White Paper

A modern approach to data center SAN

Optimizing performance, security, and cost

NetApp authors: Steve Collins, Mike Hommer, Alan Kravitz, Artie Noel, Troy Presler, Rusty Young

Broadcom Authors: Jason Massae, Naem Saafein, Jim Zucchero

July 2024 | WP-7369

In partnership with

Abstract

This paper presents a compelling case for the modernization and optimization of SAN architecture using NetApp® ASA C-Series arrays with capacity flash, Brocade Fibre Channel switches, Emulex HBAs, and VMware vSphere 8. These technologies, when deployed with mission-critical database workloads, create a future-proof environment that strikes the optimal balance among performance, cyber resilience, and cost.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Executive summary

Data is the lifeblood of future-thinking companies. The consequence of increasing reliance on data will be a never-ending expansion in the size of the global datasphere, which, according to IDC forecasts, is anticipated to grow to 181ZB to by 2025,[1] skyrocketing to 291ZB by 2027.[2] As enterprises navigate the complexities of data management in a digital-first world, they are confronted with the challenge of optimizing performance, ensuring cyber resilience, and managing costs effectively. This white paper explores how NetApp storage, Brocade SAN switches, and the VMware by Broadcom hypervisor can be jointly leveraged to address these challenges.

Performance optimization through the integration of NetApp® ASA C-Series arrays, Brocade SAN switches, and the VMware vSphere 8 hypervisor offers a robust solution for organizations seeking to enhance the performance of their IT infrastructure. The synergy between NetApp's all-flash storage, Brocade's high-speed networking, and VMware's resource management capabilities help applications run efficiently, with high throughput and low latency. Lab tests with Oracle and Microsoft SQL Server workloads have demonstrated consistent performance with response times within the 2–3ms range under various conditions, showcasing the system's ability to handle demanding workloads.

Cyber resilience is a critical aspect of modern IT infrastructure. NetApp's commitment to security certification, along with the Commercial Solutions for Classified (CSfC) validation of NetApp ONTAP®, provides a secure storage platform. Brocade's SAN products bolster this with a suite of authentication and encryption features that protect data and network fabrics from unauthorized access. The combined solution offers a multilayered defense strategy that enhances the overall security posture of the organization.

Cost optimization in IT infrastructure is a multifaceted challenge that requires balancing performance and security without overspending. The NetApp Storage Design Workshop aids businesses in understanding the complexities of cost by considering virtual computing, flash storage solutions, and cloud technologies. By adopting a service design approach, IT can align technology with business objectives, offering predictable services with measurable costs. With this approach, IT infrastructure can meet the demands of the digital economy while maintaining cost effectiveness and operational efficiency.

The combination of NetApp storage, Brocade SAN switches, and the VMware by Broadcom hypervisor presents a compelling solution for organizations looking to modernize their IT infrastructure with an eye on performance, security, and cost. The designs and configurations discussed provide a framework for enterprises to adapt to their unique requirements, so that they are well positioned to face the challenges of today's data-intensive landscape.

---

[1] Statista, Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025, 2024.
[2] John Rydning, Worldwide IDC Global DataSphere Forecast, 2023-2027, IDC, April 2023.

Introduction

In the evolving landscape of data management, organizations face increasing challenges in managing capacity-intensive, business-critical workloads such as databases, VMware environments, and backup and recovery systems. The high-level goal of IT is to provide resources to support an application. Applications are the lifeblood of any organization, and they're used to view, modify, correlate, and ultimately make decisions on data. Historically, the main challenge was finding a balance between performance and cost. More recently, there has been an added challenge of making sure environments are secure and protected against threats such as ransomware. Fortunately, recent developments in technology have allowed these three components—security, performance, and cost—to effectively be balanced without significant compromise on any of them.

This white paper describes how the components of NetApp storage, Brocade SAN switches, and the VMware by Broadcom hypervisor can be leveraged in various designs to support a range of business and workloads. These designs are based on lab-tested configurations combined with NetApp, Brocade, and VMware tools and best practices. They are intended to show the art of the possible backed by lab results and TCO analysis.

This white paper is not intended to be the final authority on architecture. Every environment has its own unique features and needs. Additionally, there are thousands of other "what ifs" and variables that will force adjustments and modifications to the designs presented here. However, as a framework for the broader discussion on cost, scale, performance, and security, these designs are well suited for the relative comparison presented. They open conversation points and considerations that customers should investigate as they look to modernize and update their infrastructures.

NetApp value

NetApp ASA systems deliver modern solutions to your SAN infrastructure. They enable you to accelerate your business-critical applications, keep your data available, and simplify your operations. ASA systems are built on the proven NetApp A-Series family of products and include NetApp ASA C-Series capacity flash models used in these reference architectures. They are optimized for cost-effective, large-capacity deployments.

The ASA systems are part of NetApp's full portfolio of storage systems, including submillisecond-performing NetApp AFF and hybrid FAS unified storage arrays. NetApp's Storage Design Workshop aligns application performance requirements with business needs, and organizations can optimize their storage infrastructure and operations with NetApp ONTAP powering all their storage, from SAN to NAS to cloud.

The need for dedicated, high-performance block storage solutions that can handle these demands without compromising on cost, performance, or security is more crucial than ever. The NetApp ASA C-Series provides sophisticated solutions tailored to these demands for most Fibre Channel (FC) workloads.

Designed for enterprises that require secure, dependable block storage, the ASA C-Series offers a resilient and flexible architecture that is cost effective for handling dense workloads and aligns with the strategic needs of modern IT infrastructure. Notably, the ASA C-Series stands out for its financial viability, and it uses advanced all-flash, all-NVMe technology to enhance performance.

ASA C-Series systems are characterized by high reliability with six-nines availability, leading storage efficiency, and robust cybersecurity measures, including tamperproof NetApp Snapshot™ copies. They support comprehensive disaster recovery capabilities and cloud connectivity, and they use NetApp ONTAP software for streamlined storage management. This integration facilitates a more sustainable and secure storage environment that significantly reduces TCO and decreases power consumption.

Organizations looking to optimize their storage without compromising on performance will find the ASA C-Series to be a pivotal resource. This white paper explores how the ASA C-Series not only addresses immediate storage challenges but also supports scalable, future-proof growth and operational efficiency.

Brocade value

Broadcom's Brocade has been the leading provider of storage networking solutions worldwide for more than 20 years, supporting the mission-critical systems and business-critical applications of most large enterprises. Brocade supports the high-end network infrastructure requirements and demands of today's workloads. As datasets for AI, databases, and other critical workloads continue to grow, Brocade offers industry-leading network reliability, scalability, and security to support tomorrow's most demanding workloads.

Brocade's expertise in high-performance switching and NetApp's latest generation of storage arrays and management software expertise combine to deliver compelling solution sets. Brocade FC SAN fabrics provide industry-leading high availability and reliability that enable organizations to reliably run critical workloads with a maximum throughput across all network connections in the absence of a failure.

Brocade's latest FC infrastructure, Gen 7, also unleashes performance with reduced latency and increased bandwidth. In addition, Brocade fabrics offer integrated intelligence and automation that are built on analytics and telemetry data to further simplify and optimize the environment. This infrastructure lays the foundation for an autonomous SAN by combining powerful analytics and advanced automation capabilities to maximize performance and ensure reliability.

Broadcom's Gen 7 64Gbps FC switching platforms, which feature the industry's most advanced switching ASIC, revolutionize SAN technology. Compared with Gen 6, the Gen 7 technology provides 50% lower latency (460-ns latency) and twice the bandwidth for critical workloads, fabricwide latency monitoring, 50% more buffers per ASIC for distance support and congestion management, and increased encryption and compression capacity. The Gen 7 platforms deliver unparalleled data center infrastructure security and resilience. The Brocade SAN offers the highest port-density platforms, allowing consolidated device connectivity, reduced capital expenditures, and lower operational costs. With a total system bandwidth of up to 39.6TBps, Brocade's switches and routers are equipped to handle modern workloads. Moreover, the integration of powerful analytics software enables a cyber-resilient network, protecting against cyberattacks and disruptions while optimizing performance and reducing TCO through comprehensive visibility, automated processes, and actionable insights. Upgrading to the high-density Brocade Gen 7 64G platforms ensures data security, simplifies management, reduces opex, and optimizes performance, yielding long-term benefits.

Emulex value

High-speed networking technology is a critical element for achieving maximum systemwide performance. FC is purpose-built for storage networks, meeting the requirements for high availability, scalability, predictable performance, and low latency. Compared to the previous generation, Emulex FC host bus adapters (HBAs) offer up to 2 times higher bandwidth, 3 times better latency, enhanced security, and operational efficiency for 64GFC and 32GFC SANs aligned to NetApp's new A-Series and ASA C-Series systems, respectively. Emulex fully supports new industry standards such as fabric performance impact notifications (FPINs), including link integrity notification (FPIN-LI), congestion notification (FPIN-CN), peer congestion notification (FPIN-PN), and delivery notification (FPIN-DN). The Emulex SAN Manager application, a free, easy-to-use solution, is the first application in the industry that uses the FPIN-CN standard to automatically identify, minimize, and mitigate application performance problems caused by SAN congestion.

The Emulex Dynamic Multi-core Architecture delivers unparalleled performance and the most efficient port utilization with 8 processing cores and 16 threads that dynamically apply ASIC resources to any port that requires them, ensuring that SLAs are met. The LPe35000-series delivers 12800MBps (two 32GFC ports) or 25600MBps (two 64GFC ports) full duplex, provides 3 times better hardware latency, and

supports an industry-leading IOPS rate of up to 10 million.[3] The fastpath design provides hardware acceleration for Emulex Dynamic Multi-core Architecture, reducing latency for each transaction by processing I/O requests in hardware, thereby operating significantly faster than software-based solutions. These performance advances enable Emulex Gen 7 HBAs to handle demanding workloads and peak-workload I/O spikes like no other FC HBA in the industry.

NetApp and Broadcom have been providing joint technology solutions for customers for several decades. NetApp is an OEM partner of Brocade and has provided SAN solutions since 2002. Our joint customers have continued to invest in, use, and depend on these solutions to meet their most demanding business-critical large-scale workloads.

VMware value

VMware vSphere 8 is a next-generation infrastructure virtualization platform that assists customers in modernizing and optimizing their VMware environments. It delivers enhanced performance, scalability, and security features that enable businesses to run complex applications efficiently. With its artificial intelligence and machine learning (AI/ML) capabilities, vSphere 8 provides smarter resource management, ensuring that workloads are optimally distributed and balanced across the estate. Additionally, it offers simplified lifecycle management and a unified platform for both traditional and containerized applications, facilitating a seamless transition to a modern, hybrid cloud architecture. This ensures that customers can leverage the latest innovations in virtualization to drive their digital transformation initiatives while maximizing their existing VMware investments.

These numerous features and enhancements added for scale, resilience, and security are why customers should run the latest updates. Fixing issues that might crop up with system stability, confidentiality, integrity, or availability is essential to a secure and stable environment. Some of these fixes are disclosed publicly, but some are improvements made quietly inside the products as a response to changing security threats. A good example is improving the “out of box” system defaults for security, which helps customers be secure without additional staff and time expenditures.

Beyond performance and security, there are other great reasons to use the latest packages from VMware including VMware Cloud Foundation (VCF) or VMware vSphere Foundation (VVF). New versions contain performance enhancements, support for hardware performance-enhancing capabilities, updates to storage hardware drivers, or new hardware support, including in-box drivers. Another example is support for new CPUs from AMD and Intel, as well as the feature sets available in those CPUs to power AI workloads.

By staying current with patches and upgrading to the latest version whenever possible, you take a proactive stance in ensuring a secure and resilient storage environment. Remaining current with your software is crucial, because it not only enhances your system’s security but also contributes to its overall resilience and performance.

