Envision a safer and smarter world with Dell EMC PowerScale

This white paper demonstrates how Dell EMC PowerScale enables the organizations to meet the challenges of storing, managing and securing the growing safety and security data while reducing capital expenditures and operating expenses.

June 2020

Revisions

Date	Description	Author	Support
March 2020	Initial release	Anupam Pattnaik	Vincent Ricco, Menaka Thillaiampalam, Chhandomay Mandal, James Meakin, Mordekhay Shushan
June 2020	Update for Dell EMC Powerscale	Anupam Pattnaik	Vincent Ricco, Menaka Thillaiampalam, Chhandomay Mandal, James Meakin, Mordekhay Shushan

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Table of Contents

Executive summary

The global safety and security industry is booming. An IDC study suggests that there will be 41.6 billion IoT-connected devices by 2025, an increase of 75% over 2019. The data generated from IoT cameras and other devices will amount to 79.4 ZB in 2025, up from 13.6 ZB in 2019. These data points illustrate that safety and security is now a data challenge. Organizations face escalating demands for accessing, managing, storing and securing massive amounts of data that is growing exponentially.

The explosion in video data is also bringing changes in the design of safety and security systems. Higher resolutions take more bandwidth to transmit the video streams and require more space to store the imagery. Common data storage problems place limits on many centralized safety and security systems, especially those with more than 200 cameras. Traditional storage systems that statically map camera streams to volumes or logical unit numbers (LUNs) are time consuming to manage and difficult to expand. Storage-attached networks (SAN), direct-attached storage (DAS), and scale-up network-attached storage (NAS) are inefficient because they require the use of many disparate volumes, which increases management overhead. Aligning video streams with volumes reduces storage efficiency and drives up capital expenditures (CAPEX). The overall efficiency rate of traditional storage approaches that store video in LUNs or volumes is about 55 percent to 65 percent. In safety and security systems, the management and storage of data contributes to about 30 percent of expenditures. Traditional storage systems seem attractive for use in safety and security for their low entry cost but are marred by large operating expenses and a high rate of costs for underutilized capacity.

Dell EMC PowerScale scale-out NAS solves these problems. With a distributed file system that presents a cluster of storage appliances as a global namespace, all camera streams in a safety and security system point to a single, scalable volume of storage. When the addition of cameras or an increase in resolution requires more capacity or performance, PowerScale can help organizations scale performance and capacity with ease. Organizations can increase cluster capacity to PB's of storage by simply adding another node—with no downtime or disruption of their safety and security solution. The cluster ingests and distributes high-bandwidth video data by using standard application-layer network protocols. This white paper demonstrates how PowerScale clusters fulfill the requirements of a large, centralized safety and security system by providing simplicity, efficiency, agility, and scalability.

[1] IDC, Worldwide Global DataSphere IoT Device and Data Forecast, 2019–2023

Introduction

Safety and security systems are evolving to adopt IT-centric mechanisms such as the virtualization of servers, networking, and storage. Safety and security systems are increasingly segregating the data plane from the control plane, as the architectures of the systems are adapted to megapixel cameras, high-bandwidth audio and video streams, and longer retention periods. The deployment strategies and network topologies of safety and security systems lead to numerous options for storing audio and video data. Many of these options have originated from the history of safety and security systems, the advent of different data transport protocols, the compression of audio and video images and the demands of emerging technology. Companies and the industry are also coming up with new use cases for ever more powerful and diverse IoT devices, like temperature or vibration sensors in addition to cameras. Those will boost data storage and management needs even more.

Today's safety and security requirements

The days of DVR-like systems are long gone. Safety and security is now a data challenge and demands the same IT-grade systems other business systems and applications leverage. Here are some key trends that are shaping the safety and security industry.

