
SPLUNK ENTERPRISE 8.2.8 NEW FEATURES

Contents

End User Experience.....	3
Introducing Splunk Dashboard Studio	3
In-Line SPL Comments.....	4
Seamless SPL History Navigation	4
Federated Search	4
Improved Workload Management.....	5
Admin Productivity	6
Enhanced Performance.....	8

End User Experience

Introducing Splunk Dashboard Studio

Dashboard Studio has advanced visualization tools and flexible layout options to easily create visually-compelling, pixel perfect dashboards. It offers out-of-the-box support for dashboard customization and an intuitive editing interface that enables new and experienced users to easily create the visualizations.

You can access Splunk Dashboard Studio directly within the Search & Reporting app.

It comes with enhanced visualizations for Single Value, Single Value Icon, Table, and Choropleth SVG.



While many features and visualizations are similar to the classic Splunk dashboard framework, there are differences, both in what features are available in the new framework and the way visualizations look.

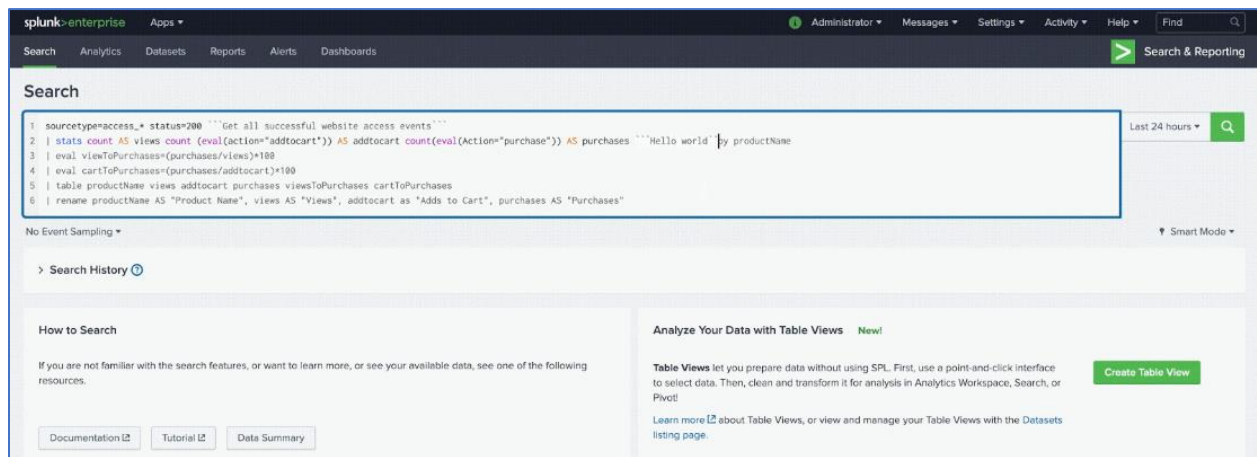
Please refer to below link for more details,

https://www.splunk.com/en_us/blog/platform/dashboards-ga-introducing-splunk-dashboard-studio.html

In-Line SPL Comments

SPL Commenting can make SPL easier to read for very long SPL.

All you need to do is use **three backticks before and after your comment**. You can add as many as you'd like, and it has syntax highlighting for both light and dark mode.



Seamless SPL History Navigation

Search History is an easier way to navigate searches; you can use keyboard shortcuts to iterate through previous searches.

One can toggle through search history in search bar using the below ,

ALT+P → Previous search

ALT+N → Next search

Federated Search

A key capability shipping in this release is Federated Search in hybrid deployments.