[3] Tolly Enterprises, Emulex Gen 7 LPe36002 Host Bus Adapter, test report #221123, May 2021.

Example architectures

The setup of these components is straightforward. The configuration examples are meant as general guidance for various scaling options; they are not the only configurations supported. All components can be tuned to meet specific business and application requirements.

These example architectures include the following key NetApp, VMware, and Broadcom technologies:

- Cost-optimized NetApp ASA C-Series arrays with capacity flash storage and 32Gb FC
- Brocade sixth (32Gb FC) and seventh (64Gb FC) generation host and fabric technology
- Emulex LPe36000/35000-series Fibre Channel HBAs
- VMware vSphere 8 hypervisor

Independently, each of these technologies will improve the data center, but when combined, the additive benefits provide game-changing performance benefits with end-to-end visibility. For all environments, the gains with VMware vSphere 8 are universal.

Upgrading to VMware vSphere 8 offers several compelling advantages, including enhanced security features such as encrypted vMotion and Virtual Machine Encryption, providing a more robust defense against evolving cyberthreats. Additionally, vSphere 8 introduces improved performance and scalability, enabling organizations to efficiently manage larger workloads and scale their virtual environments as needed. With features like vSphere Lifecycle Manager, the upgrade process becomes streamlined, reducing downtime and simplifying management tasks. Overall, migrating to vSphere 8 ensures greater agility, security, and efficiency for your virtual infrastructure, empowering your organization to meet the demands of modern IT environments effectively.

Small architecture

For smaller environments or workloads, the NetApp ASA C250 array and Brocade G610 are a great combination. This pairing can easily support a minimal best practice three-server vSphere cluster with a few hundred virtual machines (VMs), and allows room to grow—either by adding more architecture pods, or adding more servers—and capacity and scale-out as needed on demand.

The ASA C250 system features four onboard 16Gb FC ports per controller with two expansion slots for 4-port 32Gb FC cards. On the capacity side, it can start with as few as 8 15TB SSD drives, 65.9TiB usable (122TB raw). It can grow to 24 drives internal plus an additional 24-drive expansion shelf for a maximum raw capacity of 570TiB usable (734TB raw) when using 15TB drives or 1.11PiB usable (1.47 raw) with 30TB drives.

The Brocade G610 industry-leading Gen 6 FC switch gives small-to-midsize data centers high-performance storage access, and offers the freedom to scale on demand—from 8 to 24 ports auto-sensing 4, 8, 16, and 32G port speeds as well as a total bandwidth of 768Gbps. A point-and-click UI makes it all fast and easy to install.

The Emulex LPe35000-series FC HBAs by Broadcom are designed for demanding mission-critical workloads and emerging applications. Emulex LPe35000-series HBAs are available with single, dual, or quad 32G FC optics. The single-port and dual-port models can be upgraded with 64GFC optics. Emulex 32GFC also provides seamless backward compatibility to 16GFC and 8GFC networks to provide an upgrade path for existing SAN fabrics.

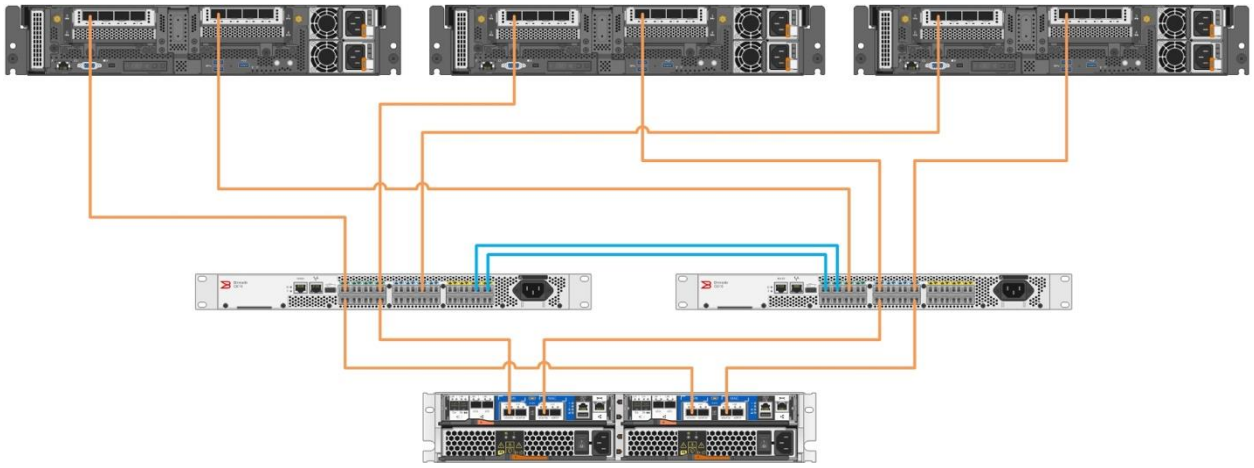


Figure 1) Small example architecture.

Medium architecture

For larger environments or workloads, the NetApp ASA C400 system and Brocade G720 provide a solid foundation for today's needs without sacrificing the growth of tomorrow. Organizations can start with a few hundred VMs and a handful of servers and then scale within a high-availability (HA) controller pair or cluster to dozens of servers running densely packed VMs.

The ASA C400 supports four 16Gb FC ports per controller with five expansion slots for 4-port 32Gb FC cards, offering plenty of connectivity. On the capacity side, like the ASA C250, it can start with as few as 8 15TB SSD drives, 65.9TiB usable (122TB raw) but in an external shelf, and it can be further expanded to a total of four external 24-drive shelves, reaching a capacity of 1.1PiB usable (1.47PB raw) with 15TB drives or 2.23PiB usable (2.95PB raw) with 30TB drives.

The Brocade G720 is designed for maximum flexibility and value. This enterprise-class FC switch offers pay-as-you-grow scalability with ports on demand (POD). Organizations can quickly, easily, and cost-effectively scale from 24 ports to 64 ports to support higher growth. The Brocade G720 provides 48 64G SFP+ ports and 8 2x64G double-density SFP-DD ports, all in an efficient 1U package, and it can auto-negotiate speeds to align to the specifications of NetApp systems. The Brocade G720 base configuration comes with 24 ports enabled and can scale to 64 ports by installing SFP licenses and an SFP-DD POD license in any order and any combination. With a maximum bandwidth of 4.096TBps and auto-sensing of 8, 10, 16, 32, and 64G port speeds along with 10Gbps optionally programmable to fixed port speed, the Brocade G720 is well matched with the ASA C400's scalability.

As with the small architecture, the Emulex LPe35000-series FC HBAs by Broadcom can provide the bandwidth and interfaces required to support a growing environment.

20

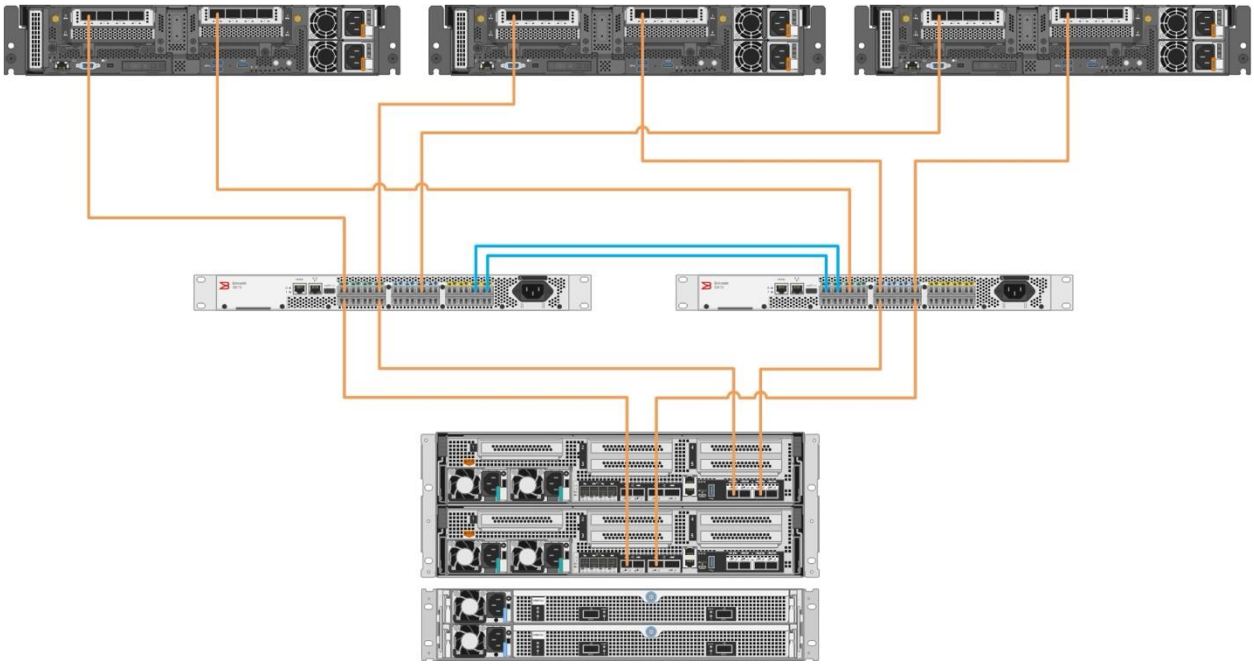


Figure 2) Medium example architecture.

Large architecture

For the largest organizations and workloads, the NetApp ASA C800 system and Brocade X7 Director meet the requirements for the most expansive environments. For thousands of VMs across hundreds of physical servers, this pairing sets an organization's infrastructure foundation on solid footing for the present and the future.

The ASA C800 boasts impressive technical specifications that make it a top choice for enterprise storage. It features high-density NVMe SSDs and supports flexibility in connectivity for 32GFC, NVMe/FC, NVMe/TCP, and iSCSI. It delivers blazing-fast performance with ultralow latency, enabling rapid data access and over 630K IOPS at 2–4ms latency. Its scalable architecture allows seamless expansion, starting at 118.9TiB usable (183TB raw) via 12 15TB internal NVMe SSD drives, and supporting up to 240 30TB NVMe SSDs—48 internal and 8 external 24-drive shelves—for a maximum HA controller capacity of 5.39PiB usable (7.37PB raw). With the ability to cluster up to six HA pairs (12 total nodes) while having performance and capacity scale near linear to over 3.7 million IOPS and over 32PiB usable, the ASA C800 makes it easy for an organization to accommodate growing data requirements. As with all NetApp ONTAP based systems, the ASA C800 also incorporates advanced data reduction technologies, including inline deduplication and compression, which can achieve data reduction ratios of up to 10:1, effectively reducing storage footprint and lowering operational costs. Furthermore, with enterprise-grade data protection features such as RAID protection, NetApp Snapshot copies, and encryption, the ASA C800 maintains data integrity and security, meeting the stringent requirements of modern business environments.

Meet ever-increasing demands for quicker, more reliable data access with the Brocade X7 Director family. With ultralow latency and 64G links that auto-negotiate to 32G and 16G FC, these directors provide the highest level of performance needed for next-generation data centers. Combined with autonomous SAN technology, Brocade X7 Directors harness the power of analytics and the simplicity of automation to optimize performance, ensure reliability, and simplify management. The FC64-64 blades provide 32 ports of up to 64G, 32G, and 16G FC with up to 8 blades per chassis for a total of 512 ports. Leveraging these

capabilities enables organizations to realize a self-learning, self-optimizing, and self-healing SAN, making the Brocade X7 Director a highly efficient and resilient solution.

