Improving Distributed Analytics and Private Cloud Through Enhanced Networking

October 2016

All questions and enquiries regarding this white paper should be directed to:

Dan Cybulski
CTO
dan@cognitiocorp.com

Background and Objectives

Every agency buys computational capacity to enable its mission objectives. Servers provide these agencies with the computational horsepower needed to tackle todays complicated national security and intelligence problem sets. Unfortunately, the commoditization of the server market has led to decision makers focusing solely on components (such as CPU's, memory, and disks) when developing the specifications for new server procurements. Other system components are viewed as being commoditized or standardized to the point that they lack performance or feature differentiation. This is particularly true with regard to network adapters, where little attention is paid beyond the advertised bandwidth (1/10/25/50/40/100 Gbps) and connection medium (Fiber, Copper, etc.).

"The parallel and distributed nature of today's applications and datacenters puts tremendous importance on a servers networking components."

In contrast, the parallel (multi-core) and distributed (multi-server/multi-location) nature of today's applications and data centers puts tremendous importance on a server's networking components. Whether servers are used to implement a private cloud infrastructure or deliver bespoke mission capabilities, maximizing performance and scalability while minimizing latency is key. Data must be rapidly, securely, and seamlessly moved in and out of servers for efficient processing and analysis to deliver rapid results to end-users. Likewise, systems must minimize the latency that they introduce into communications channels to avoid impacting mission performance and application usability.

This paper will illustrate how choosing Solarflare® network adapters when buying servers can immediately enhance the performance of mission systems and applications. Moreover, this paper will highlight the unique functionality enabled by Solarflare adapters when combined with configurable software to accelerate, monitor, and secure mission systems.

Value to Mission

Solarflare's industry leading adapter technology and software solutions enable mission systems to keep pace with the increased demands of modern computational architectures and evolving analytic workloads through:

Native Performance Enhancement

Solarflare's ASIC technology and OS bypass architecture provide a native performance boost without the need for added software or modification to existing applications.

Cost Effectiveness

Factory supported Solarflare adapters provide superior performance and enhanced capabilities as a cost neutral alternative to standard OEM 1/10/40GbE adapters.

Enhanced Functionality

Solarflare adapters enable a suite of industry leading capabilities to enhance the performance and security of mission systems while maintaining full application compatibility.

Commoditization of the Network

Federal agencies are some of the largest purchasers of IT services and equipment. Today the U.S. federal government represents the largest single vertical market for IT expenditures. Agencies have historically used this purchasing power to drive the product roadmaps and innovation programs at OEMs to create products and technologies to help them meet unique mission objectives. This, in part, has led to the vast array of options available when purchasing server hardware.

As with most things, choice is good. Having this wide range of hardware options allow agencies to specifically tailor their purchases to meet mission requirements. When purchasing server hardware, it is important to carefully consider its intended use in order to ensure that a machine has the proper components and configuration to support a given workload. For instance, some applications are highly parallel or memory intensive, requiring that system specifications focus on core count and memory density. Meanwhile, others might benefit more from higher clock speeds, optimized bus architectures, or localized high speed storage.

"the capabilities of the network adapter have a significant impact on the performance, reliability, and security of a deployed resource"

Despite the intricacies of developing hardware specifications to meet specific workload demands there is one common thread, the network adapter. More often than not network adapters are viewed as an undifferentiated component leading purchasers to select the lowest cost adapter while considering only the adapters raw bandwidth (1/10/25/50/40/100 GbE). However, the distributed and service oriented nature of today's network intensive applications and compute frameworks, coupled with increased security requirements, has magnified the significance of the network adapters role. Whether connecting

to an internal LAN, a corporate WAN, or a commodity cloud fabric, the capabilities of the network adapter have a significant impact on the performance, reliability, and security of a deployed resource.

This is particularly true in today's public and private cloud infrastructure where general purpose servers support a wide range of virtualized systems and containerized applications. In this case the network adapter plays a critical role in enabling the performance and reliability of these workloads. More advanced adapters, like those from Solarflare, provide added functionality, beyond raw performance, to enable the seamless management and security of systems at scale. Simply selecting a Solarflare adapter while building out the specifications for a new system will provide agencies with industry leading performance and security capabilities while also enabling a wide range of enhanced capabilities.

Enhancing Performance and Security

With limited on-adapter intelligence, most current network adapters serve to simply move network packets between the operating system and the communications medium. While this is certainly a core function of a network adapter, there are several major drawbacks to this approach, particularly when dealing with data-intensive scale-out workloads. First, this approach increases the load on the host processor, as it must look at all incoming traffic to determine if it is intended for one of its processes. It must also perform any required filtering and inspection of the traffic for security reasons. Second, this approach requires that all traffic, even potentially malicious traffic, be delivered to the host operating system for inspection and filtering. By indiscriminately delivering packets, the adapter may open the door for malicious traffic to bypass host-based security tools.

Solarflare's suite of application-intelligent networking solutions address these issues through a unique combination of advanced hardware and software capabilities. The Solarflare adapter design implements a OS bypass architecture to drive higher throughput and lower latency. It is capable of accelerating the performance of native applications while its use of custom ASICs (Application Specific Integrated Circuit) and FPGAs (Field Programmable Gate Array) enable a wide range of both on adapter and software driven capabilities to monitor and secure agency networks. For instance, Solarflare adapters provide inline packet filtering capabilities through the SolarSecure Filter Engine. The Filter Engine can provide up to a 10x improvement in server performance over host based alternatives like iptables. Once filtered, the adapters provide hardware assisted distribution of traffic directly to the application, via the Onload™ capability, to ensure efficient use of CPU cycles.

Technical Approach

Solarflare's network platforms are differentiated by its unique combination of hardware and software expertise. As both the designer of the hardware and creator of the software, Solarflare is able to deliver the most tightly integrated networking capability in the industry. Nowhere is this more evident than in the creation of the ASICs in its Flareon® server adapters.

The current generation of Solarflare ASIC technology provides five key functions capable of driving

enhanced mission capabilities:

High Performance

The PCIe Gen 3.1 host interface provides a full 16 lanes to support bidirectional performance on multiple 40GbE interfaces.

CPU Offloading

Hardware based TCP segmentation and reassembly offloads, VLAN, VxLAN and OVS offloads.

Flow Processing

Dedicated parsing, filtering, traffic shaping and flow steering engines can operate flexibly and with an optimal combination of a full hardware data plane with software based control plane.

Switching

A hardware switch fabric on the silicon, provides the ability to steer flows based on the Layer2 level protocol between physical and virtual interfaces. The switch fabric also fully supports a software defined network control plane with DCB/PCI-IOV virtualization acceleration for high performance operating systems and virtual appliances via physical or virtual functions.

High-precision Timestamping

A fully integrated timestamp unit on the ASIC can be used to generate high-precision hardware timestamps both as packet meta-data and inserted into frame data.

Together with Solarflare's software solutions, these hardware functions serve to enable countless implementation scenarios that will enhance the performance, monitoring, and securing of mission systems. For instance, the Flareon adapter coupled with the Onload software solution has been shown to provide up to a 3x performance improvement for distributed in-memory workloads. This enhancement is driven by the native high performance of the Flareon ASIC along with Onload's kernel bypass capabilities which allows data to be passed directly from the adapter to user-space applications, eliminating the need for a costly context switch.

Enhancing Mission Capabilities

In addition to the out-of-the-box performance and security enhancements that Solarflare adapters provide, Solarflare's software solutions open the door for agencies to implement a wide range of capabilities to enhance the monitoring, security, and overall capabilities of their networks.

Distributed, Active Security

SolarSecure Domain Fortress™ is designed to centrally manage all the on-adapter hardware traffic filtering capabilities of every Solarflare NIC within every server in your agency. It can then enforce a very strict white-list access that could be unique for every server, while using a simple graphical security policy management system. SolarSecure Domain Fortress also includes a learning mode to detect and alert on new network traffic flows entering and leaving the server. It can be deployed to create a fully distributed security solution focused on the target of most attacks – the servers.

High Fidelity Capture and Replay

Capture SolarSystem is like a network DVR for your agency, it can be deployed to provide agencies with the ability to precisely capture, query, and replay network traffic on even the highest speed networks.

Real-time Analysis at the Edge

ApplicationOnload® Engine provides agencies with the ability to run custom on-adapter applications to provide true real-time analysis and alerting capabilities on edge systems.

Application Acceleration

Onload is an open source application accelerator supported by Solarflare adapters to deliver predictable latency and high message rates for the most network intensive workloads including distributed in-memory applications. Solarflare has also made available an open source DPDK driver.

Summary

It has been said that latency breeds contempt, this is especially true in the defense and intelligence communities where seconds can be the difference between life and death. To keep pace with rapidly evolving mission demands, agencies are constantly advancing their capabilities in the areas of distributed analytics and private cloud. Today, agency compute infrastructures rely on networking, not only for the delivery of content to end users, but increasingly for the distributed real-time processing of mission critical data. However, the server market, once dominated by differentiated offerings from a myriad of OEMs, has been commoditized by the adoption of virtualization and cloud computing technologies and services. While this commoditization has led to countless new analytic capabilities, it has also shifted the focus away from the hardware components and onto the software stack which has, in turn, created inefficiencies in both the overall performance and security of deployed systems.

"The inefficient performance of network adapters can overwhelm host CPU's, creating bottlenecks that starve systems of data…"

The network has evolved to become one of the most critical components of any individual system or distributed application. The inefficient performance of network adapters can overwhelm host CPU's, creating bottlenecks that starve systems of data and diminish workload performance. Moreover, the reliance on Operating System (OS) or kernel level security exposes systems to countless network based cyber-attacks. These may include zero-day attacks which target unknown OS and kernel level software vulnerabilities. Solarflare's suite of direct and OEM available application-intelligent networking hardware and software can be deployed to help agencies eliminate these performance bottlenecks and optimize the security of deployed resources. Solarflare's unique blend of on adapter processing capabilities and host-based software make it easy for agencies to accelerate native cloud and analytics workloads, while also enabling a wide range of network monitoring and security capabilities to enhance the resilience of their critical mission systems.