



# Advanced Splunk

## CODICE

NOVSAD

## DURATA

2 Giorni

## PREZZO

1.600,00€ (iva escl.)

## LINGUA

Italiano

## MODALITÀ

Virtual Classroom

## SCHEDULAZIONE

- A Richiesta

Splunk is a software platform used for searching, analyzing and visualizing machine-generated big data.

This instructor-led, live training (online or onsite) is aimed at data analysts, data scientists and data engineers who wish to carry out advanced data search, analytics, and visualization using Splunk.

By the end of this training, participants will be able to:

- Create a Splunk application and a technology add-on.
- Use different data input methods and sources.
- Implement advanced search, analysis and visualization of large datasets.
- Customize and share dashboards and reports.

## Format of the Course

- Interactive lecture and discussion.
- Lots of exercises and practice.
- Hands-on implementation in a live-lab environment.

## Course Customization Options

- This training is based on the latest version of Splunk.
- To request a customized training for this course, please contact us to arrange.

## PREREQUISITI

- Experience with business intelligence and data visualization
- Knowledge of Splunk fundamentals

## DESTINATARI

- Data analysts
- Data scientists
- Data engineers

## CONTENUTI

- How to create a Splunk App
- Statistical Commands: Analyze data with stats functions, fieldsummary, appendpipe, count, list, eventstats, and streamstats.
- eval Command Functions: Enhance searches using conversion, text, comparison, informational, statistical, and makeresults functions.
- Lookups: Leverage lookups for advanced data enrichment, including advanced lookup options, lookup-based filtering, KV Store, external, geospatial lookups, and best practices.
- Alerts: Implement comprehensive alerting mechanisms, including logging alert events, using lookups, outputting results, webhook alerts, and log event alerts.
- Field Creation and Management: Advanced field extraction methods, regex field extraction, and regex performance optimization.
- Self-Describing Data and Files: Understand self-describing data, use spath, eval with spath, and multikv commands.
- Search Macros: Master nested macros, macro preview, and using knowledge objects with macros.
- Acceleration Options: Leverage report and summary indexing acceleration, data model acceleration, tsidx files, and tstats commands.
- Search Efficiency: Understand Splunk architecture components, search flow, streaming, transforming, ordering, and job inspector.
- Search Tuning: Pre-filter data, use Lispy operators, wildcards, and TERM.
- Data Manipulation and Filtering: Use bin, xyseries, untable, foreach, strftime, multivalued fields, makemv, mvexpand, and transactions.



- Time Management: Effectively utilize time fields and handle common values/different field names.
- Subsearches: Utilize subsearches for filtering and troubleshooting.
- Prototype Creation: Define XML syntax, follow best practices, and troubleshoot views.
- Forms: Understand tokens, use tokens with form inputs, create cascading inputs, and define token filters.
- Performance Improvement: Identify performance optimization techniques and use tstats and base/post-process searches.
- Dashboard Customization: Customize chart and panel properties, set refresh and delay times, disable search access, and create event annotations.
- Drilldowns: Define drilldown types, use predefined tokens, and create dynamic drilldowns.
- Advanced Behaviors and Visualizations: Implement event handlers, event actions, and contextual drilldowns.

*Prezzi e corsi potrebbero subire variazioni; si consiglia di verificare sul sito [www.novanext.it/training](http://www.novanext.it/training).*