- **Emergence of new devices:** Safety and security systems are starting to benefit from innovations, including edge capabilities, in cameras and device mobility (drones/balloons, body cameras). We are in the midst of these advanced devices which has accelerated wider adoption into main-stream video-based use cases/applications. This rapid adoption is driving pressure on the backbone infrastructure for ensuring uninterrupted capture, retrieval and sharing of video feeds from these sophisticated devices.
- **Higher pixel resolution requirements:** Megapixel cameras are now a common place, where-as the high-end cameras have moved from 4K to 8K cameras. Adding to the pressure are modern user needs for sharper clarity that comes from higher pixilation and faster frame rate capture. Driving a need for a flexible, future-ready infrastructure to accommodate the still evolving safety and security landscape.
- **Increase in device count and retention times:** With technological innovations comes creative ways security professionals are using the deluge of public and private video data. To enable judicious use of data, there are evolutions in government and industry regulations, increasing retention times from 1 month to 90-180 days and at times longer to better serve new/creative security strategies and mitigate litigation risks.
- **A dramatic shift in the amount of storage and compute required to support today's safety and security systems:** The increase in the retention time and generation of metadata on the videos requires more storage. Storage types are moving from standard HDDS to safety and security specific HDDS. In addition, the requirement for larger flash drives are increasing. The video process would require more compute, GPU and TPU abilities which would enable better handling of videos.
- **Need to support modern use cases like Computer Vision, Artificial Intelligence:** The industry is moving towards use of analytics, machine vision and artificial intelligence. These technologies now exist at the Edge with video and IoT sensors as well as server-based solutions. The video needs to be processed and they produce a lot of video metadata. The metadata needs to be processed as well. In order to enable such technologies, there is a need for video acceleration, GPU and TPU abilities. Digital transformation mega trends via machine learning and artificial intelligence require melding together of disparate IoT device data with traditional data sources to enable real-time analytics and insights for safety and security professional (object/threat detection, license plate recognition, facial recognition). These modern, large video footprint applications are accelerating the need for enterprise-grade infrastructure backbone to efficiently manage uninterrupted capture and use of continues data-streams.

The primary trends in safety and security include longer retention times, better graphics functions for clients, and higher resolutions. While higher resolutions increase the number of pixels for human and machine analytics, higher resolutions also require more processing power and bandwidth.

Streaming video data

Streaming video requires various amounts of bandwidth. When video streams from cameras to the VMS and then to the storage system, the resolution, frame rate, and scene dictate the average bandwidth. The information that follows average bandwidths and frame rates with different resolutions illustrate how much bandwidth each camera can consume with a busy scene.

Resolution	4CIF	1080P	3MPixel	5MPixel	10MPixel
Frame rate (FPS)	15	15	15	15	15
Average bandwidth (Mb/s)	1.5	6	7.7	9.6	21

Table 1: Resolution, frame rate dictating average bandwidth

Predicting the bandwidth that a camera requires, however, can be difficult. A camera's average bandwidth varies not only by resolution, frame rate, and scene but also by manufacturer and model due to the use of different video compression implementations. The primary video compression standard used in safety and security, H.264, compresses video by sending frames that represent changed or changing pixels in a video sequence.

With H.264, the group of pictures (GOP) sequences (see Figure 1) define how the compression standard transcodes the video. A GOP sequence determines how well the transcoding handles packet losses and highly dynamic content in a scene. The nonstandard sequencing of the I, P, and B frames in the GOP contributes to the difficulty in predicting how much bandwidth a camera requires:

- **I frame:** Intraframe has no reference to any frame and is stand alone
- **P frame:** Interframe refers to an earlier P or I frame
- **B frame:** Bi-predictive interframe refers to earlier and future frames

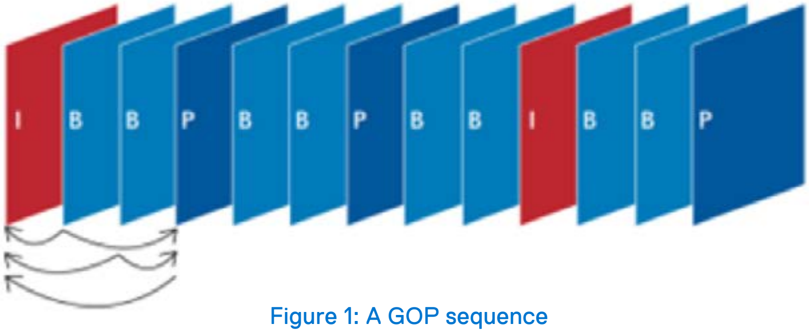

Figure 1: A GOP sequence

The camera manufacturer's implementation of H.264 causes a video stream's bandwidth to vary over time with changes in the scene. Given the same camera and different scenes shot in different light, the video bandwidth varies from 10 percent to 50 percent, making it difficult to predict the average network bandwidth of a camera's video stream. Streaming video from safety and security cameras represents a highly variable, high-volume data flow.

