di sicurezza.
   - vendor_sales.log: Contiene dati sulle vendite, utile per analisi di vendite e transazioni.
2. Formato dei Dati:
   - I log vengono generati quotidianamente e contengono eventi con timestamp degli ultimi sette giorni, rendendo i dati freschi e rilevanti per l'analisi.
   - I file di log sono in formati standard che Splunk può facilmente indicizzare e analizzare utilizzando i sourcetype appropriati.

Svolgimento esercizio

L'esercizio è guidato, pertanto si rimanda allo slide M6W24D1