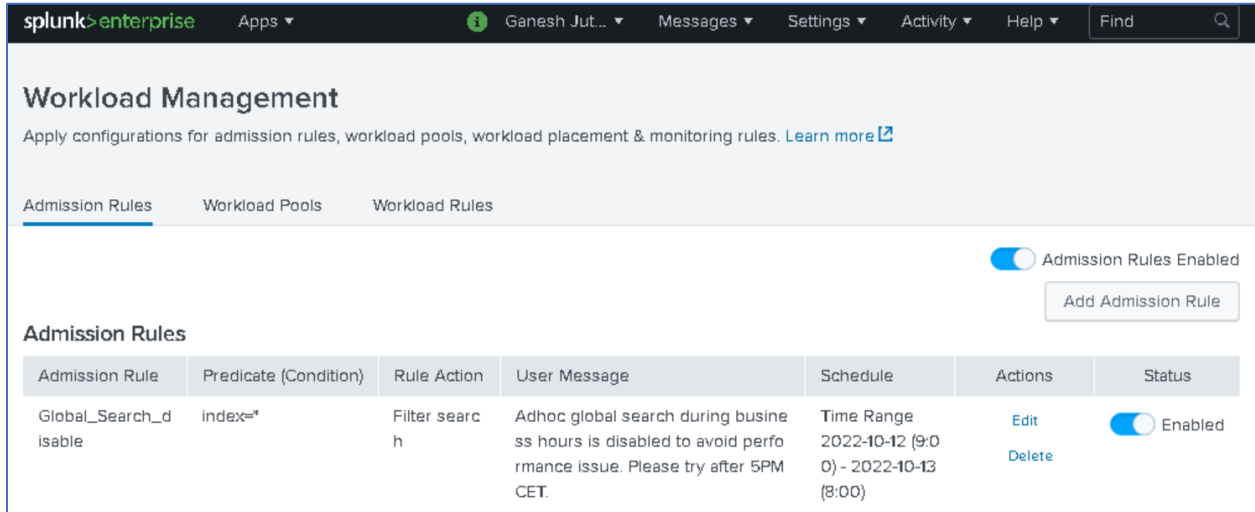
There may be times when you want to run a single query across different Splunk deployments.

This may especially apply if some deployments require regional presence or are subject to data policies.

Improved Workload Management

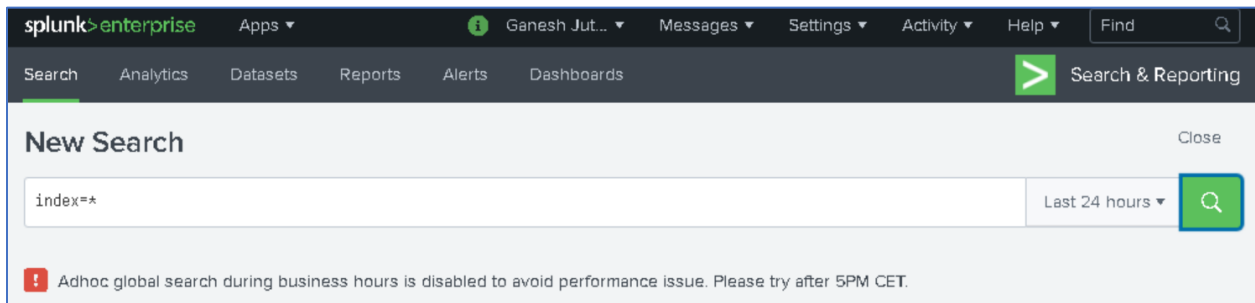
This feature prioritize workloads based on business needs and manage them through user-defined rules.

It's a very powerful tool for you to reduce the impact of unexpected workloads when you need Splunk the most.



The screenshot shows the 'Workload Management' page in Splunk Enterprise. The page has a header with the Splunk logo and navigation links. Below the header, there's a section titled 'Workload Management' with a subtitle 'Apply configurations for admission rules, workload pools, workload placement & monitoring rules. [Learn more](#)'. There are three tabs: 'Admission Rules', 'Workload Pools', and 'Workload Rules'. The 'Admission Rules' tab is active. On the right, there's a toggle switch for 'Admission Rules Enabled' which is turned on, and a button 'Add Admission Rule'. Below this is a table of admission rules.