The Emulex LPe36000-series boasts impressive performance specifications, including support for PCIe 4.0, which doubles the bandwidth compared to PCIe 3.0, enabling faster data transfer—up to 10 million IOPS. With NVMe/FC support, it delivers ultralow latency and high throughput, facilitating rapid access to data for demanding applications. This Emulex series is available with single- or dual-port 64G FC, with backward compatibility to 32G FC and 16G FC networks. These performance specifications make the Emulex LPe36000-series ideal for high-performance computing environments where speed, reliability, and scalability are paramount.

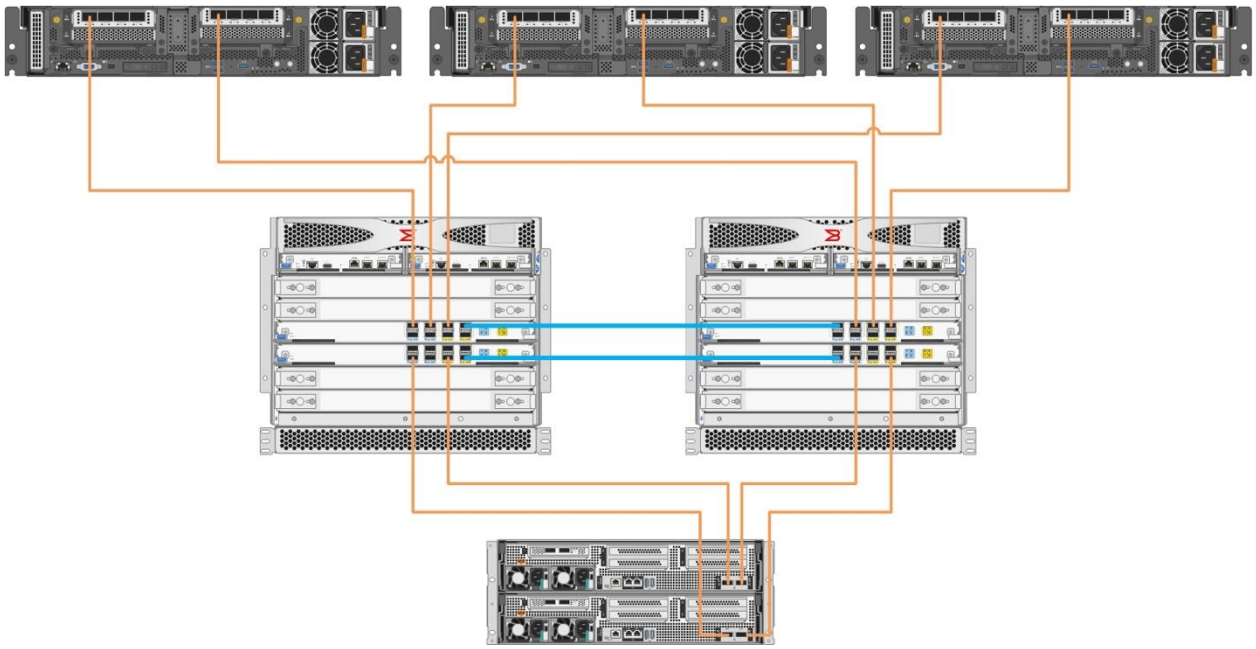


Figure 3) Large example architecture.

Performance optimization

When organizations are in the market for new IT infrastructure solutions, performance optimization plays a critical role in the decision-making process. The ability of a system to efficiently handle workloads, scale with business growth, and maintain high levels of productivity can significantly influence the return on investment (ROI) and TCO.

Organizations must first understand their specific performance requirements, which can vary widely depending on the nature of their workloads, the size of their operations, and their future growth plans. This assessment helps in identifying solutions that not only meet current demands but also have the potential to scale for future needs without costly overhauls.

After requirements are established, the capabilities of potential solutions must be evaluated. Organizations must balance performance requirements with resource utilization. For example, the NetApp ASA C-Series offers cost-efficient, all-flash storage, which meets the performance requirements of most workloads. The Brocade SAN's high-speed networking and advanced fabric services ensure that data is transferred efficiently across the network, while VMware vSphere 8's virtualization efficiencies allow optimal resource allocation and management.

A solution's ability to scale is essential. Buyers need to consider how well the solution can adapt to increasing data volumes and transaction rates. A system that can scale easily, such as the NetApp ASA C-Series with its cluster-mode capabilities, will be more attractive than one that requires significant additional investment to grow.

The combination of NetApp ASA C-Series, Brocade SAN, and VMware vSphere 8 creates a cohesive environment where each component's strengths are amplified. End-to-end capabilities across the storage and fabric layers keep data flowing efficiently from the storage array to the hypervisor. Brocade's robust SAN infrastructure supports the high-speed data transfer requirements of NetApp's flash storage, and VMware's advanced virtualization features efficiently allocate these resources where they are most needed.

Proactive monitoring and analytics from each component's ecosystems—NetApp Active IQ® Digital Advisor, Brocade Fabric Vision, and VMware vSphere—provide a comprehensive view of the infrastructure's health and performance. This integrated monitoring facilitates a proactive approach to system management, allowing timely adjustments and keeping performance at peak levels.

The strategic integration of NetApp ASA C-Series, Brocade SAN, and VMware vSphere 8 delivers a SAN environment that is high performing, resilient, and efficient. By leveraging the advanced features and capabilities of each component, an organization's SAN infrastructure is not only equipped to handle current demands but is also future-proofed for emerging data-intensive workloads. This synergy drives operational efficiency, reduces TCO, and provides the agility needed to respond to the ever-changing landscape of enterprise IT.

Testing

To validate the performance ability of modern NetApp capacity-flash-based systems, Brocade Gen 7 switches, and VMware vSphere 8, the following lab test demonstrates the results that common higher-end workloads such as Oracle and SQL Server can achieve.

Oracle test configuration

As shown in Figure 4, we deployed four Fujitsu Primergy RX2540 M4 servers. We installed VMware ESXi 8.0.0 on each server and installed four Oracle Linux 8.7 VMs, one per server. Each VM contained one Oracle Database 19c instance in a RAC configuration, as shown in Figure 4.

We allocated a 10TB database on the Oracle RAC. For our FCP testing, we distributed the database across 32 data LUNs and 8 log LUNs.

We configured each ESXi host to have two 32Gb FC ports; each was connected to two G720 Brocade switches. The ASA C800 had four 32Gb FC connections on each of two storage nodes, resulting in a total of eight 32Gb connections to these G720 switches. We configured zoning on the Brocade Director by using single-initiator zoning and worldwide port names (WWPNs) to identify zone members. Port zoning on the G720 switches was configured to allow each initiator port to map to eight target ports (four targets on each ASA C800 node).

Only the Virtual Machine Disks (VMDKs) for the databases and logs were stored on the ASA C800 systems. We stored the host VMDKs on a separate NetApp AFF A300 storage system.

For Ethernet connectivity, each of the hosts had both 1Gb and 10Gb links for management, vMotion, and other provisioning traffic.

Table 1) Hardware for joint solution with Oracle 19c.

Hardware	Quantity
Storage ONTAP 9.13.1 NetApp ASA C800 HA pair with 4 32Gb FC target ports and 48 NVMe 15TB capacity flash SSDs	1
Switches Brocade G720 32Gb FC Switch 10Gb Ethernet Switch	 2 1
Fibre Channel HBAs Emulex LPe32002-M2 32Gb FC	 4
x86 servers Fujitsu Primergy RX2540 M4	 4

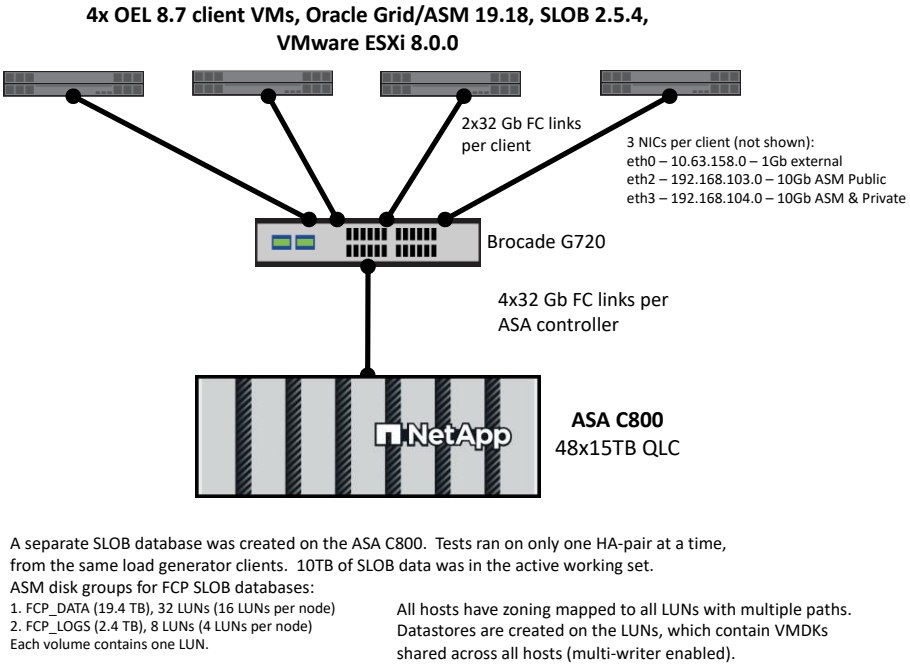


Figure 4) NetApp, VMware, and Brocade Oracle testbed.

Oracle workload design

To drive workload to storage systems, we used SLOB2 (Silly Little Oracle Benchmark)—the preferred tool for evaluating database performance. It was developed by Kevin Closson and is available from his website. It takes minutes to install and configure and uses an actual Oracle database to generate I/O patterns on a user-definable tablespace. It is one of the few testing options available that can saturate an all-flash array with I/O. It is also useful for generating much lower levels of I/O to simulate storage workloads that are low IOPS but latency sensitive.

We ran two suites of load points:

- 100% SELECT statement workload (simulating a 100% random-read workload)
- 75% SELECT and 25% UPDATE statement workload (simulating an ~80% random-read workload)

We allocated a 10TB database on the Oracle RAC. For our FCP testing, we distributed the database across 32 data LUNs and 8 log LUNs. We used the *obfuscate* option in SLOB to randomize the data patterns used to populate the database and reduce unrealistic data reduction in ONTAP.

Oracle solution verification

To validate the solution performance of the ASA C800 system, we validated and compared the performance with the demands of VMware-hosted Oracle workloads. This testing highlights the consistent performance offered by ASA C-Series systems with latency that meets all but the top few percent of workloads.

