Getting started with IT Essentials Work

Your IT team is well on the path to IT modernization, having already identified some use cases for Splunk and started to get your data in. Now, you need to kick things up a notch. You're experiencing a range of problems associated with wrangling data stuck in multiple, disparate tools and apps - from incomplete insights and long investigation times, to difficulty in pinpointing root causes. Many of the processes you’re following are inefficient and difficult, resulting in a lot of frustration within your team and ultimately, impacting your customers.

Some of the questions you're probably asking include:

• How can I see what's happening in my entire infrastructure, at a glance?
• How can I troubleshoot problems more quickly?
• How can I use more sophisticated alerting techniques to triage faster?

IT Essentials Work helps you in all of these areas. By consolidating tools, reducing cost and complexity, and correlating all IT data into a single view, IT Essentials Work helps you better understand the performance and health of your entire environment. With prescriptive, curated content that reduces your learning curve, you get step-by-step guidance to expand and accelerate your adoption of Splunk for common IT tasks and use cases.

How it works

IT Essentials Work helps you better manage the entities within your environment. An entity is an IT component that requires management in order to deliver a service. Entities are usually hosts, but can also be cloud or virtual resources, network devices or applications.

IT Essentials Work gives you access to all the default entity integrations, including *nix, Windows, and VMware. After you import your entities, you can view and monitor your entity types in the Infrastructure Overview and drill down further into individual entities to analyze associated log data and track performance metrics.

This diagram shows a basic entity integration workflow, configured to monitor hosts, containers and virtual infrastructures as entities.

IT Essentials Work is well-suited to be used in tandem with IT Essentials Learn. IT Essentials Learn offers a use case...
library with prebuilt search content to teach you how to use Splunk without actually using your own data. IT Essentials Work offers out-of-the-box customizable dashboards and capabilities to onboard your data once you’re ready to work, with easy upgrade to ITSI — helping you visualize and execute on your IT monitoring maturity.

How can I see what's happening in my entire infrastructure?

The Infrastructure Overview helps you to keep tabs on entity health. Out-of-the-box dashboards provide a quick view of the status of key KPIs for different entity types. You can understand what’s going on at an entity level, as well as across your entire infrastructure with Infrastructure Overview. Visualizations let you see which specific entities have high CPU usage and drill down into that specific entity to see what’s causing it. The ability to group by entity type, apply filters and see logs associated with specific metric data enables log-based analysis for speedy and seamless troubleshooting.

From a single view, you can see all your data — whether metric or log event data — and correlate key dimensions for context and performance. You can define groups to easily group and filter infrastructure metrics, status, alerts and investigations. This holistic view allows for a better understanding of infrastructure health so you can observe and understand the performance of your entities. Having one workspace with high-level visualizations makes it easier to determine trends, conduct immediate investigations and reduce context switching.
How can I troubleshoot problems more quickly?

IT Essentials Work lets you use out-of-the-box dashboards to get up and running immediately and see the status of key KPIs over time. You can quickly identify trends or specific points in time where KPI status changed, and drill down into the entity health page where you can monitor metrics like average CPU usage, average memory usage, average datastore latency and average network traffic across all hosts. With IT Essential Work, you can see what’s happening, troubleshoot faults and get a specific, entity-level view of the issue — without writing queries or code or building custom dashboards.

IT Essentials Work includes a feature called Event Data Search, that lets you quickly analyze the health of your infrastructure. Event Data Search looks at entity status across different infrastructure types and identifies inactive entities that could be causing issues in the production environment. With this capability, you can track the status of entities based on variation in data ingestion rate, drill down into individual entities to analyze log data to track performance entities and speed up troubleshooting using the infrastructure data from application logs.

How can I use more sophisticated alerting techniques to triage faster?

Custom-triggered alerting at a group or entity level lets you perform root cause analysis faster. You can also triage alerts more effectively by understanding which conditions triggered the alert, assessing the severity of the alert and viewing all
triggered alerts to decide what actions to take. By setting up thresholds and generating alerts at a specific infrastructure level and being able to analyze alerts across different infrastructure types, you can get alerted on your most vital metrics.

Next steps

Splunk ITSI is your next step on your journey - providing end-to-end service visibility and streamlined incident resolution through business and IT service monitoring, intelligent incident management, and machine learning and predictive analytics.

Find out more about Splunk ITSI here.

Additionally, these Splunk resources might help you understand and implement the recommendations in this article:

- Training: IT Essentials Work - Walkthrough (free course)
- Splunk Docs: Just the Essentials: how we reinvented getting started for IT use cases
- Blogs: Install IT Essentials Work
- Tech Talks: Monitor and troubleshoot VMware infrastructure with Splunk
- .conf: My start will go on: Splunk’s TA for Windows part 1
- .conf: My start will go on: Splunk’s TA for Windows part 2
- .conf: Splunk fundamentals: Working with web server data part 1
- .conf: Splunk fundamentals: Working with web server data part 2
- .conf: Get monitoring tricks for all your *nix - part 1
- .conf: Splunk for Microsoft SQL Server, Part 1
- .conf: Splunk for Microsoft SQL Server, Part 2