Admission Rule	Predicate (Condition)	Rule Action	User Message	Schedule	Actions	Status
Global_Search_Disable	index=*	Filter search	Adhoc global search during business hours is disabled to avoid performance issue. Please try after 5PM CET.	Time Range 2022-10-12 (9:00) - 2022-10-13 (8:00)	Edit Delete	<input checked="" type="checkbox"/> Enabled

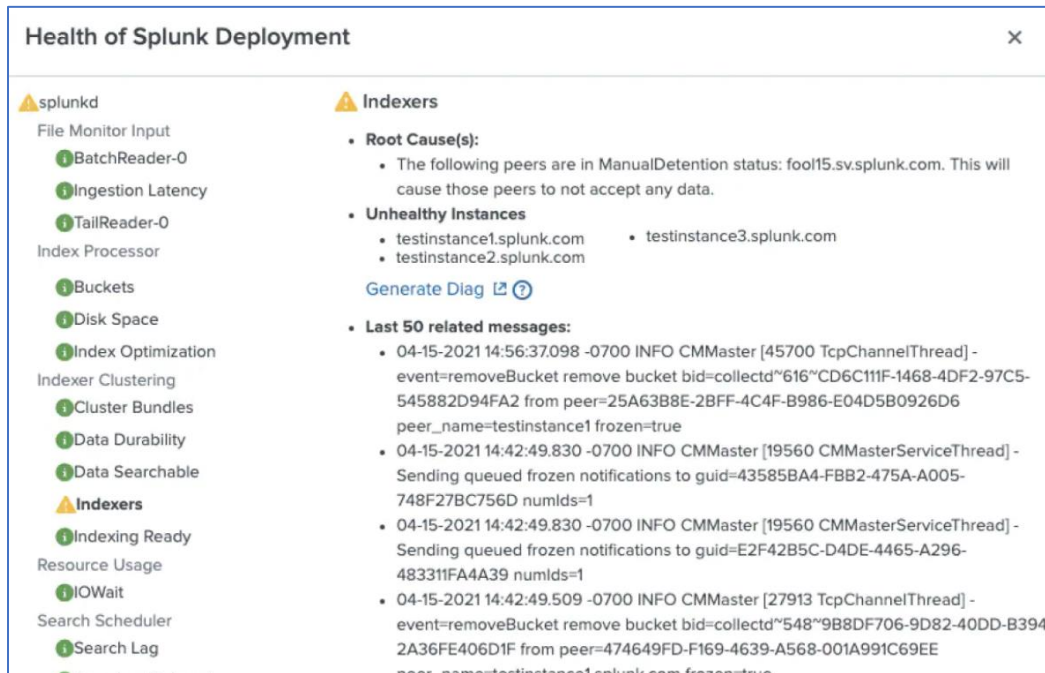


The screenshot shows the 'Search & Reporting' page in Splunk Enterprise. The page has a header with the Splunk logo and navigation links. Below the header, there's a section titled 'New Search' with a 'Close' button. There's a search bar with the text 'index=*' and a dropdown menu for 'Last 24 hours'. A green search button is on the right. Below the search bar, there's a warning message: 'Adhoc global search during business hours is disabled to avoid performance issue. Please try after 5PM CET.'

You can filter for any all-time range searches, disallow searches in peak hours or do ad hoc wildcard searches.

