Gaining better visibility in Microsoft O365

Applicability

• Product: Splunk ITSI or IT Essentials Work
• Feature: Microsoft 365 content pack
• Function: Dashboards and glass tables; Services and KPIs; Entity types and vital metrics

To access the Microsoft O365 content pack library, you'll need to install the Splunk Add-on for Microsoft Office 365 and the Splunk App for Content Packs. For more information, see About the content pack for Microsoft 365.

Problem

Microsoft 365 is your productivity cloud across work for office apps, intelligent cloud services, and world-class security. However, Microsoft provides limited visibility into these critical processes, workflows, and activities. You need better awareness of their status and impact on you or your customers, so you have downloaded and installed the Splunk Add-on for Microsoft Office 365. You need to know how to get started using it.

Solutions

The Content pack for Microsoft 365 provides the elements necessary to collect Office 365 data from the hosts in your server environment and monitor your various services such as the performance, availability, security, incidents, and messages across your Microsoft 365 services. The content pack provides preconfigured services with KPIs that monitor critical functions.

If you are a customer using IT Essentials Work, some of the features in Microsoft 365 content pack will be more limited than the features available for customers using Splunk ITSI.

This content pack provides:

• 49+ services with over 300 KPIs
• 7 glass tables (Splunk ITSI users only)
• A saved service analyzer view for Microsoft 365 (Splunk ITSI users only)
• Several entity types to help you group and analyze entities receiving data from Microsoft 365
• 13 dashboards for various use cases (Limited dashboards available for IT Essentials Work users)

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
**Visualize and monitor the interrelationships and dependencies across your IT and business services**

Glass tables enable you to visualize and monitor the interrelationships and dependencies across your IT and business services. You can use the preconfigured glass tables to create dynamic contextual views of your IT topology or business processes and monitor them in real time. You can add metrics like KPIs, ad hoc searches, and service health scores that update in real time against a background that you design. Glass tables show real-time data generated by KPIs and services.

- The M365 Executive Overview glass table provides insights across 7 major components along the bottom (including Active Directory), along with Security and M365 App Availability on the top, and a rolled up M365 status in the middle. At a single glance, you can quickly understand the status of your environment and use a single click to gain deeper insights.

- The M365 Overview Dashboard glass table puts key operational metrics, trends, and security summaries all on a single view. You can see performance and availability across the 7 core Microsoft 365 apps and Active Directory, along with summary of incidents and messages. Further, this dashboard provides login successes and failures, a summary of key KPIs by each of the 6 main apps, 6 key security summaries, and overall Microsoft 365 health.

- The Microsoft 365 Service Incidents and Messages Dashboard gives visibility into and awareness of what service incidents are happening and each of their statuses, along with insights from messages on what is going to happen.

- The M365 Security Dashboards (Overview, Threat Detection, and Threat Management) provide insights into security highlights across your tenants. The Overview glass table provides roll-up of nearly 100 data points on a single screen, including trending, and threshold notifications where appropriate. To allow for more focused views, the Threat Detection and Threat Management glass tables show details for those specific areas, along with other key indicators across Microsoft 365 to compliment the security focus.

**Monitor service health and ensure your IT operations are in compliance with business SLAs**

- A KPI is a recurring saved search that returns the value of an IT performance metric and is used to monitor the health of a service. The Content Pack for Microsoft 365 ships with 380 KPI’s, built using Microsoft best practices and Splunk research, some with configured thresholds and alerting rules.

- The M365 Service Analyzer provides a visual representation of your Microsoft 365 services and the dependencies between them. You can use this custom view to see the KPIs, entities, and most critical episodes associated with a service. Select an Microsoft 365 service in the dependency tree to investigate its associated KPIs and entities, and perform more granular root cause analysis of issues that arise. You can click View All to manage all critical and high episodes in Episode Review, or select an individual entity to view its health page.

- Episode Review provides a unified view of all your service-impacting episodes. You can drill down into individual episodes to perform more granular root cause analysis, such as viewing an events timeline or examining common fields. As an analyst, you can use Episode Review to gain insight into the severity of episodes occurring in your Microsoft 365 environment. Use the console to triage new episodes, assign episodes to analysts for review, and examine episode details for investigative leads.

**Use associations to visualize and troubleshoot various entities**

- Vital Metrics. The M365 Tenants entity type contains a set of vital metrics which describe the overall health of
entities of that type, including: Azure Active Users, Exchange Active Users, Microsoft Teams Active Users, OneDrive Active Users, SharePoint Active Users, and Yammer Active Users. You can view these metrics on the Entity Health page and drill down further into individual Exchange entities.

- Event Data Search Dashboard. The Event Data Search dashboard displays the 100 most recent log events associated with an entity for the last 60 minutes. The dashboard provides a high-level overview of entity performance across your whole environment, regardless of the entity type you associated with the entity.

- Entity Analytics Dashboard. The Entity Analytics dashboard lets you analyze metrics and logs for specific entities in Splunk ITSI. You can populate the dashboard with metrics and logs according to analysis data filters Splunk ITSI associates with a given entity.

---

Additional resources

The content in this use case comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed. These additional Splunk resources might help you understand and implement these recommendations:

- Splunk Docs: Overview of the glass table editor in Splunk ITSI
- Video: Microsoft 365 content pack for ITSI from Splunk
- Video: Getting started with ITSI glass tables