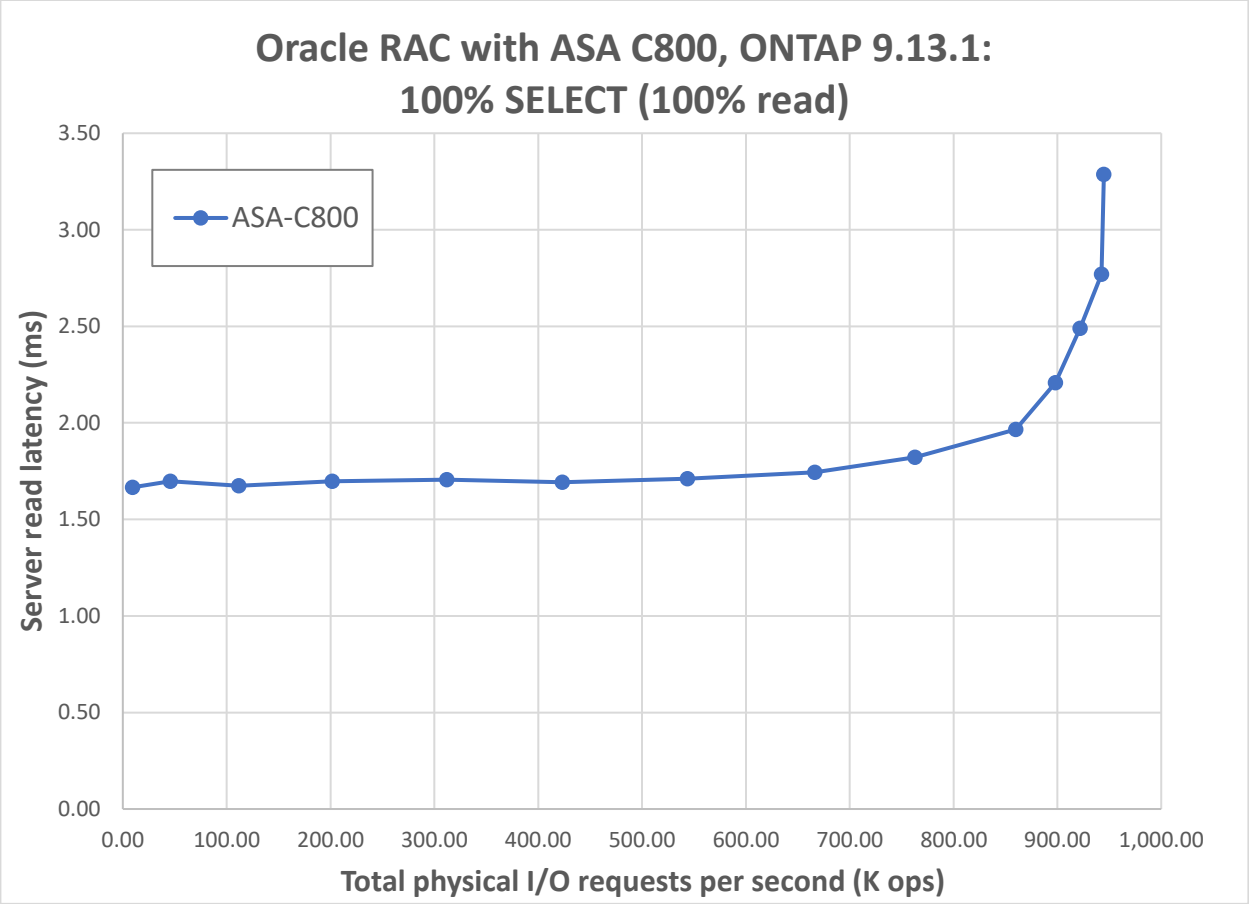


Figure 5) Oracle RAC with ASA C800, 100% SELECT.

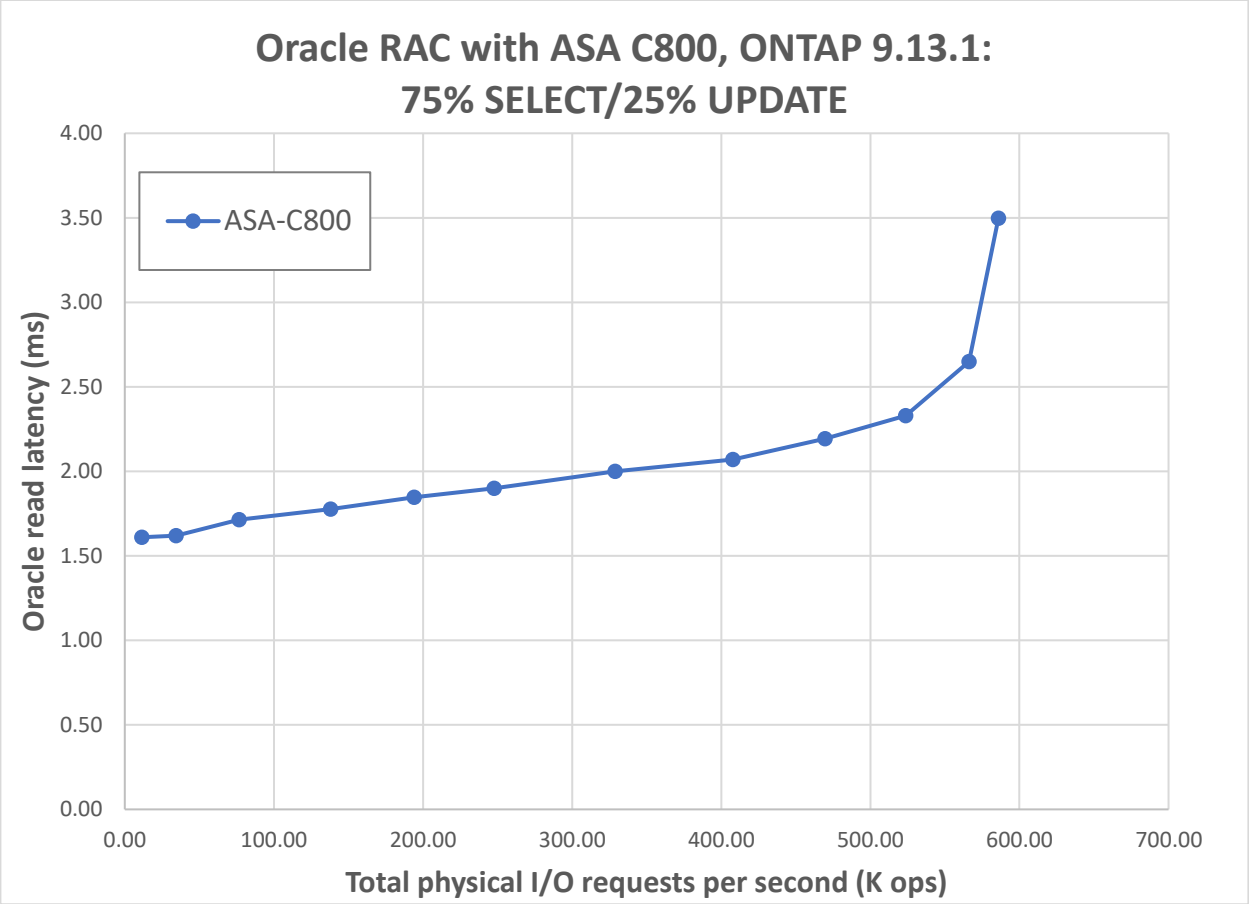


Figure 6) Oracle RAC with ASA C800, 75% SELECT/25% UPDATE.

Microsoft SQL Server testbed configuration

Starting with the base configuration of servers from the Oracle testbed, two additional servers were added as shown in Figure 5.

Each of the (ESXi hosts) SQL Server hosts also had two FCP ports that were connected to each G720.

Each ASA C400 node had four FCP target ports that were also connected to the G720 switch, for eight total connected target ports.

Each server had two 10Gb IP connections for workload communication and a 1Gb IP public interface.

VMware ESXi 8.0.0 was installed on each x86 host. The ASA C400 storage system contained two nodes, with a single data aggregate (21 data disks, 2 parity disks, 1 spare) on each node. We configured FCP using a single ONTAP storage virtual machine (SVM). The Virtual Storage Console (VSC) was used to configure host settings to best practices.

ONTAP best practices for vSphere are to use a single LUN/namespace for each datastore, with a recommended size of 4TB to 8TB. This size is a good balance point for performance, ease of management, and data protection (using either tape backup or remote replication). For FCP, datastores were provisioned using the VSC with:

- Thin provisioning (NetApp FlexVol® volumes, LUNs, and VM files)
- FlexVol volume auto-size (VSC default)

- Default configuration for all storage efficiency settings for ASA C-Series systems, delivering excellent space savings without performance penalties
- Supported Snapshot copies (not scheduled or reserved)

Table 2) Hardware for joint solution with MSSQL Server.

Hardware	Quantity
Storage ONTAP 9.13.1 NetApp ASA C400 HA pair with 4 32Gb FC target ports and 24 NVMe 15TB capacity flash SSDs	1
Switches Brocade G720 32Gb FC Switch 10Gb Ethernet Switch	 2 1
Fibre Channel HBAs Emulex LPe32002-M2 32Gb FC	 4
x86 servers Fujitsu Primergy RX2540 M4	 4

Because ONTAP systems are designed for multiple workloads and tenants, the best performance is obtained when at least four FlexVol volumes are used per node. IT teams evaluating ONTAP systems for vSphere should keep this in mind. It might be simpler to configure a single datastore with a single LUN for a proof-of-concept (POC) evaluation; however, this doesn't represent a normal vSphere storage environment and will not deliver the best performance from an ONTAP system. Likewise, performance is best tested with multiple VMs. Testing storage performance by running a storage benchmark tool in a single VM is not representative of typical virtualization workloads.

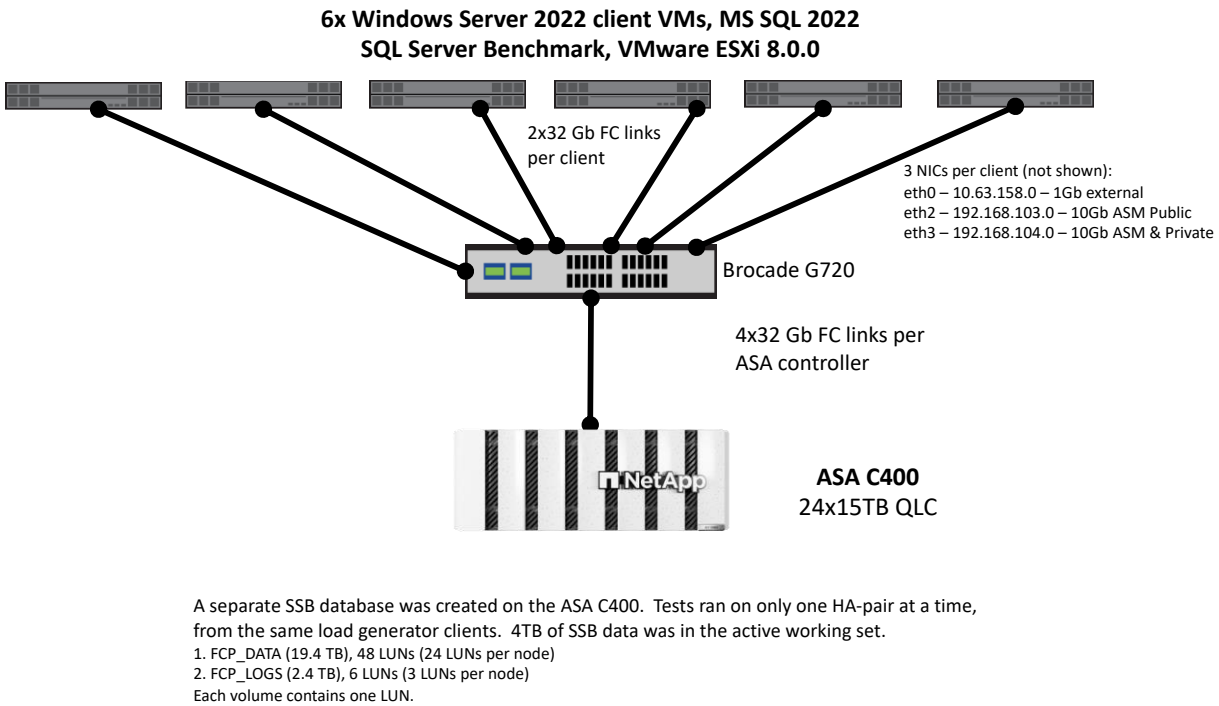


Figure 7) NetApp, VMware, and Brocade SQL Server testbed.

SQL Server workload design

For our testing, we used a NetApp-internal SQL Server workload generator tool called SQL Server Storage Benchmark (3SB). 3SB can drive massive-scale SQL execution against a SQL Server 2022 database to simulate an OLTP workload. We used 3SB to generate a workload by making SELECT and UPDATE SQL statement calls directly to the SQL Server database environment installed on our host systems. We configured the 3SB workload generator on a dedicated server to ensure that the workload execution did not disrupt our test workload.

