splunk>

FACT SHEET

Splunk® App for Microsoft® Exchange

End-to-end operational visibility and analytics for Microsoft Exchange-based email infrastructures

HIGHLIGHTS

- Real-time, service-centric visibility into health and performance across the entire messaging infrastructure
- Proactive end-to-end monitoring and correlation across diverse message delivery components and the supporting IT infrastructure
- Comprehensive operational analytics for resource planning, capacity forecasting, security intelligence and user behavior

Every organization's messaging infrastructure is mission critical. A disruption in email services means lost orders, impaired customer communications, decreased internal communications and can damage IT's, or even an entire organization's, reputation.

Datacenters are complex, with hundreds of technologies and devices layered together to deliver business services. Unfortunately the tools, platforms and components that comprise IT are all delivered in silos. IT operations teams consume valuable time and must use multiple toolsets to monitor and manage these environments. Tracking down issues and evaluating performance and availability are largely manual processes. Having immediate insight into the inner workings of your messaging infrastructure is crucial when problems arise.

The Splunk App for Microsoft Exchange

As an app that runs on the Splunk Enterprise platform, the Splunk App for Microsoft Exchange 3.0 delivers a fundamentally different approach for IT. The app provides insights from across the entire messaging infrastructure, including critical dependencies, such as the operating system, supporting applications, devices and services, resulting in a single, infrastructure-wide view of the entire environment. From that view, the app proactively highlights problem areas to help administrators resolve issues quickly, minimizing and avoiding service degradation and downtime.

By correlating performance, security and user event information, administrators can identify and resolve non-Exchange related issues that can impact the entire messaging service—for example, host OS information or processes that are causing downtime. This approach also allows you to view Exchange data in the context of all other ancillary message delivery components including load balancers, proxy servers, firewalls and more. This visibility provides a number of benefits like rapid root cause analysis and reduced support costs.

The Splunk App for Microsoft Exchange also includes out-of-the-box content for operational analytic needs, such as capacity monitoring, resource forecasting, user behavior tracking and security event identification. The app runs on the Splunk Enterprise platform, which enables you to collect any machine data to create customized dashboards, alerts and reports for your organization's unique analytic requirements.

The Splunk App for Microsoft Exchange helps you:

- Identify infrastructure problems, such as non-running services and load issues
- Monitor the performance of all servers throughout your messaging environment
- Track inbound and outbound messages throughout your messaging environment
- Correlate infrastructure health and performance issues with service response time or availability issues
- Gain end-to-end visibility across Exchange and non-Exchange related message delivery components, such as proxy servers, firewalls and more
- Monitor client usage, including mobility usage via ActiveSync
- Monitor security events such as anomalous logons and litigation holds
- Track administrative changes to the environment
- Analyze long-term mail operations trends
- Plan for capacity expansion
- Monitor your organization's outbound email sender reputation
- Use Splunk Enterprise to combine non-Exchange component, performance and operations data

Splunk App for Microsoft Exchange Features

Packaged Correlation—easily identify the relationships between service performance and health with security events using out-of-the-box dashboards and reports (see Figure 1).

Operations Dashboards—receive up-to-the-minute information on the health of your Exchange environment and the supporting infrastructure, such as Windows Server and Active Directory, including service availability, organizational reputation, performance data and administrative reports (see Figure 2).

Dashboard Builder—quickly and easily create, save and share custom reports of related services and components by simply querying on contextual information, such as logouts, performance, health and more (see Figure 3).

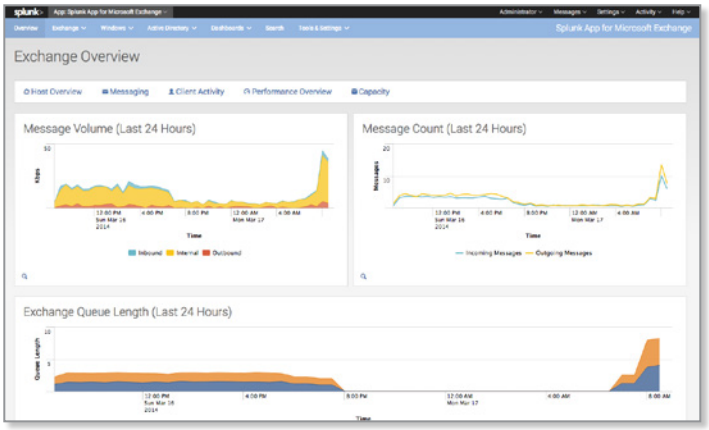

Figure 1: Receive visibility into how your system is being used.