Topologies for safety and security systems

The demands of streaming video often dictate the topology of a safety and security network. Although the trend is to consolidate and simplify the components of a safety and security system's deployment, there are networking barriers that continue to block consolidation and simplification.

Despite such technologies as multiprotocol label switching, data center bandwidth becomes a linear scalar. Safety and security systems that are constrained by the bandwidth of WAN connections benefit from VMS appliances at each site. The following scenarios for the server, software, and storage components of a safety and security system typify the solutions:

- VMS appliance or NVR
- Bare metal servers with VMS software
- Virtual machines with VMS

In an ideal world, the scenario governs the technology that you deploy:

VMS appliance: When there are many distributed video sites, limited network access can create congestion. This scenario leads many system architects to deploy VMS appliances. At each site, the VMS software processes the video streams, which require some direct-attached storage for retention. To satisfy longer retention periods, the systems frequently transfer some of the video data to remote storage sites during network downtimes.

Bare metal servers with VMS software: Hardware procurement guidelines can force system administrators to host VMS applications on bare metal or commodity servers.

Virtual machines with VMS: During the late 2000s, the popularity of VMware and other hypervisors led VMS vendors to adopt virtualization to align with the IT-centric consolidation strategies taking place in data centers. At the same time, virtualization helped overcome the common limit of about 500 Mb/s per VMS server instance, or about 100 cameras per VMS server instance.

Each of these approaches requires a storage system. Video piles up fast, and the volume and velocity of video imagery continues to accelerate. Table 2 provides an example of contemporary high-definition safety and security requirements.

Video scenario	Storage requirement
1080 pixels and 15 frames per second at 4 Mb/s	45 GB per day
A campus with 1,000 cameras	4.5 TB per day
Retention of 30 days	1.5 PB

Table 2: High-definition video storage requirements

Retention periods lead to tiering. Although a VMS server can implement tiers of storage and move data across the tiers, this legacy functionality stems from the days when VMS vendors had to develop a tiering solution because a lack of open APIs, standards, and data access protocols hindered the use of other, more efficient ways of managing the data.

Safety and security systems typically contain a video metadata database as well as the video files. The metadata database includes information mapping the video to a storage location, alerts, operator notes, temporal and spatial information, and other custom data. The video data is usually separate, and many VMS vendors tier the video data between the short term, often 14 days, and the long term, longer than 14 days.

Storage options

There are three primary methods for storing data from video management systems, which are shown in Table 3.

Storage option	Description
Direct-attached storage (DAS)	The VMS uses its on-server disks with an on-server RAID controller.
Storage area network (SAN)	The VMS connects to a SAN with Fiber Channel, Fiber Channel over Ethernet, or iSCSI.
Network-attached storage (NAS)	The VMS transmits the data to the NAS system with a protocol like SMB, NFS, or HTTP.

Table 3: The three primary storage methods for video management systems

The drawbacks of SAN and DAS

The SAN and DAS approaches share some common problems:

- The static mapping of video feeds to each volume and physical disks requires multiple volumes with various groupings of video feeds mapped to them. With a storage area network, for instance, 1.5 PB might take 96 16 TB volumes. The loss of a volume results in a loss of video for playback. Because the bandwidths of cameras vary, hot spots can create a loss of playback and viewing as video feeds are migrated from one volume to another.
- Drive failure frequency and larger drive capacities requiring longer rebuild times can increase the risk of multiple, concurrent drive failures, compromising the availability of safety and security content.
- For DAS, every volume has a limit set by the operating system. Although the limit depends on the operating system, the limit usually varies between 2 TB and 16 TB. Microsoft® Windows® Server 2008, for instance, is limited to 16 TB. For large safety and security systems with storage requirements over 500 TB, the volume limit means that a large number of volumes must be managed. More issues arise because most VMS manufacturers require contiguous volumes for each camera, which entails that a camera feed can write only to a single volume, resulting in high levels of inefficiency. Similarly, the need to defragment the volumes results in additional overhead.