For this project, we ran a set of 3SB workloads to ramp from 4 to 400 SQL Server users. Each data point ran a fixed number of users and threads for 15 minutes. This allowed us to gather performance metrics at a range of different load points and determine peak performance. Client metrics were collected by 3SB from Windows *perfmon*. Each set of data points was run three or more times for each workload mix to ensure repeatable results. All sets of workloads were run on an ASA C400 system.

We ran two suites of load points:

- 100% SELECT statement workload (simulating a 100% random-read workload)
- 70% SELECT and 30% UPDATE statement workload (simulating an ~80% random-read workload)

We used the 3SB tool to create 800GB SQL Server databases. We spread the database across eight 200GB VMDK files, and one additional 200GB VMDK to handle the database log activity. For the FCP environment, we deployed nine thin-provisioned 250GB LUNs on each of the four SQL Server hosts. We created one LUN per volume, one datastore per LUN, and one VMDK per datastore.

The tool allowed each virtual user to randomly access the schemas in the database and choose where to read or update within that schema. This ensured that the working dataset used the entire database and wasn't completely resident in memory.

SQL Server solution verification

To validate the solution performance of the NetApp ASA C400 system, we validated and compared performance across two key SQL Server workload mixes. The following charts show the test results for both workloads as the workload is scaled to limits of the platform. This verification highlights the consistent performance offered by ASA C-Series systems delivering latency that meets all but the top few percent of workloads.

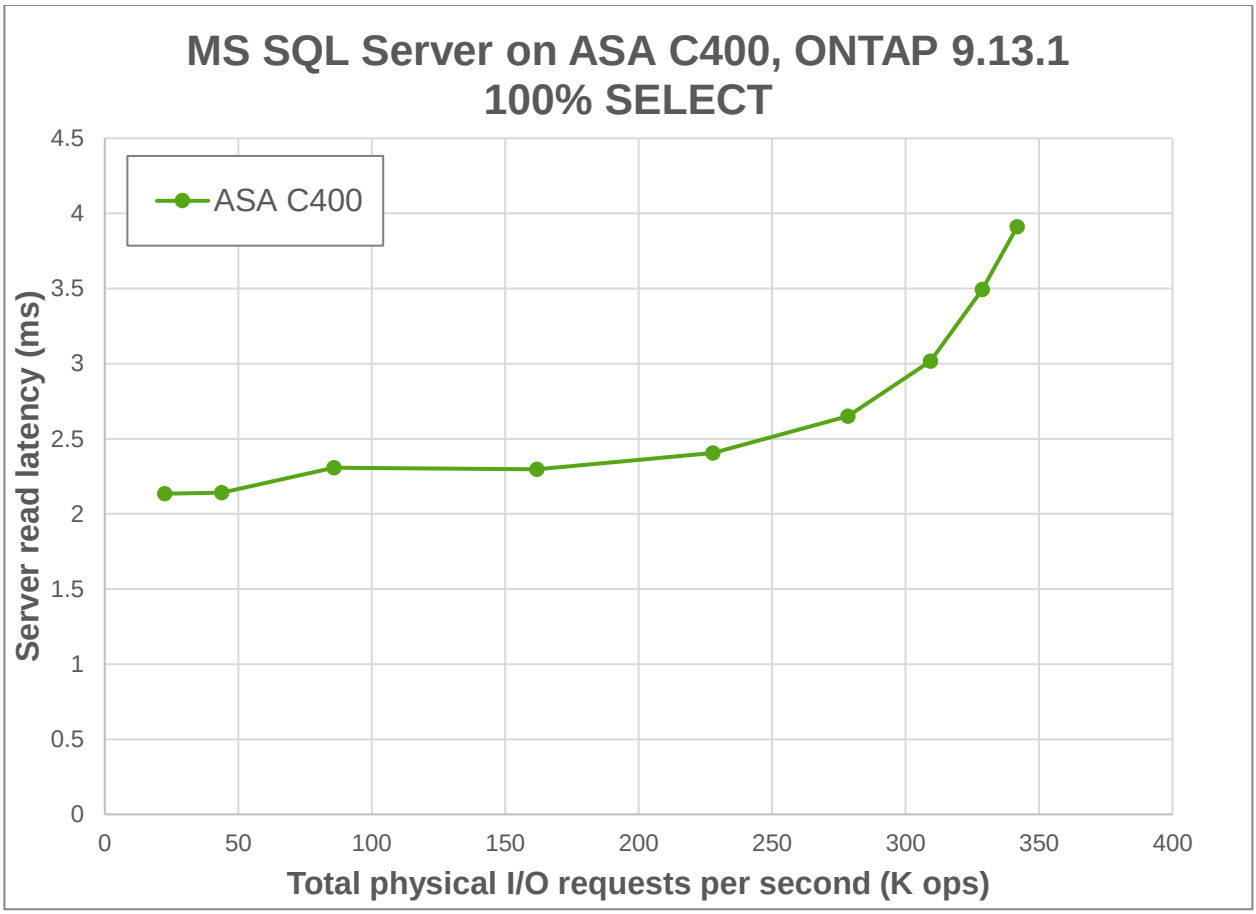


Figure 8) SQL Server on ASA C400, 100% SELECT.

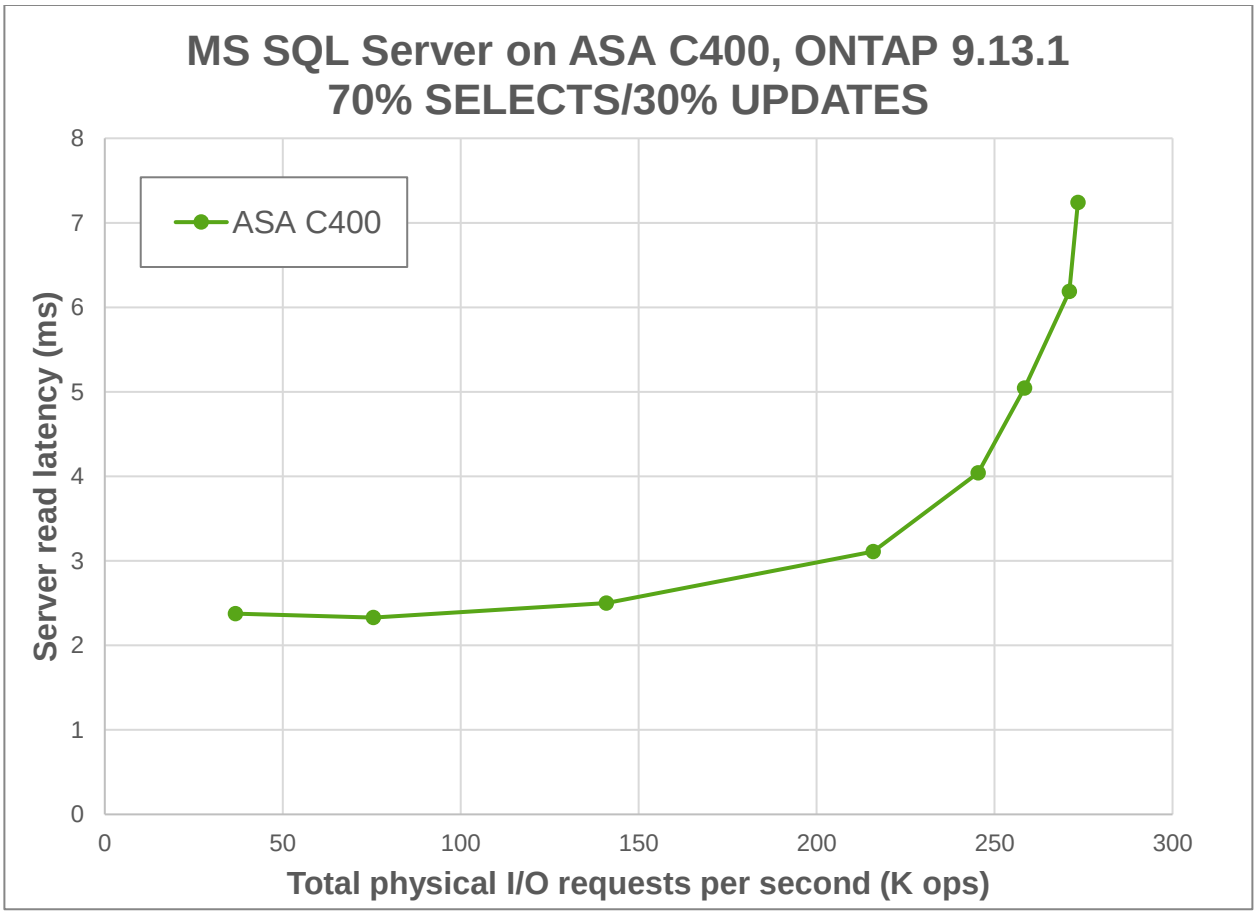


Figure 9) SQL Server on ASA C400, 70% SELECT/30% UPDATE.

Testing impact

For both Oracle and SQL Server testing, the results highlighted the NetApp ASA C-Series' ability to consistently perform with 2–3ms response times under different conditions.

With the ASA C800 system, our Oracle FCP tests showed 2ms or better at 800K IOPS for reads (SELECT) and over 500K IOPS for a mixed read/write (SELECT/UPDATE) environment. This is high performance for most workloads.

We observed the ASA C400 system over FCP at 2–3ms up to 300K IOPS as shown by the 100% SELECT workload and over 200K IOPS in mixed SELECT/UPDATE workload. The ASA C400 provides excellent top-end performance at consistent, higher response times.

Performance optimization allows an organization to choose the appropriately sized platform that will meet the application requirements and keep costs in check without compromises. As for the third concern—security—the NetApp, Brocade, and VMware stack has that covered too, as we discuss in the next section.

The most important question with any sizing effort is "What do you need?" For example, there is no reason to pay for IOPS capabilities or latency benefits if the workload does not rely on them. A POC that is based on nothing more than which configuration shows the highest IOPS potential on a test isn't useful unless you know that the limiting factor for a given business need is genuinely raw IOPS. In addition, a pure IOPS test ignores additional critical factors, such as latency. Not all workloads can be numerically

quantified. Sometimes the only option is to take some time to understand the business need. For example, who is using the application? Are they just making updates, or are they running intensive reports that require millions of individual I/O operations? For example, in working with an Oracle database, the gold standard is the AWR report. It takes only a moment to run `awrrpt.sql` and generate a detailed performance breakdown of a particular hour in which I/O was known to be high, users were complaining, or critical processes were running. This tells you what level of IOPS you really need, what the current latencies look like, and whether storage is even a performance problem in the first place. When you have an idea what your needs are, you can select the right platform.

Cyber resilience

Top of mind for all companies is disruption due to a cyberattack. It is less a question of **if** and more preparing for **when** an attack will occur. Enabling security features at every level helps provide a robust defense that delivers protection, early detection, and rapid recovery.

The infrastructure should have the additional protection of network firewalls, intrusion detection systems, intrusion protection systems, application security, layer 2 design security, layer 3 design security, and layer 1 access security. However, today's infrastructure can help in its own defense, bolstering security efforts already in place. Many of these security features and functions are included and just need to be set up or enabled.

NetApp security

NetApp is committed to security certification to meet organizations' needs for confidentiality, integrity, and data availability—at a level that can only be achieved with decades of security hardening. As the #1 provider of data storage and management to the U.S. federal government, NetApp understands the importance of security.

NetApp ONTAP is the first enterprise storage and data management platform to achieve Commercial Solutions for Classified (CSfC) validation—a cybersecurity program led by the U.S. National Security Agency—for data at rest. CSfC validates commercial IT products that have met the highest level of strict encryption standards and rigorous security requirements for both hardware and software solutions. With this validation, organizations around the globe can benefit from the robust security capabilities of ONTAP to protect information on premises and in remote locations from foreign actors, ransomware attacks, and other data loss threats.

