splunk>

SOLUTIONS GUIDE

Splunk® Enterprise™ for Windows®

End-to-End Real-time Visibility of Your Microsoft Windows Infrastructure

HIGHLIGHTS

- Monitor Microsoft Windows Server and key applications in real time
- Identify and resolve issues faster and greatly reduce costly escalations
- Monitor your heterogeneous Windows, Unix and Linux environment with a single, integrated console
- Deploy on an extendable platform that covers the full Microsoft infrastructure install base

Microsoft Windows environments are a complex but crucial component of an IT organization's infrastructure. When you add heterogeneous connectivity to Linux- and Unix-based systems and factor in virtualized and cloud-based instances, you have a mission-critical infrastructure that runs a business, yet poses a significant monitoring challenge. When one system fails, an entire service is impacted, resulting in alerts in multiple locations—with each alert acting alone. Each isolated system has a monitoring solution, creating a silo of management, with each silo having its own procedure and language. Problem resolution becomes a monumental task as IT departments analyze multiple silos to determine the root cause of an outage.

Product Overview

Splunk Enterprise is the platform for machine data. It collects, indexes and harnesses the machine data generated by all your Windows Server systems and Microsoft infrastructure—physical, virtual and in the cloud. Machine data is one of the fastest growing, most complex segments of data in your organization. It's also one of the most valuable, containing a definitive record of user transactions, customer behavior, machine behavior, security threats, fraudulent activity and more. Splunk Enterprise for Windows collects machine data securely and reliably from wherever it's generated. It stores and indexes the data in real time in a centralized location and protects it with role-based access controls. Splunk Enterprise lets you search, monitor, report and analyze your real-time and historical data. Now you have the ability to quickly visualize and share your data, no matter how unstructured, large or diverse it may be.

Troubleshoot application problems and investigate security incidents in minutes instead of hours or days, avoid service degradation or outages, deliver compliance at lower cost and gain new business insights. With Splunk Enterprise you can gain rapid visibility, real-time insights and intelligence for IT and the business. Use Splunk Enterprise software and monitor your entire Microsoft Windows infrastructure from one place in real time—from operating system environments to business-critical applications.

Splunk Enterprise Features for Microsoft Windows

Splunk Enterprise provides several specialized features to monitor Microsoft Windows data, including:

- **Windows Event Logs**: Monitor logs generated by the Windows Event Log service on any event log channel that is available on any Windows machine. Collect logs on the local machine, or gather log data remotely using the Splunk Universal Forwarder or WMI.
- **Performance monitoring**: Collect performance data on Windows machines with Splunk and then alert or report on that data. Any performance counter that is available in Performance Monitor is also available to Splunk. You can monitor performance locally or remotely through WMI or a universal forwarder.
- **Registry monitoring**: Monitor changes to the local Windows Registry using the built-in registry monitoring capabilities. You can use a universal forwarder to gather registry data from remote machines.
- **Active Directory monitoring**: Audit any changes to the Active Directory—including changes to user, group, machine and group policy objects.

Microsoft Windows Server Workload Monitoring Solutions

Splunk software is an enterprise platform that allows you to scale to meet the demands of the business. With supported App extensions that cover the full install base of a Windows Server infrastructure, Splunk Apps deliver a defined user experience with pre-built dashboards and views that extend the Splunk-for-Windows experience, delivering deeper insight to key workloads.

Infrastructure

The Splunk App for Windows provides pre-built data inputs, searches, reports, alerts and dashboards for Windows server

and desktop management that allow you to monitor, manage and troubleshoot Windows operating systems.

Messaging

The Splunk App for Microsoft Exchange consumes logs from your Microsoft Exchange systems to give you deep visibility into the health and performance of your Microsoft Exchange environment, from Edge and Hub Transport servers to the Client Access servers and the Mailbox Store itself.

Identity and Access

The Splunk App for Windows Server Active Directory gathers performance metrics, log files, and Powershell data from the domain controllers and DNS servers of a Microsoft Active Directory forest and its underlying infrastructure.

Virtualization

The Splunk App for VMware collects and harnesses data from the virtualization layer to enable true end-to-end visibility in virtualized environments.

Web Analytics

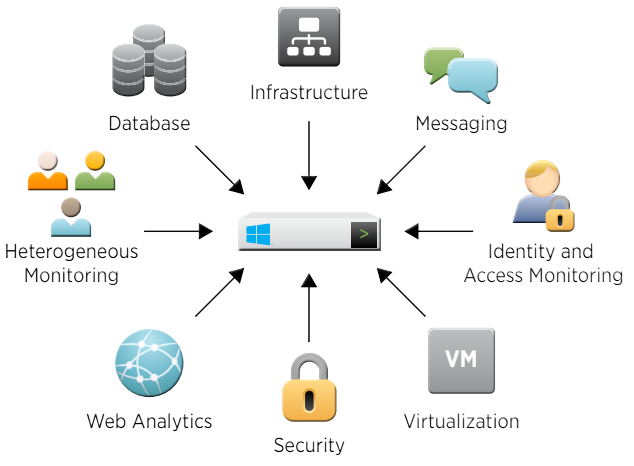
Splunk App for Web Intelligence provides insight into your web traffic for both IT and business users. Use it to track real-time visitor metrics, perform ad hoc analyses on your data and view historical trending and reporting.

Heterogeneous Management

The Splunk App for Unix and Linux provides pre-built data inputs, searches, reports, alerts and dashboards for Linux and Unix management that allow you to monitor, manage and troubleshoot *nix operating systems.

Database

Splunk DB Connect is a generic SQL database plugin for Splunk that allows you to easily integrate database information with Splunk queries and reports.



Splunk Enterprise on Windows Workloads

Splunk Apps are developed by and supported by Splunk. To extend the platform further, apps created by Splunk partners and the Splunk user community are available to extend Splunk on Windows further to deliver a complete end-to-end solution.

It's Software; Download it and Install it in Minutes. Splunk is enterprise software made easy. Try Splunk on your laptop and then deploy it to one or more datacenters. You're up and running with a web interface for users and a powerful engine for indexing your machine data.

Features	Splunk Free	Splunk Enterprise
Maximum indexing volume per day	500MB	Unlimited (based on license)
Universal, real-time indexing	•	•
Real-time and historical search	•	•
Reporting	•	•
Knowledge mapping	•	•
Dashboards	•	•
Monitoring and alerting		•
Distributed search		•
Data forwarding and receiving	•	•
Role-based access controls		•
Single sign-on		•
Developer APIs	•	•
Community Apps	•	•
Enterprise Apps		•
Standard support	•	
Enterprise support		•

Microsoft Partner
Gold Application Development

Free Download

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

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

Item # SG-Splunk-Windows-106