

Integration with the IBM Tivoli Suite

Splunk is the IT search engine. It indexes and lets you search and navigate all of your IT data in real time. Splunk's professional services team is able to deliver seamless integration between IBM Tivoli's family of event consoles and correlation engines and Splunk.

Our Splunk - Tivoli integration service ensures that Splunk is quickly integrated into your existing workflow and processes. It leverages best practices and components developed through working with many customers using Splunk to complement their Tivoli investment, while ensuring a customized solution tailored to the specifics of your topology, users and data.

The Splunk - Tivoli integration can include any console or correlation engine in the Tivoli suite, including:

- Tivoli Enterprise Console (TEC)
- Tivoli Enterprise Portal (TEP)
- Tivoli Netcool Omnibus
- Tivoli Netcool Webtop
- Tivoli Netcool Desktop
-

What's Included

Contextual search from console alerts

Splunk can be launched from alerts appearing in any of the Tivoli consoles, with details of the alert automatically translated into an appropriate Splunk search, usually for all events surrounding the time of the alert occurring on the same host. Splunk's consultants can extend this logic to use any elements of your organization's Tivoli TEC, TEP or Netcool Omnibus schema.

In the Tivoli Enterprise Console (TEC), this is accomplished via the launch application feature. In the Tivoli Enterprise Portal (TEP), this can be accomplished via Splunk's browser toolbars or the built-in launch feature.

For the Netcool Webtop and Netcool Desktop. Splunk will configure tools it has created to implement this functionality natively. Customers can also opt to use the browser toolbar with the Netcool Webtop.

Splunk alerts sent to the console

Splunk's own alerts based on any saved search can be sent to TEC, TEP or Netcool Omnibus via SNMP. Splunk consultants will customize a rules file for any of these engines to ensure that Splunk alerts are informative and correctly mapped to your TEC, TEP or Omnibus schemas. The typical implementation ensures that a single alert appears for each host in a given search, and that a URL is included to launch Splunk with the results of the search.

Real-time indexing of monitoring events

Splunk's consultants will configure your monitoring systems as data inputs to Splunk, so that events that pass through their correlation engines, as well as correlated events, are indexed alongside other IT data and searchable in Splunk. For Tivoli Enterprise Console this will be accomplished via scripting the 'wtdumpurl' utility. For Netcool Omnibus, this can be accomplished through either the Omnibus file or socket gateways.

Benefits

Deploying Splunk significantly improves customer service, increases availability and cuts operational cost by making all of your IT data universally accessible and actionable. Tight integration with Tivoli increases these impacts while improving the effectiveness of your Tivoli implementation.

Get more out of Splunk

- Eliminate the friction of switching between tools during incident investigation and recovery
- Leverage existing incident and problem management processes to handle Splunk alerts

Get more out of Tivoli

- Extend monitoring coverage to your entire environment by harnessing all IT data sources for alerting via automated Splunk searches
- Improve the quality and coverage of Tivoli event correlation by gaining visibility into all of the IT data generated by your environment

Pricing

The Tivoli Integration service is priced at Splunk's standard daily professional services rate of \$2,000 per day plus travel and expenses. The length of the engagement will be determined based on scoping for your specific environment. Contact sales@splunk.com to request a quote.