NetApp follows a security lifecycle model to maintain solution integrity. The ONTAP kernel and NetApp architecture provide reliability and security in the following ways:

- **Confidentiality:** preventing unauthorized access to customer data
- **Integrity:** preventing unauthorized changes to customer data
- **Availability:** maintaining the availability of customer data (resisting denial-of-service attacks)

Brocade security

Brocade products support a wide range of authentication, encryption, and management tools to protect fabrics and data from unauthorized access:

- **Authentication.** Authentication protocol support includes CHAP, DH-CHAP, FCAP, IKE, IPsec, RADIUS, TACACS+, and P-EAP/MS-CHAP for RADIUS.
- **Encryption (AES/3-DES).** Brocade provides AES-128 and AES-256 encryption and 168-bit 3-DES encryption for IP links on extension products and management connections. Brocade also supports AES and 3-DES with IPsec. These solutions provide high-performance encryption and compression.

- **In-flight encryption over Inter-Switch Links (ISLs).** Brocade X6 with Gen 6 FC port blades, Brocade X7 with Gen 6 or Gen 7 FC port blades, and Brocade G720, G630, and G620 switches support in-flight encryption for traffic over ISLs to minimize the risk of unauthorized access to data within the data center and over long-distance links. Data-at-rest and data-in-flight encryption are complementary technologies that serve different purposes, and each might be required to achieve regulatory compliance.
- **Secure boot.** A switch validates the integrity and authenticity of the Fabric OS (FOS) boot image to establish a hardware-based root of trust through the manufacturing supply chain.

To an attacker, multiple layers of challenge provide the best protection against all types of threats.

VMware security

The components of a vSphere environment are secured out of the box by several features, such as authentication, authorization, and a firewall on each ESXi host. You can modify the default setup in many ways. For example, you can set permissions on vCenter Server objects, open firewall ports, or change the default certificates. You can take security measures for different vSphere objects, for example, vCenter Server systems, ESXi hosts, VMs, and network and storage objects.

A high-level overview of different areas of vSphere that require attention helps you plan your security strategy. You also benefit from other vSphere Security resources on the VMware website.

Hardening

To start, ensure that the equipment is configured to only do what is required to meet the business objectives. Although vendors ship products with many security features enabled by default, adjustments can still be made to further refine the configuration. NetApp, Brocade, and VMware all publish hardening guides that provide easy lists of settings that can be adjusted to improve security. These guides are meant as roadmaps to the features and settings that can be tuned; you should select and align security settings on your infrastructure in accordance with your organization's security policies. By proactively reducing vulnerabilities and mitigating risks, security hardening aims to enhance the resilience of the system against unauthorized access, data breaches, and other security threats.

NetApp hardening

Advanced and dynamic threats and vulnerabilities are constantly increasing in sophistication. Because of more effective obfuscation and reconnaissance techniques on the part of potential intruders, system managers must address the security of data and information in proactively. NetApp's hardening guide seeks to help operators and administrators in that task with the confidentiality, integrity, and availability integral to the NetApp solution.

The guide provides guidance on:

- ONTAP image validations
- Administrator and local account security and operation best practices
- Data encryption
- Protocol security
- Platform access control
- And much more

For more information, see the latest security hardening guide for ONTAP.

Brocade hardening

Brocade FOS firmware, SANnav software, and hardware platforms are able to restrict and protect from malicious intent. The capabilities, content, and references in the Brocade hardening guide are based on

features and functionality available with Brocade FOS 9.2.x. If you're using a different version of FOS, reference the appropriate administration guide for configuration details. Among the topics covered are:

- Platform access
- Account and authentication
- Fabric security
- ISL encryption
- Zoning and configuration best practices

For the latest information: https://docs.broadcom.com/doc/FOS-Security-UG

VMware hardening

The VMware vSphere Security Configuration & Hardening Guide has been a trusted resource for over 15 years, guiding virtualization administrators in safeguarding their infrastructure. Although optimal security often conflicts with daily administrative tasks, this guide aims to strike a balance. It offers a foundational set of security best practices, considering both the current threat environment and product capabilities.

For more details, see the vSphere 8 Security Configuration & Hardening Guide.

Zero Trust

The next step in improving the security posture of the infrastructure is to begin introducing the design elements of Zero Trust, because threats can come from insiders as well as outsiders. Zero Trust is a security framework that assumes no inherent trust in any user, device, or network component and requires continuous verification and authorization for access: "Never trust, always verify." It challenges the traditional perimeter-based security model by treating everything as untrusted, regardless of location or context. Key principles of Zero Trust include identity-based access, least privilege, continuous monitoring, micro-segmentation, and encryption. By adopting a Zero Trust approach, organizations aim to improve security by minimizing the potential impact of security breaches, detecting and responding to threats in real time, and reducing the lateral movement of threats within the network.

NetApp Zero Trust

NetApp's approach to Zero Trust security focuses on continuously validating and verifying access to resources and data, regardless of the user's location or the device they're using. NetApp integrates Zero Trust principles into its data management and storage solutions by providing robust access controls, encryption, and data protection mechanisms. With NetApp's intelligent data infrastructure, organizations can seamlessly manage and secure their data across on-premises, hybrid, and multicloud environments while adhering to Zero Trust principles. NetApp solutions incorporate advanced security features such as role-based access controls, encryption at rest and in transit, and data loss prevention capabilities to safeguard sensitive information from unauthorized access or exfiltration. By implementing NetApp's Zero Trust approach, organizations can mitigate the risk of data breaches, enhance compliance with regulatory requirements, and maintain the confidentiality, integrity, and availability of their data assets.

For detailed information, see the NetApp and Zero Trust technical report.

Brocade Zero Trust

Brocade's Gen 7 FC SAN's point-to-point architecture prevents attackers from being able to see—let alone infiltrate—connected storage devices. This, combined with integrated security features, delivers a strong line of defense to protect an organization's valuable digital assets and add controls around the Zero Trust principles of micro-segmentation and authentication. Brocade SANnav software provides monitoring and alerting on security configuration changes and events. It also allows organizations to create customizable monitoring and alerting thresholds to meet their specific security requirements,

helping with the Zero Trust principles of management and monitoring. For more details, see Safeguard your SAN with Brocade® Gen 7.

VMware Zero Trust

VMware vSphere 8 introduces enhanced security features aligned with the Zero Trust model. With its capabilities, vSphere 8 implements granular access controls, micro-segmentation, and encryption to secure data and workloads regardless of their location, whether on premises or in the cloud. Through features like encrypted vMotion and Virtual Machine Encryption, vSphere 8 ensures data confidentiality and integrity, even during migration or at rest. Additionally, vSphere 8's integration with VMware Carbon Black Cloud further strengthens security by providing advanced threat detection and response capabilities, helping organizations proactively identify and mitigate security risks across their virtual environments. By adopting VMware vSphere 8 and embracing the Zero Trust model, organizations can significantly enhance their security posture, reduce the attack surface, and protect sensitive data from evolving cyberthreats.

For more details, see the VMware Zero Trust page.

Ransomware

The most conceptualized type of cyberattack that has been elevated to boardroom conversation is ransomware. Disabling a company's ability to use their data can bring operations to a halt. Applying the previously described security considerations is a good foundation for basic protection that can be further enhanced with features and functions within the NetApp, Brocade, and VMware portfolios. There is no single feature that can deter a ransomware attack; rather, it takes a full security perspective to layer in protection from known attacks, detection for evolving attacks, and recovery options to ensure a rapid return to operation with minimal disruption.

NetApp and ransomware protection

NetApp offers several features to combat ransomware, including NetApp Snapshot technology for point-in-time data recovery; NetApp SnapLock® for immutable storage and robust data backup and replication capabilities; NetApp StorageGRID® for creating immutable object versions with retention policies, and backup to cloud for off-site/third-site protection. ONTAP software aids in detecting ransomware patterns, FPolicy in real-time file monitoring, and volume encryption in protecting data at rest. NetApp also emphasizes security hardening, provides predictive analytics through Active IQ, and supports integration with various security tools. However, it's crucial to complement these technological measures with comprehensive security strategies, including user training, security audits, and incident response planning.

For more information, read the technical report on NetApp solutions for ransomware.

The NetApp Ransomware Recovery Guarantee program

Although best-in-class software, tools, and technology can help detect and prevent cyberthreats from occurring, there is never a guarantee that any IT organization can avoid attacks completely. When ONTAP and the NetApp technologies and solutions just mentioned are configured properly in advance of a threat (with the assistance of NetApp Professional Services or an authorized channel partner), they enable you to protect against, detect, and recover from a ransomware attack. NetApp is so confident in our technology that we guarantee that your data can be protected and recoverable if an attack occurs. NetApp Professional Services is here to assist you in recovering your data in case of an attack.

For more information about the Ransomware Recovery Guarantee, read the program's full terms and conditions.

Brocade and ransomware protection

Brocade plays a crucial role in mitigating the risk of ransomware attacks by providing robust network security measures and solutions. Brocade's networking infrastructure, including switches, routers, and firewalls, incorporates advanced security features such as access control lists (ACLs), network segmentation, and intrusion detection and prevention systems (IDPS) to detect and prevent unauthorized access and malicious activities within the network. By implementing Brocade's security solutions, organizations can create secure network environments that limit the spread of ransomware and other cyberthreats, reducing the likelihood of successful attacks and minimizing the impact of potential breaches. Additionally, Brocade's network visibility and analytics tools enable organizations to monitor network traffic for suspicious behavior and potential indicators of compromise, allowing them to respond swiftly to emerging threats and protect critical assets from ransomware attacks. Overall, Brocade's comprehensive approach to network security helps organizations enhance their resilience against ransomware and safeguard their data and operations effectively.

VMware and ransomware protection

A virtual environment provides unique security features that are unavailable to traditional bare-metal deployments. Because each VM is essentially a piece of software, customers have more options to protect against or recover from ransomware attacks. If you have a good backup solution that can detect anomalies between backups, you can quickly take action to recover. Plus, you can isolate different workloads and environments to avoid potential cross-attacks. When combined with the NetApp SnapLock Compliance feature, which can be used to create immutable data copies that cannot be modified or deleted once created, this approach protects backups from being encrypted or deleted, providing a secure recovery solution if an attack occurs.

Proactive defense is the best way to avoid ransomware. Defense-in-depth is the idea of having multiple points or layers as heterogeneous lines of defense. Having different forms of security measures in place to protect the most common areas of attack is an excellent way to help protect against attacks. You want to make sure that if one solution misses an attack, another solution can possibly catch it.

Combined approach

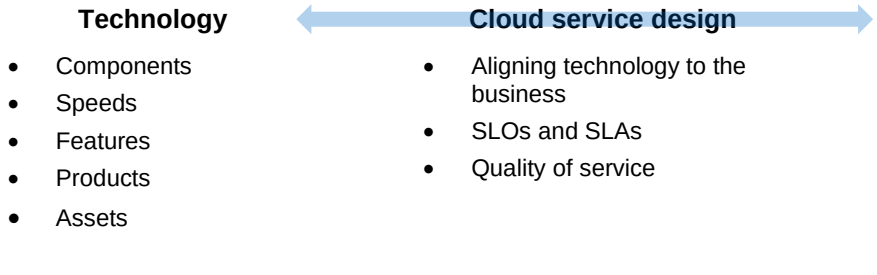
Adopting the security capabilities from NetApp, Brocade, and VMware is recommended from day zero as part of the deployment. Due to the individual requirements of each organization, this paper cannot recommend a particular configuration. However, because deployment and configuration of the NetApp, Brocade, and VMware security components are flexible, you can implement the right configuration for your organization. We suggest that these considerations be discussed and decided upon during the architecture and design phase of your environment to provide optimal performance and protection.