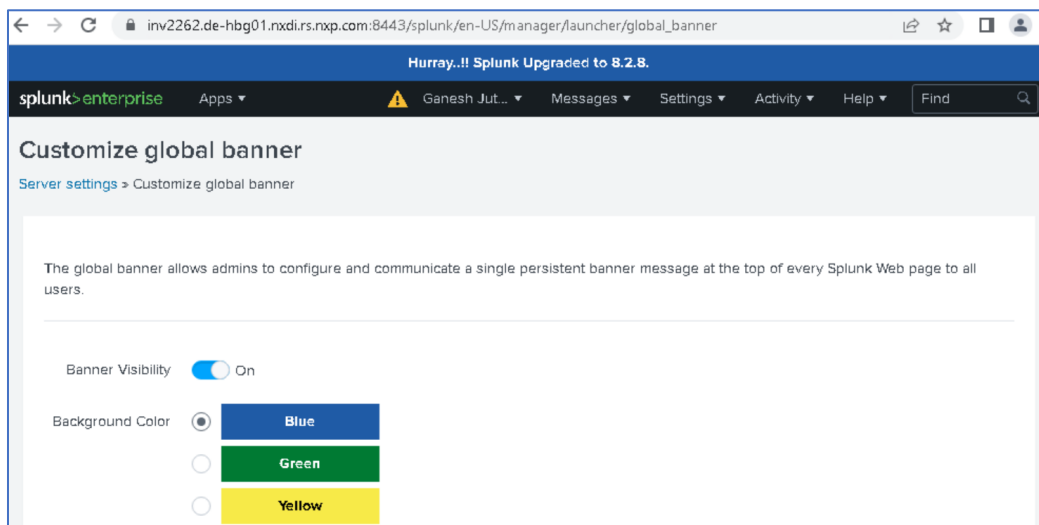
Admin Productivity

- The Splunk Health Report now displays information that is rolled up in a distributed environment so that admins don't have to login to every node.



The screenshot shows the 'Health of Splunk Deployment' report. On the left, a sidebar lists various components: splunkd (File Monitor Input, BatchReader-0, Ingestion Latency, TailReader-0, Index Processor, Buckets, Disk Space, Index Optimization, Indexer Clustering, Cluster Bundles, Data Durability, Data Searchable, Indexers, Indexing Ready, Resource Usage, IOWait, Search Scheduler, Search Lag), Indexers, and Search Lag. The main panel displays the 'Indexers' section, which includes a 'Root Cause(s)' section stating that peers are in ManualDetention status, an 'Unhealthy Instances' section listing testinstance1.splunk.com, testinstance2.splunk.com, and testinstance3.splunk.com, and a 'Last 50 related messages' section showing log entries related to bucket removal and frozen notifications.

- The ability to persist a global banner at the top of every Splunk page so that admins can announce something to all your users! This lets admins to decide what gets put in there, in addition to customizing banner color and hyperlink.



The screenshot shows the 'Customize global banner' settings page in Splunk. The page has a blue header with the Splunk logo and navigation links. The main content area is titled 'Customize global banner' and includes a description: 'The global banner allows admins to configure and communicate a single persistent banner message at the top of every Splunk Web page to all users.' Below this, there are two settings: 'Banner Visibility' (a toggle switch set to 'On') and 'Background Color' (a dropdown menu with options for Blue, Green, and Yellow, with Blue selected).

- Enabled a way to monitor I/O Wait and Ingestion Latency in the Splunk Health Report.
- Included a new set of internal logs that track configuration file changes at the filesystem level for auditing purposes.
- A new feature which allows admins to restrict the end user's search results based on the age of the event.
- Admins will be able to view inheritance for roles or users so that you can see which roles contribute to indexes, on a hierarchical and assignment level. This helps admins to spend less time trying to troubleshoot who has access to what and validating what users should not be able to see. You can now also search as a specific user to validate your RBAC configurations are behaving as expected.
- RapidDiag - offers a way to collect troubleshooting data from OS provided utilities and Splunk Enterprise tools, and place the results into one file. It is designed to ease data collection tasks when working with Splunk Support on troubleshooting your Splunk platform instances.

Enhanced Performance

- 10X faster scheduling of searches
- Performance improvements to support deployments scaling to 40 million buckets, enabling reductions in memory footprint and faster time to recovery.
- Improved search processing performance with optimized lookups and refactored query execution thus day-to-day use of Splunk will be more responsive and streamlined.
- On-premises Splunk Enterprise, the lookups are modified in such a way which are possible at ingest time, not just at search time.
- Major Improvements to Our Metrics Store - aggregate across more than 2M metrics events per second, increasing throughput and speed.
- The use of WiredTiger storage engine in the KV Store, to replace MMAP - improves read/write performance and introduces a pathway for significant reduction in storage requirements.

Compared to current version,

- ✓ rolling restarts are 60% faster.
- ✓ Cluster Manager consumes 75% less memory following a rolling restart.
- ✓ replication and search factors are 73% faster following a rolling restart.