TRIPWIRE®
LOG CENTER

RECOMMENDED INSTALLATION SIZING

HARDWARE CONFIGURATIONS FOR SMALL, MEDIUM AND LARGE DEPLOYMENTS

CONFIGURATION	CPU	MEMORY	STORAGE	OS	DATABASE
Small	Dual processor/ Quad core	16GB	2x7200rpm local	Windows 2012 64-bit	Fewer than 500k events/ month, embedded PostgreSQL on the TLC Manager. 500k–1M events/month: MySQL or PostgreSQL, on dedicated DB server with minimum 10,000rpm drive. For >750k events/ month, Microsoft SQL Server on similarly-provisioned hardware is strongly recommended.
Medium	Quad processor/ Quad core	32GB	2x10,000rpm local	Windows 2012 64-bit	Similar to above, but due to the likelihood of exceeding the stated threshold, consider SQL Server or PostgreSQL from the outset. MySQL is sufficient only if the number of events remains lower than limits stated above.
Large	Quad processor/ Six cores	64GB	4x10,000rpm local	Windows 2012 64-bit	Similar to above, but due to high likelihood of exceeding the stated threshold, SQL is strongly recommended from the outset. MySQL is not recommend for this configuration.

TRIPWIRE LOG CENTER INSTALLATION DEPLOYMENT LEVELS

DEPLOYMENT LEVEL	APPLICATION
SINGLE: Single installation, no secondaries	Hundreds of assets, low number of assets (hundreds), low EPS (~500 sustained EPS) Average event size (~500 bytes for Windows; ~120 bytes for Syslog), minimal in-console work Designed to handle spikes arising from increased activity, "catch-up" spikes due to temporary network outages, etc., but still able to facilitate in-console work
INTERMEDIATE: Distributed installation	One primary manager handles "indexing" (aggregated data streams from secondaries), and limited in-console work Secondaries can be TLC-Small Intermediate number of assets (high 100s–mid 1,000s), intermediate EPS (sustained: in the low 1,000s; spikes into the mid 10,000s) Average event size (~500 bytes for Windows; ~120 bytes for Syslog), minimal in-console work Distributed install, designed to handle "spikes" arising from increased activity, "catch-up" spikes due to temporary network outages (more common in distributed environments), etc., but still able to facilitate some in-console work
ENTERPRISE: Large distributed installation	One primary manager using TLC-Large handles "indexing" (aggregated data streams from secondaries); second primary manager using TLC-Small limited in-console work, reports, etc. Secondaries can be TLC-Small. Intermediate number of assets (mid 1,000s), high EPS (sustained: in the high 1,000s; spikes into the mid 100,000s) Average event size (~500 bytes for Windows; ~120 bytes for Syslog) Distributed install, designed to handle "spikes" arising from increased activity, "catch-up" spikes due to temporary network outages (more common in distributed environments), etc., but still able to facilitate some in-console work

tripwire®

◆ Tripwire is a leading provider of endpoint detection and response, security, compliance and IT operation solutions for enterprises, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. Learn more at tripwire.com ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

©2016 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc.
All other product and company names are property of their respective owners. All rights reserved.

TLCSMX721a 201606