Ultimately, leveraging these capabilities together with the other components in your security strategy reduces risk, enhances protection and detection, and minimizes downtime. The combined security capabilities of NetApp, Brocade, and VMware provide a significant improvement in the overall protection of data in the enterprise.

Cost optimization

Cost can seem like a binary conversation, but when you're also trying to balance performance and security, the equation becomes more complex. To understand the true cost that an infrastructure incurs and optimize it for the best use of resources, you need clear, precise, and detailed information about your IT environment today and how it is used. The NetApp Storage Design Workshop helps businesses understand how virtual compute, flash solutions, and cloud technology deployment can contribute to a more integrated approach to measuring and assessing cost.

Service design bridges the gap between technology and business, enabling IT to function as a service provider. This approach reduces costs, improves performance, and enhances agility. It aligns IT with business needs, helping IT adapt to the digital economy's demands.



Operate like a service provider

Cloud service providers have adopted a business model that offers predictable services with measurable cost and performance per unit of service, similar to a restaurant providing a menu of priced meals. This service model's success lies in careful management of value and cost per unit of capability.

To embrace this approach and break down silos, defining a menu of IT service levels is crucial. This empowers organizations to leverage cloud advantages both internally and externally. By establishing a menu-like structure, businesses optimize resource allocation, enhance cost management, and align IT services with customer expectations, enabling seamless cloud adoption and unlocking the full potential of this transformative IT model.

There are five steps to achieving a service provider delivery model:

1. Define service metrics.
2. Assess application demands.
3. Define virtual compute and share storage service levels.
4. Architect a shared infrastructure.
5. Automate delivery.

Step 1: Define service metrics

Choosing the appropriate service metrics is critical to being able to deliver a service to applications so that end users get the results they seek. Servers and storage hardware deliver capabilities like access (networking) to compute cycles (CPU/GPU cores), access to system memory (RAM), and access to storage and retrieval of data (bytes) as measured in IOPS or throughput capacity per second (MBps).

Virtualized compute resources are sometimes referred to as "T-shirt" sizes (small, medium, large, extra-large) that specify how much virtual compute, virtual RAM, and shared storage an application has been allocated to consume but not to exceed.

For shared storage systems, you will use the relationship between IOPS and capacity to define service levels. The relationship is expressed as IOPS divided by stored capacity in terabytes: IOPS/TB. This single metric is critical in defining the design of the underlying architecture—all the way down to the storage hardware. The industry term for this storage metric is *I/O density*: the density of IOPS for a given amount of capacity stored.

Latency is a secondary metric that measures how quickly—or slowly—the service is delivered (typically specified in milliseconds).

There is a range of service consumption metrics for IT beyond storage and compute. These metrics can include, for example, application-related services looking at users and transactions; and data protection and recovery, where RTO and RPO play a role in the service.

Step 2: Assess application demands

Start by assessing how applications are consuming infrastructure. For virtual servers, the maximum amount of vCPU and vRAM an application is actually consuming over a given period usually differs greatly from the amount that has been allocated or provisioned. For example, a given application might have an XL “T-shirt size” provisioned with eight vCPU cores allocated and 64GB of vRAM allocated, but when measured over a 30-day period, this application may be consuming only two vCPUs and 8GB of vRAM. This would be four times more than needed, indicating an overprovisioning situation.

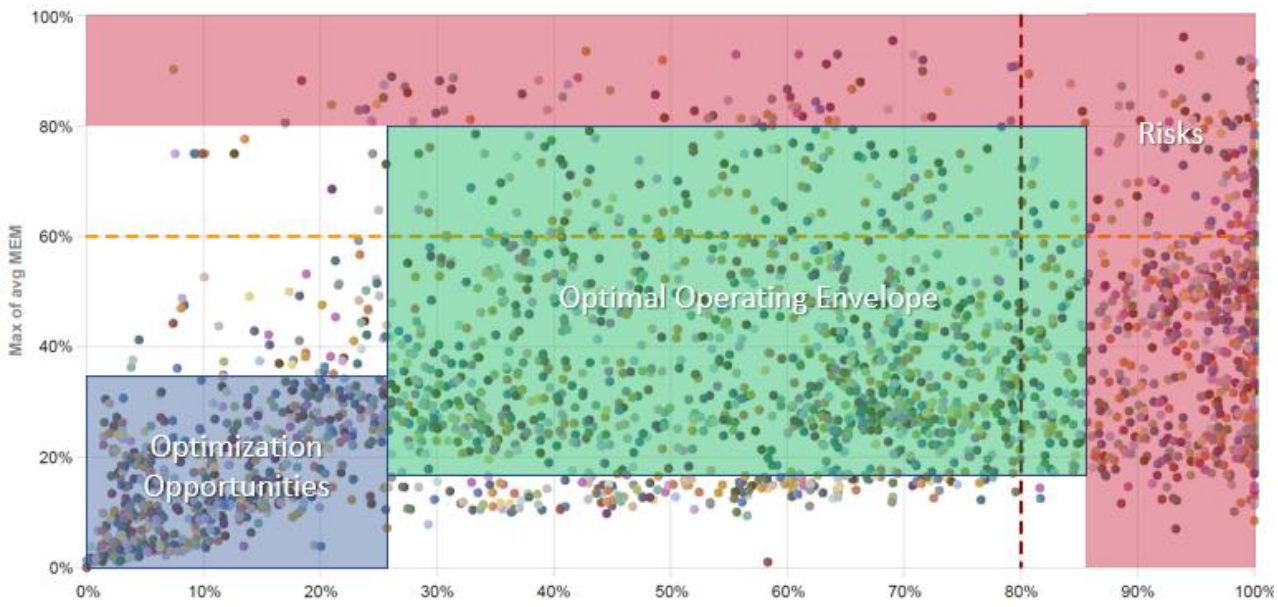


Figure 10) VM optimization.

Figure shows that servers in the blue area are overprovisioned and good candidates for optimization. In contrast, servers in the red area are running at or above recommended settings and should have an adjusted resource pool. Delivering the proper resources to achieve business outcomes for the VMs ensures that the performance expectation will be met without cost waste due to overprovisioning.

Storage hardware delivers operations measured in IOPS, along with storage capacity measured in bytes. You will use the relationship between IOPS and capacity to define service levels. This relationship is expressed as IOPS divided by stored capacity in terabytes: IOPS/TB. This single metric is critical when defining the design of the underlying architecture. The industry term for describing this storage metric is *I/O density*: the density of IOPS for a given amount of capacity stored.

Next, assess the distribution of peak latency by capacity stored. This distribution illustrates how well your services are being delivered by the current infrastructure.

Step 3: Define virtual compute and shared storage service levels

Virtual compute catalog

Evaluate all servers in the virtual environment and map them according to their vCPU utilization, vRAM utilization, and storage utilization. This process helps identify risks (red area in Figure) as well as those servers that could benefit from optimization. This analysis provides two critical pieces of data. First, it quantifies and identifies the virtual servers that are likely working in a degraded fashion or whose customers may be experiencing performance issues—usually measured with latency of more than 20ms.

Second, it provides details about where those servers' underutilized CPU and memory could be recovered to stabilize the on-premises environment.

This data can also be used to understand the distribution of resources for supporting the VMs. As shown in Figure , the unoptimized environment has a large number of different memory and vCPU combinations. This raises costs due to not only resource misappropriation but also increased operational complexity.

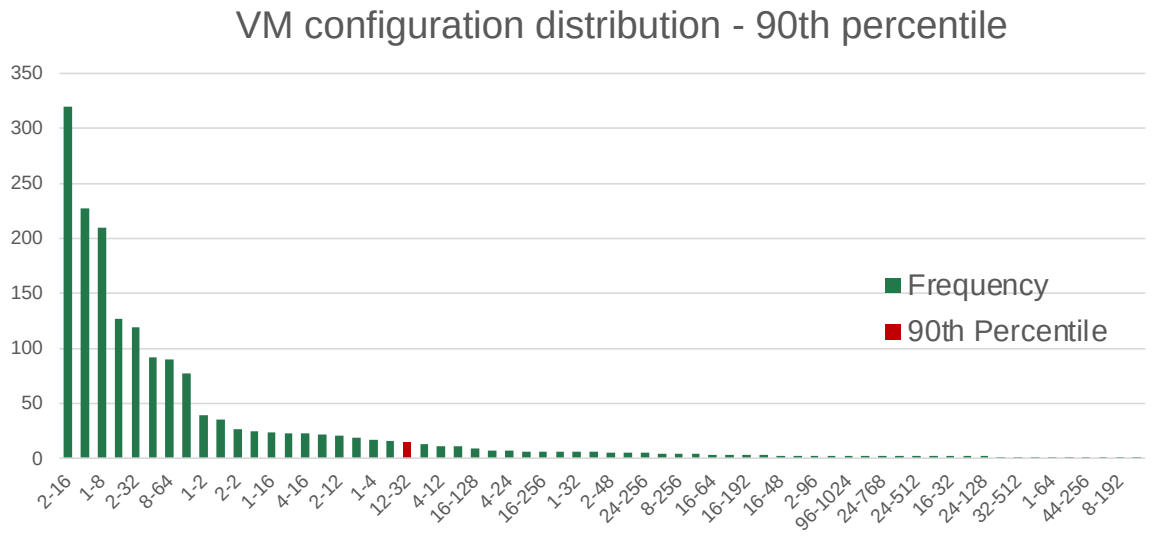


Figure 11) VM resource distribution.

This collection of data can be used to build a service catalog that allows VMs to be placed into building blocks so that performance goals are met while optimizing resources—all based on measured data. Additionally, by reducing the catalog to a well-defined set rather than dozens of different RAM and vCPU combinations, it also drives operational efficiency. The catalog items shown in Table 3 can handle 90% of the environment shown in Figure .

Table 3) VM service catalog.

Service Levels	Tiny	Small	Medium	Large	Xlarge
RAM:CPU Ratio	4	4	4	4	4
GB:CPU Ratio	25	25	25	25	25
vCPU Cores	1	2	4	8	16
vRAM GB	4	8	16	32	64
System Disk GB	25	50	100	200	400
Premium VM Invoice/mo	$ 47.01	$ 52.88	$ 64.63	$ 88.12	$ 135.11
Standard VM Invoice/mo	$ 46.89	$ 52.64	$ 64.15	$ 87.17	$ 133.21
Dense VM Invoice/mo	$ 44.82	$ 48.50	$ 55.86	$ 70.59	$ 100.03

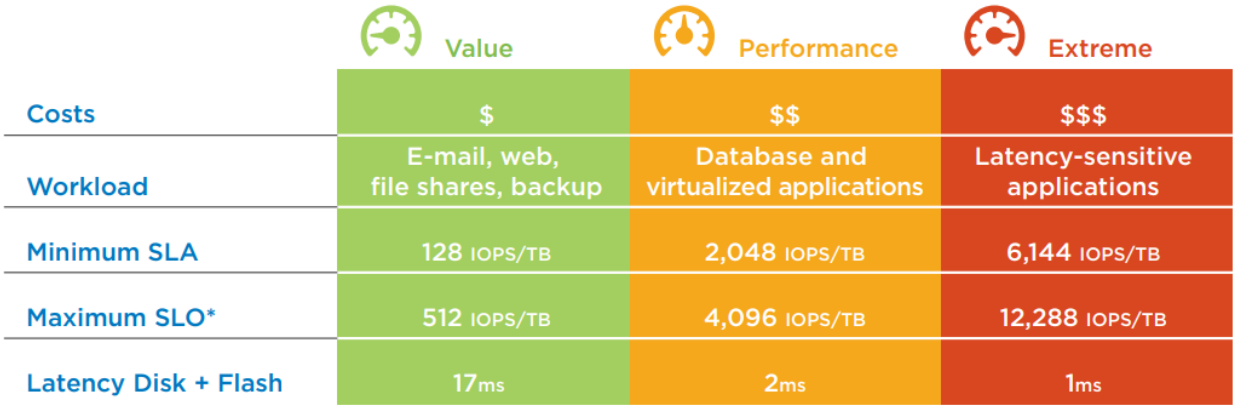
Storage service levels

In data centers that have evolved application by application, you will find hundreds or even thousands of unique configurations. Limiting your service offerings is the first step in simplifying IT infrastructure to provide predictable performance, cost, and agility.

