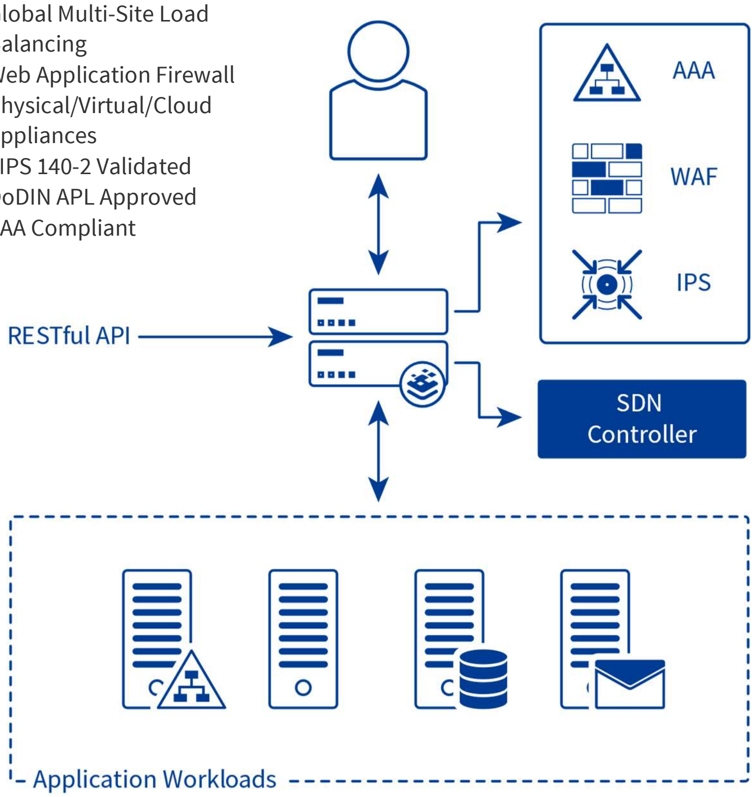
LoadMaster™ Appliances

- Advanced Application Load Balancing
- Global Multi-Site Load Balancing
- Web Application Firewall
- Physical/Virtual/Cloud Appliances
- FIPS 140-2 Validated
- DoDIN APL Approved
- TAA Compliant



Kemp LoadMaster™ is an advanced Layer 4-7 load balancing and content switching application delivery controller (ADC) available as physical, virtual or cloud appliances, providing advanced software optimization and enterprise application integration, allowing intelligent and efficient distribution of traffic to deliver the best Application Experience (AX™) for your users.

LoadMaster™ is an essential component to include for the high availability of critical application infrastructures in the modern datacenter with active/passive failover and global server load balancing for multi-site deployments.

Combining the latest advancements in Layer 4- 7 application delivery technology with support for high-performance hardware and virtualization platforms, the LoadMaster™ is the load balancer of choice for providing high availability services in web, application and cloud infrastructures.

Kemp LoadMaster™ Operating System (LMOS) is approved for use on the DoDIN-APL under Cyber Security Tools.

Investment Protection

- A single LoadMaster™ can support up to 1,000 servers, offering scalability for growing environments.
- Time-tested software optimized to take advantage of the underlying platform.
- Advanced application delivery and security optimization features like content switching, web application firewall, caching, edge security, data compression, intrusion prevention and TLS (SSL) termination provide all of the functionality needed in virtualized application infrastructures.
- Native support for enterprise applications such as Microsoft® Exchange, Skype for Business, SharePoint, SAP® and Oracle® Enterprise Business server.

Cost Containment

- With competitive pricing and unbeatable performance to cost ratio, LoadMaster™ allows for shortened realization of ROI.
- Key functionality included in every LoadMaster’s base price provides the most comprehensive feature set in the industry –further lowering TCO.
- With low overhead for training, administration and setup, LoadMaster allows for the quickest time to production for line of business and corporate wide applications and web services.

Ease of Use

- All LoadMasters come with an intuitive and simple to use Web User Interface (WUI) and CLI, enabling administrators to easily configure, maintain and integrate LoadMaster™.
- Easily orchestrate operation with VMware vRealize Orchestration and Microsoft System Center VMM.
- Wizard-driven setup and optimized configuration templates simplifies deployment in existing traditional datacenter and hybrid cloud infrastructures.
- Secure SSH and HTTPS WUI remote access, real time performance and availability metrics, SNMP support allows LoadMaster™ and the applications it supports to be easily managed and monitored.

FIPS 140-2

What is FIPS 140-2

FIPS 140-2 is the mandatory standard associated with encryption of unclassified information. There are two basic approaches to achieving compliance with FIPS 140-2, all require the use of National Institute of Standards and Technology (NIST) certified encryption modules. FIPS 140-2 Level 1 can be achieved by incorporating a software based certified encryption module. FIPS 104-2 Level 2 can be achieved by incorporating a hardware based certified encryption module. FIPS 140-2 includes three key processes, private key creation/storage, digital signature, and encryption.

Is FIPS 140-2 required?

Load Balancers/Application Delivery Controllers (ADCs) are used to securely connect users to applications using Secure Socket Layer (SSL) or Transport Layer Security (TLS). SSL/TLS is an encryption process for protecting data in motion. To meet federal mandates, SSL/TLS must use NIST certified FIPS 140-2 cryptography. ADCs typically terminate the incoming SSL/TLS connection from the user and create the SSL/TLS connection to the application server.

Legal Basis.

Federal Information Processing Standards (FIPS) are mandated under US Public Law (100-235 and 104-106).

The US Federal Information Security Management Act of 2002 eliminated any agencies ability to waive mandatory Federal Information Processing Standards.
US Department of Defense National Security Telecommunications Information Systems Security Policy (NSTISSP) # 11 is an acquisition policy that must be complied with prior to the purchase of information technology (IT) for DoD. NSTISSP #11 mandates FIPS 140-2 for all systems that encrypt DoD unclassified information.

Network-Attached Hardware Security Module (HSM)

FIPS 140-2 network-attached HSMs provide for secure creation/storage of private keys associated with certificates. Network-Attached HSMs use secure connections to the ADC to share private key information needed for the ADC to establish SSL/TLS connections. ADCs create/terminate SSL/TLS connections from the user to the application server. The cryptography used by the ADC to encrypt these connections must be FIPS 140-2 certified. Network-Attached HSMs can improve upon a FIPS 140-2 compliant system by providing a single point to manage certificates. Network-Attached HSMs cannot make a non-FIPS system compliant to FIPS 140-2.

Kemp and FIPS.

Kemp LoadMaster Operating System (LMOS) is used in all Kemp appliances (physical/virtual/cloud).
LoadMaster Operating System (LMOS) 7.2 is FIPS 140-2 Leve 1 validated.
https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2473

Select Kemp LoadMasters include FIPS 140-2 Level 2 certified encryption.
https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2316

Kemp LoadMaster can interface with FIPS 140-2 certified network-attached HSM.

For further information please contact us at federal@kemp.ax.