Splunk® IT Service Intelligence
Service Insights Manual 4.8.1 Cloud only

Overview of Service Insights in ITSI

Generated: 3/15/2021 11:40 am

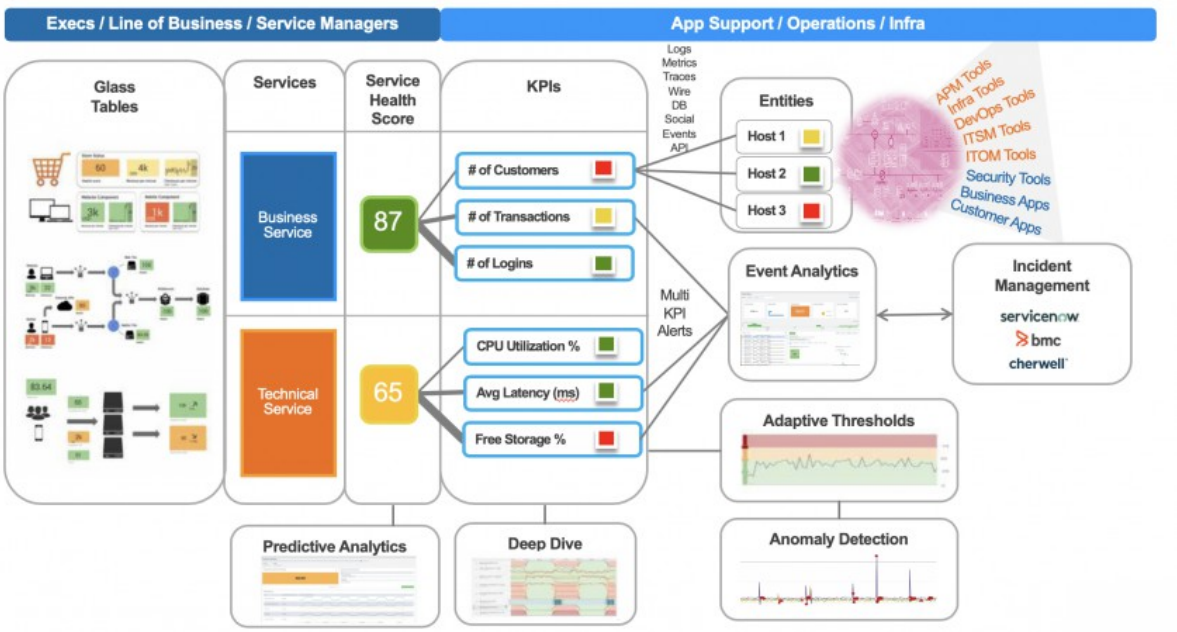
Overview of Service Insights in ITSI

Service Insights in IT Service Intelligence (ITSI) represents the mapping and monitoring of business and technical services within your organization. The information derived from Service Insights helps you better detect problems, simplify investigations, triage issues, and accelerate resolutions.

Within ITSI, a service is a set of interconnected applications and hosts that are configured to offer a specific service to the organization. Services can be internal, like an organization email system, or customer-facing, like an organization's website. For example, creating financial reports through a web-based application requires a computer, web server, application server, databases, middleware, and network infrastructure. These applications and hosts are all configured to offer the service of financial reporting.

ITSI Service Insights helps you map these service dependencies based on a connection between devices and applications. This top-down mapping functionality helps you immediately see the impact of a problematic object on the rest of the service operation.

Service insights provides the following features and functionalities that work together to provide visibility and insight into the health of your services:



Glass tables

Glass tables are custom visualizations that help you monitor KPIs and service health scores. Create glass tables to provide dynamic contextual views of your IT topology or business processes and monitor them in real time. Glass tables feature a drawing canvas where you can add visualizations in the form of KPIs and service health scores, upload images and icons, and add charts.

For more information, see Overview of the glass table editor in ITSI.

Services

A service is a logical mapping of IT objects that applies to your business goals. The definition of a service is fairly broad. For example, a service can be any of the following:

- An application or group of applications
- An infrastructure tier, such as a web, database, or network tier
- A business service, such as an online store, with multiple tiers
- A single process, such as one instance of an application running on a host

Create business and technical services that model those within your environment. Some services might have dependencies on other services. Services contain KPIs (Key Performance Indicators), which make it possible to monitor service health, perform root cause analysis, receive alerts, and ensure that your IT operations are in compliance with business service-level agreements (SLAs).

For more information about creating services, see Overview of creating services in ITSI.

Service health scores

A service's health score is a weighted average of the severity values of a service's KPIs and dependencies. Technically, the health score is a KPI attached to every service, but it's populated by a single search within ITSI. Service Insights uses the health score to assign the service a severity level and color in the Service Analyzer and in glass tables. For more information, see How service health scores are calculated.

KPIs

A KPI (Key Performance Indicator) is a recurring saved search that returns the value of an IT performance metric, such as CPU load percentage, memory used percentage, response time, and so on. A KPI is used to monitor the health of a service.

You create a KPI within a specific service. It defines everything needed to generate searches to understand the underlying data, including how to access, aggregate, and qualify with thresholds. You can use the search result values to monitor service health, check the status of IT components, and troubleshoot trends that might indicate an issue with your IT systems.

For example, `cpu_load_percent` is a KPI that measures the CPU load percentage on a server. If your organization has a site uptime guarantee of 99.9% per month, you will need to monitor the status of this KPI (and others) to ensure that CPU performance remains within acceptable parameters.

For more information, see Overview of creating KPIs in ITSI.

Deep dives

Deep dives are an investigative tool to help you identify and analyze issues in your IT environment. They display a side-by-side view of KPIs and service health scores over time to help you zoom in on metric and log data and visually correlate root cause. For more information, see Overview of deep dives in ITSI.

Entities

An entity is an IT infrastructure component that requires management to deliver an IT service. Each entity has specific attributes and relationships to other IT processes that uniquely identify it. Entities are usually hosts, but can also be items as diverse as cloud or virtual resources, network devices, applications, users, and cell towers.

ITSI entities can be any of the following components:

- Physical, virtual, or cloud resources
- Network devices (switches, routers)
- Users (AD/LDAP)
- Storage systems, volumes
- Operating systems or processes
- Software application (db, web server, business app)
- Application process instances (for example, 2 instances of the same web server application is 2 separate entities)
- Cell towers

Entities contain information ITSI uses to associate services with information found in Splunk searches, imports, and integrations. You can use this entity information to filter items according to the entity definition.

An entity is similar to a "configuration item" in the ITIL framework, but an entity is never a service itself.

Define entities before creating services. When you configure a service, you can specify entity matching rules based on entity aliases that automatically add the entities to your service. For more information about importing, defining, and managing entities, see the IT Service Intelligence *Entity Integrations Manual*.

Adaptive thresholds

Adaptive thresholds are a type of threshold configuration for a KPI that's populated based on a statistical distribution of historical KPI data. They use machine learning techniques to analyze historic data and determine what should be considered normal in your IT environment. The adaptive thresholds automatically recalculate on a nightly basis so that slow changes in behavior don't trigger false alerts. For more information, see Apply adaptive thresholds to a KPI in ITSI.

Anomaly detection

Anomaly detection generates notable events when a KPI IT Service Intelligence (ITSI) deviates from an expected pattern. These notable events represent detected anomalies for service-level (trending) and entity-level (cohesive) KPI data. The algorithms learn KPI patterns continuously in real time and detect when a KPI departs from its own historical behavior. For more information, see Apply anomaly detection to a KPI in ITSI.

Next step: Event Analytics

After configuring Service Insights within ITSI, including ingesting entities and configuring services, it's time to start configuring alerts to notify you when your services and KPIs perform abnormally. That brings you to Event Analytics. To begin setting up alerts and configuring alert actions, see the IT Service Intelligence *Event Analytics* manual.