A limited set of service levels aligns to the way that people make choices:

- Slow, medium, or fast?
- Cheap, midrange, or expensive?

With a shared infrastructure that delivers a limited range of service levels, your consumers can choose the service level that best fits their performance and cost requirements. They can rely on storage architects and operators to design and deliver the service that predictably meets their needs.



	Value	Performance	Extreme
Costs	$	$$	$$$
Workload	E-mail, web, file shares, backup	Database and virtualized applications	Latency-sensitive applications
Minimum SLA	128 IOPS/TB	2,048 IOPS/TB	6,144 IOPS/TB
Maximum SLO*	512 IOPS/TB	4,096 IOPS/TB	12,288 IOPS/TB
Latency Disk + Flash	17ms	2ms	1ms

*Maximum SLOs in the table are derived from proprietary assessments of customer workloads made over several years by NetApp Services and validated by NetApp partners.

Figure 12) Storage service catalog.

Application-aligned storage service levels

Application owners choose service levels based on the minimum number of IOPS/TB required to support their applications during peak loads. Latency is generally a secondary consideration.

Step 4: Architect a shared infrastructure

IT is constantly changing, and data has a lifecycle. The worst thing you could do in this dynamic environment would be to design your infrastructure on an application-by-application basis. Only a shared infrastructure can provide nonstop storage services on a broad range of service levels. Eliminating dedicated infrastructure by consolidating many point solutions into shared infrastructure also lowers complexity and labor costs.

The performance and cost requirements of each service level should determine your architecture—for example, whether storage is all flash or flash accelerated.

Infrastructure capabilities required for efficiency

- Support for all-flash or hybrid flash–accelerated disk
- Support for all protocols required by applications

- Constant availability without data loss
- Movement between service levels without disrupting applications
- Ability to start small and scale to very large capacities without disruption

Incorporate flash everywhere to align service levels to architecture

Today, all-flash solutions are dominating the middle and highest service levels. They dominate not only because of speed and latency, but also because physical density allows the consolidation of whole racks of spinning disk drives into a few rack units of SSDs.

Smaller SSDs, such as 800GB and 1.6TB, provide the highest-performance I/O density (IOPS/TB) for the highest service level. Large SSDs, such as 3.8TB and 15.3TB, are the lowest-cost choice for the middle service level because of the lower physical density and because storage operating systems can more efficiently store data on SSDs.

Maximize storage efficiency

Modern storage operating systems on shared storage platforms can store several times more application data than the amount of raw storage. This capability reduces your solution and labor costs to far below what direct-attached storage (DAS) can support. Your storage system should optimize the following efficiency techniques for SSDs:

- Deduplication
- Compression
- Compaction
- NetApp Snapshot copies and clones
- Thin provisioning

With these techniques, SSDs can offer significantly lower cost per gigabyte than DAS.

Manage quality of service

Quality of service (QoS) addresses many problems simultaneously. It enables a predictable cost per GB and provides a performance commitment to applications and storage consumers. Nearly every storage performance underdelivery problem is caused by an overdelivery somewhere else.

Simply overbuying infrastructure doesn’t solve the problem, because any one application can consume all the available IOPS from the allocated storage resources. Without QoS, the performance cost of any volume in the system is completely random, regardless of the underlying media.

Controller Type	ASA C800	SA C800	TRUE	ASA A900	ASA A900	TRUE
Enabled Controllers	2.00	4.00	**6.00**	1.00	1.00	**2.00**
Controller IO Budget (IOPS)	**209307**	**418614**	**627921**	**193814**	**193814**	**387627**
Node Flashcache (GB)	0	0		0	0	
Service Level	**Performance**	**Premium**	**Total**	**Extreme**	**Ultra**	**Total**
Shelves	3.00	3.00	**6.00**	2.50	0.50	**3.00**
Object Store effective TB	0	0	**0**	0	0	**0**
Disk Type (Tier)	15.3TB CF	15.3TB CF		3.8TB SSD	3.8TB SSD	
Drives	72	72	**144**	60	12	**72**
Flashpool SSD per Node (GB)	0	0		0	0	
Raw Storage (TB)	1102	1102	**2203**	228	46	**274**
Usable Storage (TB)	793	793	**1585**	164	33	**197**
Data Stored Efficiently (TB)	634	634	**1268**	131	26	**157**
Allocatable Storage (TB)	1268	1268	**2536**	262	52	**315**
Data Stored Efficiently + Cold Tier (TB)	634	634	**1268**	131	26	**157**
Max SLO @ QoS Throttle (IOPS/TB Stored)	2048	4096		12288	32768	
Min SLA (IOPS/TB Allocated)	1024	2048		6144	16384	
Required SLO IOPS**	**92748**	**185497**		**161249**	**85999**	
Required SLA IOPS**	**92748**	**185497**	**278245**	**161249**	**85999**	**247248**
Controller IO Budget Used	44%	44%		83%	44%	
Capacity Distribution %	50.0%	50.0%	**100%**	83.3%	16.7%	**100%**
IOPS Distribution %*	**15%**	**30%**	**44%**	**42%**	**22%**	**64%**

Figure 13) Example output.

The result of all the data collection and analysis is a design that is engineered around the right resources for the right application, optimizing cost without sacrificing performance. Figure shows the cost effectiveness of the ASA C800 supporting the bulk of a customer's environment with assurances of its performance meeting the needs of the Performance and Premium service levels. For the higher-performance workloads, the ASA AFF A900 meets the requirements of the Extreme and Ultra workloads but is sized appropriately for the workloads that truly require it, again based on measured data.

Step 5: Automate delivery

Service providers can provide and monitor a performance SLA with rapid service provisioning on a large, shared infrastructure by automating QoS policy management by service level and by automating service-level provisioning and orchestration.

Automated QoS policy management by service level

It is impossible to deliver the minimum performance expectation without a QoS limit on storage volumes at each service level. Use a QoS policy manager to automate QoS management at the volume level and translate service-level policies into QoS settings for individual volumes.

By having a small number of service levels that are governed by QoS, you can help prevent performance incidents and make sure that the cost for every volume is predictable.

Automated service-level provisioning and orchestration

Automated provisioning and orchestration can reduce labor costs, enhance agility, and increase the value of your services.

To automate provisioning and orchestration, you must integrate these components:

- Customer-facing service-ordering portal
- Storage volume provisioning workflow
- Orchestration workflow of other services
- Configuration management
- Reporting

Although this integration might seem complex, it is less expensive and easier overall than delayed and error-prone human processes.

Get started

Today's successful IT organizations are taking a new approach to meeting the expectations for more predictable storage costs, performance, and agility for their services. They are moving from managing assets to managing services and operating their IT like a service provider does. Connecting technology to the business is key to a successful transition. NetApp can help you get started.

A NetApp Storage Service Design Workshop helps bridge the gap between technology and business. It creates a strategy for enabling IT to function like a service provider and operate under a delivery model that offers predictability and agility.

The future

Efficiently managing costs, enhancing performance, and balancing security in a SAN environment can pose significant challenges, especially when addressing system bottlenecks and scaling up as workloads exceed initial projections. The introduction of new workloads, AI-driven requirements (such as low latency and high performance), and the need for computational and storage scalability can all have substantial impacts on your systems. By monitoring industry trends in protocols, hardware, integrations, and technology, administrators can effectively build and scale their systems on top of existing architectures. This can often be achieved through systematic upgrades, continuous improvements, and strategic planning cycles.

The NVMe-oF protocol is witnessing increasing adoption and is maturing as businesses invest in both the present and future. NVMe/FC has established a strong presence in many industry block environments and continues to expand, adding integration support across the entire host-to-network-to-storage ecosystem, with VMware virtualization at the forefront. NetApp and Broadcom continue to innovate in SAN infrastructure and encourage you to engage with your sales representatives and NetApp partners to discuss how to maintain your investment in meeting your performance growth needs.

SAN storage infrastructure will also continue to grow, scale, and adapt in various ways to optimize and enhance performance. Adaptability is crucial. Historically, block workloads have been meticulously planned and monitored. When a new system is purchased, the customer typically knows the exact capacity and performance requirements for the next 3 years. However, the advent of virtualization and containerization has disrupted this pattern, making it difficult to forecast block workloads of these types. The ability to add nodes and rebalance workloads in a clustered storage environment is a key factor in managing these complex ecosystems.

Keeping up with networking protocol trends like 64Gb FC, enhancing computational scalability for data services, fortifying new platforms with larger, faster CPUs/GPUs to boost block performance, and scaling out systems in federated pools of storage with load balancing for optimized performance are just a few

examples of areas that could affect your environment. However, as highlighted in this paper, matching the appropriate technologies, current and future, with the actual business need based on measured data is key to the adoption of future enhancements that will drive business gains. These are all important considerations for looking forward in your environment, and NetApp teams and our partner ecosystem can help with these discussions, whether they're about reference architectures or designing SAN solutions customized to your business requirements.

Conclusion

The integration of NetApp storage, Brocade SAN switches, and the VMware by Broadcom hypervisor presents a powerful alliance to address the critical pillars of modern IT infrastructure: cost optimization, performance optimization, and security.

This white paper has thoroughly dissected the complexities of achieving cost optimization in the data center. By advocating for a service-provider-like approach, it underscores the importance of defining precise service metrics and assessing application demands as fundamental steps toward aligning services with business needs. This approach, coupled with the strategic use of NetApp ASA C-Series systems for all-flash storage, enables you to significantly reduce TCO and power consumption while meeting your security, high availability, and performance needs.

Performance optimization is another cornerstone extensively explored in this document. The lab-tested configurations and best practices testify to the potential of this best-in-class solution to support a range of workloads with exceptional performance. The synergy between the storage efficiency of NetApp solutions, the high-speed networking of Brocade's Gen 7 technology, and the advanced virtualization capabilities of VMware vSphere 8 means that the most demanding applications run smoothly and efficiently, thereby maximizing the return on IT investments.

Security, the third pillar, is addressed through a comprehensive cyber-resilience strategy that encompasses hardening techniques, Zero Trust models, and ransomware mitigation. This paper details how the integration of these technologies not only protects against contemporary cyberthreats but also establishes a resilient foundation for business continuity and disaster recovery. With the increasing sophistication of cyberattacks, the importance of a robust security posture cannot be overstated, and the solutions provided here offer a proactive approach to safeguarding critical data assets.

As organizations continue to grapple with managing ever-growing data volumes and the need for rapid access to information from wherever business opportunity arises, the insights provided in this white paper serve as a valuable resource. The architectural frameworks and best practices outlined will help IT leaders make informed decisions that align with their operational objectives and future-proof their infrastructure investments.

Ultimately, the combination of NetApp ASA C-Series systems, Brocade's Gen 7 technology, and VMware vSphere 8 offers a no-compromise solution for enterprises looking to modernize and optimize their storage environments, enhance cyber resilience, and achieve cost efficiencies. By staying current with the latest technological advancements and adopting a holistic approach to IT infrastructure, organizations can ensure that they are well-positioned to capitalize on the opportunities of a data-driven future.

Version history

Version	Date	Document version history
Version 1.0	May 2024	Initial release

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp