WHITE PAPER

Enhance ArcSight 6.0 ESM Security with Fusion ioMemory™ Solutions Performance Density and High Throughput

SanDisk®
a Western Digital brand

Western Digital Technologies, Inc.
951 SanDisk Drive, Milpitas, CA 95035

www.SanDisk.com

Introduction

The HP ArcSight Security Intelligence platform is the industry's leading security information and event management (SIEM) solution for collecting, analyzing and assessing security events. ArcSight ESM sifts through millions of log records, and correlates them to find the critical events that matter, in real time. It transforms this data into actionable information, presenting it in dashboards, notifications, and reports so users can accurately prioritize security risks and compliance violations. In previous versions of the ArcSight software, as event-ingest volumes increased, write-heavy workloads slowed event correlation. Many organizations, including the US Internal Revenue Service (IRS), deploy a Fusion ioMemory-based system architecture to eliminate underlying I/O bottlenecks that can adversely impact ArcSight event correlation database processing and to dramatically improve performance.

Acting as a persistent memory tier operating at near-DRAM speeds in the server, Fusion ioMemory products are available in capacities from 365GB to 10TB and have been architected to ensure high reliability and endurance with linear performance scalability.

HP's highly-anticipated ArcSight ESM 6.0 release includes enhancements that make a joint ArcSight and Fusion ioMemory solution even more powerful. ESM 6.0 replaces the Oracle database that powered ArcSight ESM with HP's own CORR- engine. Joint ArcSight ESM 6.0 and Fusion ioMemory solutions can analyze much more data, much faster, on much less infrastructure, as compared to hard disk-based solutions, while also reducing capital and operating costs. Systems that implement this solution can achieve the following benefits:

- Up to 5X faster event correlation operations using the same hardware
- Up to 10X more capacity for event analysis resulting from a new database compression feature
- Up to 2X faster event correlation performance over previous ArcSight solutions

This gives ArcSight customers more security capabilities and the ability to detect more incidents and analyze more data in the same footprint and in much less time.

Optimal ArcSight Performance

Organizations can achieve maximum throughput on the smallest server footprint by moving the entire database onto Fusion ioMemory products deployed in the host server. Because all data is sourced from Fusion ioMemory rather than from slower rotating media such as disk drives, this configuration offers the highest possible events-per-second. Multiple Fusion ioMemory products can be aggregated together for a larger single volume of up to 40TB of capacity per server.

Example Solution Configuration

Full Database on Fusion ioMemory

Configuration

- Host entire database on Fusion ioMemory products
- Use Fusion ioMemory instead of disks

Advantages

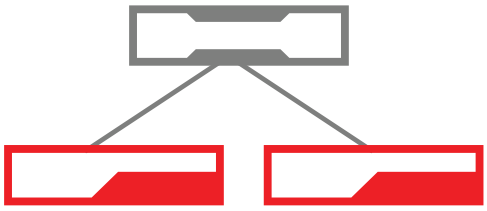
- Maximizes event, IOPS and throughput performance
- Much lower cost in infrastucture, operation, power consumption, and cooling than hard disk-based solutions
- Simpler installation and maintenance procedures

Maximizing Performance For Very Large Data Sets

If your data set is too large to fit within a single server, you can achieve similar performance improvements by deploying a shared storage node built with SanDisk ION Accelerator™ software and Fusion ioMemory products configured in a single SanDisk ION Accelerator appliance. Any number of these SanDisk ION Accelerator shared storage nodes can be connected to a single ArcSight database server. The database can then be portioned to take advantage of this additional high-performance shared flash storage capacity.

ION Shared Storage Node Configuration

HP ArcSight ESM



SanDisk ION Accelerator™

Configuration

- Connect all-flash SanDisk ION Accelerator shared storage nodes to the ArcSight database server

Advantages

- Similar in-server performance from shared storage nodes
- Ability to achieve high-availability between SanDisk ION Accelerator shared storage nodes
- Ability to scale beyond the flash capacity of a single server without requiring slow, hard-drive based shared storage

US IRS Case Study

With the previous version of ArcSight, customers typically achieved approximately 35,000 events per second. With ArcSight 6.0, customers are able to double the performance of Fusion ioMemory-based systems and achieve an order of magnitude (10X) improvement over the performance of hard disk based systems.

The US Internal Revenue Service (IRS) recently tested ArcSight 6.0 on an HP DL580 G7 server configured with four Fusion ioMemory 2.4TB ioDrive®2 Duo cards. Using Bleep, ArcSight's built-in performance tool, the IRS achieved up to 70,000 events per second with a base install. After disabling default content, they averaged 109,000 events per second with peak performance at 135,000 events per second. When asked about impact on user experience, the IRS engineer said, "Running Fusion ioMemory solutions and the ArcSight CORR database, our query times have gone from over 30 minutes to under 30 seconds."

Best Practices

1. For maximum performance, place the entire database, including logs onto Fusion ioMemory products, either within the server or using the ION Accelerator shared storage node option.

2. When working with large datasets that cannot fit within a single server, utilize one or more ION shared storage nodes.

Summary

HP ArcSight ESM 6.0 and Fusion ioMemory joint solutions enable organizations to create simple ArcSight systems that deliver consistent high-performance, low-latency responses—even as ingest load increases. Fusion ioMemory products integrate directly with the host server, providing cost-effective high-performance capacity operating at near-DRAM speeds for active data. Combining Fusion ioMemory solutions with ArcSight ESM 6.0 results in a faster, more resilient, and simpler system that dramatically improves ArcSight performance.

FOR MORE INFORMATION

Contact a SanDisk® representative, 1-800-578-6007 or fusion-sales@sandisk.com

The performance results discussed herein are based on testing and use of the described products. Results and performance may vary according to configurations and systems, including drive capacity, system architecture and applications.