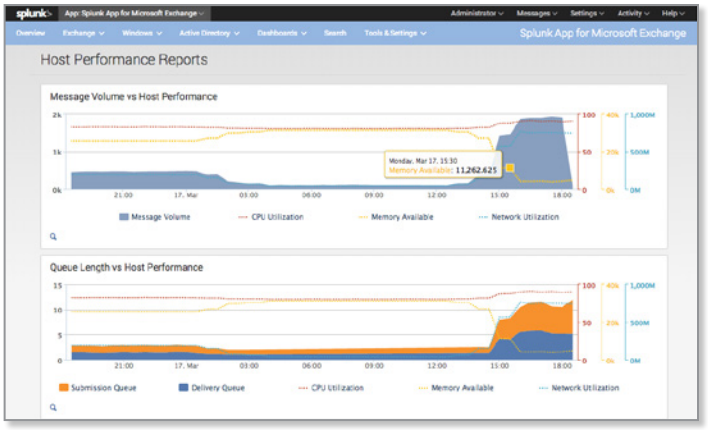

Figure 2: The operations dashboard delivers information on the health of your Exchange environment.

Messaging Activity—receive important segmentation and load information about message flow, allowing message tracking from the desktop to the gateway.

Client Behavior Monitoring—gain in-depth visibility into how the messaging service is being used. This includes the method of access (device or protocol), operating system, browser, location and mailbox usage statistics. By identifying user trends, administrators can identify potential issues or possible bottlenecks, and take proactive measures to prevent them.

Capacity Planning—provide metrics to proactively help you to plan for growth. Out-of-the-box dashboards cover messaging volume, the number of users your system is handling and full environment reports.

Enterprise Scale—scales to large email deployments, from organizations with a handful of users to full enterprises with hundreds of thousands of employees.

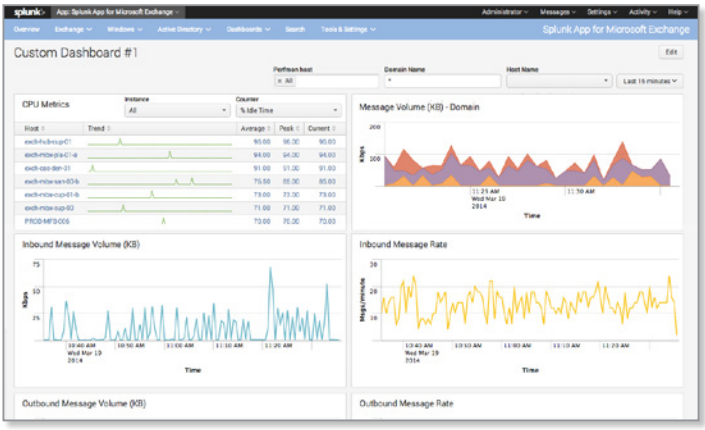

Figure 3: The dashboard builder provides custom reports on services.

Product Requirements

Supported Exchange Server Versions

- Exchange Server 2007 (requires Windows Server 2003 SP1 or Server 2003 R2 RTM or later)
- Exchange Server 2010 (requires Windows Server 2008 SP2 or Server 2008 R2 SP1 or later)
- Exchange Server 2013 (requires Windows Server 2012 RTM or later)

Splunk Requirements

- Splunk Enterprise 6.0 or later
- All Splunk indexers, search heads and universal forwarders require Splunk Enterprise version 6.0 or later
- The Splunk Add-on for Windows
- The Splunk Add-on for Active Directory (SA-LDAP Search)

OS Requirements

The Splunk App for Microsoft Exchange v3.0 and Splunk Enterprise instances can run on:

- Windows Server 2003/2003 R2, Server 2008/2008 R2 or Server 2012/2012 R2

You can also install the Splunk App for Microsoft Exchange on a non-Windows Splunk instance (e.g., Linux) to display Windows data coming from external Windows sources.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise 6 license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

A 60-day free trial of the Splunk App for MS Exchange is available at http://apps.splunk.com/app/1660/.

250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.apps.splunk.com

Item # FS-Splunk-AppMSExch-107