Typical safety and security architectures continue to combine an NVR with a traditional approach to storage. In such cases, the architecture statically maps IP cameras through NVRs to volumes or LUNs. Each volume, however, must be preconfigured for dedicated capacity, retention times, and the camera bit rate. Each volume also entails multiple points of management, making them time consuming to manage and even harder to scale. The efficiency rate of traditional approaches to storage that use LUNs or volumes is about 55 to 65 percent.

In addition to the complexity of multiple volumes, traditional storage systems forfeit a significant amount of capacity to overhead. Each volume in a safety and security system is set up for dedicated capacity plus 20 percent overhead to handle the variability of the video streams, including unpredicted growth and changes to retention times. Each volume has a baseline overhead from the disk parity of RAID 5 or RAID 6 of 20 percent. Each volume also typically sets aside about 5 percent to align video files on contiguous LUNs. In total, traditional storage systems storing video data can lose 45 percent of their capacity to overhead.

The hundreds of video feeds that are recorded by the VMS require high bandwidth to transmit them through the network and into a storage system. The advent of network protocols such as SMB, NFS, HTTP, and Representational State Transfer (REST)—which satisfy high-bandwidth requirements—has opened up the use of NAS in high-volume video environments.

Scale-out NAS vs. scale-up NAS

There are two types of NAS systems: scale-up and scale-out. A scale-up NAS system is typically a node-based architecture with separate modules for storage and processing; each module can be added to a cluster independently. In contrast, a scale-out NAS system is a node-based architecture that combines processing power and storage capacity in every node; each node adds both performance and capacity to a cluster.

Both types of NAS systems benefit safety and security systems for several reasons:

- Standard network protocols like SMB, NFS, and HTTP enable all operating systems—Linux, UNIX, Mac OS X, and Microsoft Windows—to interface with the storage system.
- IP-based storage systems deliver a rapid ROI when they store data for multiple applications because you can consolidate workflows into a single storage system.
- NAS abstracts the data protection schemes and underlying structures by using standard protocols for access and modification.
- NAS abstracts the physical location of the data, making video mappings to NAS volumes much less dependent on the data's physical location.

The primary issue with scale-up NAS systems is that they mimic traditional storage systems: Scale-up NAS systems and clustered scale-up NAS systems contain many volumes and require you to manually migrate data among components.

PowerScale overcomes the problems that undermine traditional NAS systems by combining the three traditional layers of storage architecture—file system, volume manager, and data protection—into a scale-out NAS cluster with a distributed file system.

PowerScale scale-out NAS

A Dell EMC PowerScale cluster scales out, not up. In contrast to scale-up NAS, a PowerScale cluster does not require volumes. Instead, the distributed Dell EMC PowerScale OneFS operating system combines the memory, I/O, CPUs, and disks of its nodes into a single, cohesive storage unit. Every node adds capacity and performance to the cluster. As nodes are added, the file system expands dynamically and redistributes data, eliminating the work of partitioning disks and creating volumes.

- **A single volume.** OneFS operating system enables a single volume to be shared by all the cameras streams—thus saving enormous amounts of time in initial set up. With PowerScale's single volume, single file system architecture, storage systems are simple to install, manage, and scale to virtually any size.
- **Seamless scalability.** With PowerScale's scale-out architecture, organizations can easily scale performance and capacity based on the specific requirements of their business. Organizations can increase cluster capacity to PB's of storage by simply adding another node—with no downtime or disruption of their safety and security solution.
- **Reliable, efficient data protection.** PowerScale offers enterprise level data protection. From Data-at-Rest Encryption (DARE) and self-encrypting drives to quadruple failure protection, video data is protected from accidental, premature, or malicious deletion. Dell EMC PowerScale SyncIQ software delivers high-performance, asynchronous replication of unstructured data to address a broad range of data retention and recovery objectives. Features such as auto-balancing and auto-failover help IT admins / system administrators sleep better at night knowing their safety and security data is safe-guarded.

- **High-velocity, high-bandwidth video ingestion.** For performance, OneFS load balances network connections among all the nodes to eliminate bottlenecks. Safety and security networks can establish either dual 1 GbE or dual 10 GbE connections to the nodes.

A PowerScale scale-out cluster's single volume is ideally suited to work with large, centralized safety and security systems. Scale-out NAS radically simplifies a safety and security system's design, operation, and augmentation. A PowerScale cluster also protects against failure, delivers better ROI than other solutions, and supports open standards like REST for cloud-based access. For more information on the OneFS operating system, see "Dell EMC PowerScale OneFS: A Technical Overview".

Safety and security system design and deployment

A single-volume approach to designing a safety and security system simplifies the work for you as well as your system integrators and VMS vendors. But the single-volume approach must also let you scale the volume so that capacity and bandwidth scale almost linearly.

Some NAS systems do not scale linearly. When a single volume cannot transparently aggregate the capacity and bandwidth across all the storage units, you must fragment the VMS to properly segment the volumes. The NAS system ends up with multiple volumes, resembling a traditional DAS or SAN approach. The result is many storage volumes for each VMS instance—and even more for the whole safety and security system. The system bogs down in complexity because you must group video feeds by volume, as Figure 2 illustrates.

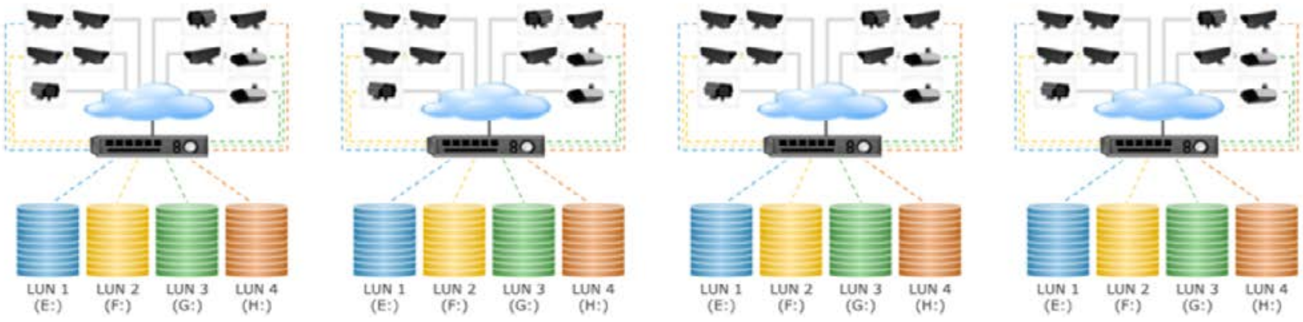

Figure 2: Safety and security system deployment with a traditional storage system

In contrast, the elegance of the PowerScale solution lets you point all the video feeds at a single volume, which the VMS servers can access by connecting to any node. The single volume lets you size the storage system's aggregate bandwidth and capacity without resorting to complex calculations involving the number of volumes.

The cameras deployed in large safety and security systems often require more bandwidth than the average bandwidth specified in the system's design. Actual bandwidth tends to exceed the average expected bandwidth because scenes change and because H.264 compression varies by camera and manufacturer. The bandwidth that a camera requires can shift between 10 and 50 percent, depending on the scene.

With traditional approaches to storage, the variation in the bandwidth of different video feeds unevenly distributes video files among volumes, as can be seen in Figure 3. In video systems with smaller volumes and fewer cameras, for example, the variation in throughput can quickly overwhelm the 20 percent overhead built in to the storage capacity unless the capacity planning assumed extremely high average bandwidths. When the bandwidth associated with a video feed exceeds expectations, the storage volume requires more capacity to meet the same retention times.

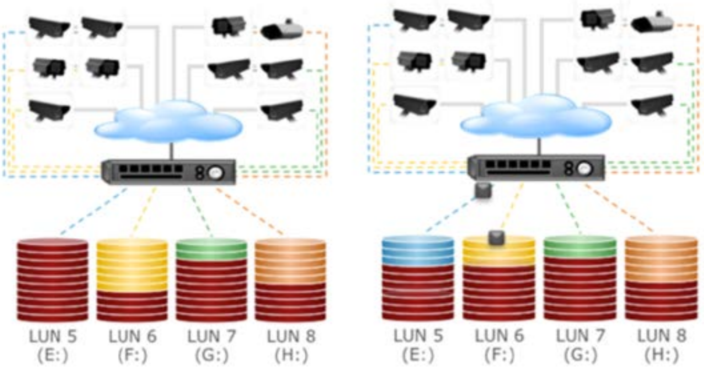

Figure 3: The distribution of safety and security traffic with a traditional storage system

When a volume reaches its full capacity, the VMS deletes the oldest video until it frees up more space. With traditional storage systems, you end up having to migrate video cameras from one volume to another—which forces the VMS to move the video feed data among the volumes. The migration strains the I/O of the VMS servers, affecting video playback to such an extent that frames are lost. Such a data migration can take anywhere from a few hours to more than 12 hours, depending on the VMS vendor and the amount of stored data.

A PowerScale cluster preempts this problem before it occurs. OneFS ingests traffic from video management systems through a single volume and then automatically balances the data among the nodes in the cluster, as Figure 4 illustrates. To address the variability of video streams, OneFS also continuously rebalances data to optimize capacity.

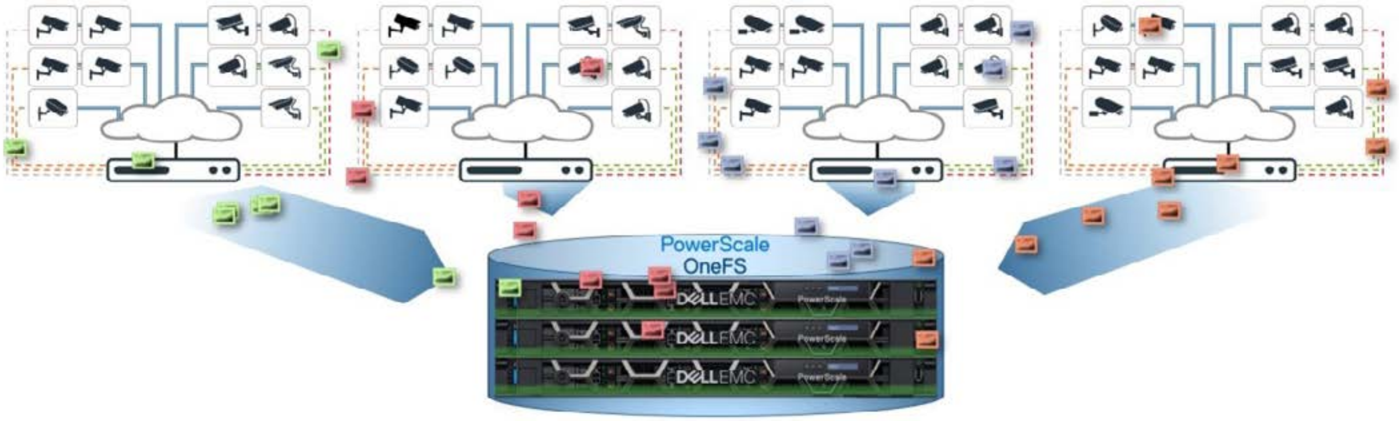

Figure 4: The distribution of safety and security traffic with a PowerScale cluster

The digital footage captured by the safety and security cameras is encoded by the VMS server, including those hosted on VMware virtualized servers, and is then transmitted over 10 GbE network connections to the PowerScale storage cluster. With a PowerScale cluster, every VMS instance can point to the same top-level directory—for example, \\video_repository. Because the OneFS distributed operating system imposes no constraints on the size of a volume, a PowerScale cluster presents all the files on the cluster within a global namespace when a server connects to any node (see Figure 5).

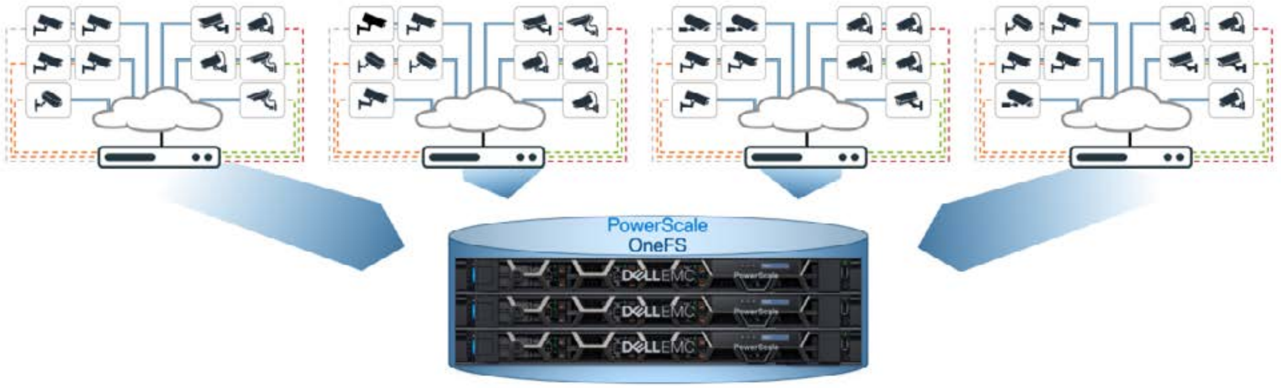

Figure 5: Safety and security system deployment with a PowerScale scale-out NAS system

OneFS further simplifies the deployment of safety and security applications by automatically load balancing incoming SMB and NFS client connections across all the nodes. By default, the OneFS load-balancing module, called Dell EMC PowerScale SmartConnect, distributes client connections using a round-robin algorithm. In this way, a PowerScale cluster is optimized, by default, for safety and security applications.

Because data writes with a large cluster can go to as many as 40 disks—which is many more disks than with a traditional file server—OneFS can write a video stream to disk with performance-enhancing parallel writes. The parallel writes that place a single, large video file on many disks have a multiplier effect on disk throughout that, when combined with the cluster's aggregate RAM, optimizes the speed with which OneFS can write video files to disk.

Large video storage systems typically require defragmentation, which introduces overhead and reduces performance. OneFS, however, eliminates the need for defragmentation by distributing data among a cluster's nodes and by restriping the data to optimize protection and data access. As a result, OneFS is commonly deployed in safety and security systems that store as much as 20 PB of video and file data without the need for defragmentation.

Meanwhile, to retain data with longer retention times or to address changes in retention times, OneFS lets you set policies to automate tiering so that you can cost-effectively store data over time. The tiering policies automatically move files among tiers of storage according to the rules that you set.

A use case from MetLife Stadium

For any organization hosting one of the biggest events in sports, fan safety is a top priority. When the NFL awarded Super Bowl XLVIII to MetLife Stadium, the world's top-grossing outdoor stadium, the organization took a fresh look at the video security monitoring the stands. The picture was not good.

The old security system stored only six days of video, limiting MetLife Stadium's ability to review incidents and identify disruptive attendees. Plus, tape backups of security video required up to 10 hours of downtime. This made backing up video impossible during weeks with multiple stadium events and risked the loss of critical footage. Time also was of the essence. The stadium needed to deploy a new solution before the football season began and be fully prepared for the Super Bowl. It was August—just a few weeks from the first home game.

After considering several options, MetLife Stadium wasted no time choosing Dell EMC PowerScale scale-out storage for its proven integration with the state-of-the-art Genetec Security Center safety and security system and security platform.

With Genetec and PowerScale, MetLife Stadium now monitors every seat in the stadium, improving fan safety and satisfaction. The stadium also increased real-time video storage retention from six to 45 days and enabled archival capacity to hold more than three years of video footage. This eliminated tape backups and associated downtime while reducing video storage administration from five hours to less than five minutes.

“We have much better visibility into what’s going on in the stadium, so we can nip problems in the bud. If there’s an altercation, we review the video to see what really happened and identify the people who started it. The stadium decides if and when these people would be allowed to attend events again. The PowerScale and Genetec solution really makes for a more enjoyable and safer fan experience at our events.”

Robert Doster, director of application services at MetLife Stadium

Storage efficiency

An ESG study says businesses today need low-latency, high-performance access to the vast bulk of their corporate file data, not just subsets of it. File storage no longer has to be just big; it must be big, fast, and efficient. Powered by OneFS operating system, Dell EMC PowerScale is big, fast and efficient and offers extreme performance with massive scalability to support the most demanding file-based workloads.

A PowerScale cluster eliminates much of the overhead that traditional storage systems require. OneFS evenly distributes, or stripes, data among a cluster’s nodes with layout algorithms that maximize storage efficiency and performance. The system continuously reallocates data to conserve space. At the same time, OneFS protects data with forward error correction, or FEC—a highly efficient method of reliably protecting data. The capacity overhead for data protection is about 20 percent in aggregate, not per individual volume. The additional capacity overhead of 20 percent required by DAS and SAN is not needed with the PowerScale cluster. In practice, a PowerScale cluster runs at 90 percent of full capacity, saving as much as 35 percent of capacity over traditional storage systems.

PowerScale delivers over 80 percent storage utilization versus about 50 percent for traditional platforms. The PowerScale platform combines extreme performance with expanded storage capacity and density to enable customers to achieve unprecedented levels of storage efficiency.

	Typical Competitor	Isilon F810 All-Flash
Raw Capacity*	1 PB	1 PB
Storage Utilization**	60%	80%
Usable Capacity	600 TB	800 TB
Data Reduction Ratio***	3:1*	3:1*
Effective Capacity per 1 PB of Raw Capacity	1.8 PB	2.4 PB

- Up to 3:1 data compression
- Dell EMC 2:1 Storage Data Reduction Guarantee
- Up to 139 PB of effective storage capacity in a single cluster
- Up to 33% more effective storage capacity per TB than major competitive offerings

* 1 PB is used for comparison purposes only. Actual raw capacities will vary by storage configurations.

** Storage utilization for traditional storage platforms typically range between 50-60%.

*** Data reduction ratios varies by data set. 3:1 data reduction ratio used in example is typical for some data sets but can vary widely.

Source: Dell EMC

Figure 6. Isilon F810 Overview and Competitive Comparison[3]

ESG mentions in the report that Isilon already was an efficient option for companies due to its utilization capabilities, tiering capabilities, post-process deduplication and other features. With Dell EMC adding inline compression and deduplication to its all-flash Isilon F810 platform makes the efficiency story even stronger. According to Dell EMC’s testing, organizations could see up to 33% more effective storage per terabyte of raw storage capacity and increased storage density for a lower effective dollar amount per terabyte. Notably, the Isilon F810 provides up to 139 PB of effective storage capacity in a single cluster.

[2] ESG Solution Showcase: Dell EMC Isilon Makes Its Efficiency Story Even Stronger, Authors: Scott Sinclair, Monya Keane, September 2019

[3] Dell EMC’s test results have not been independently validated by ESG, September 2019. Additionally, compression ratios vary by data set, sometimes greatly. The 3:1 data ratio in Dell EMC’s example is typical but may vary.

Elasticity and agility

Most safety and security systems are dynamic. As the systems mature, adding or modifying the camera configurations is a common method used to cover other lines of sight. Resolutions are increased to enlarge the field of view or to capture more visual data for analytics. With a VMS server, it takes little more than a mouse click to change a network camera's resolution from 1080 pixels to 3 megapixels.

Traditional storage systems lack agility. When changes to the video stream affect the volume of a traditional storage system, the changes can consume overhead and cause the VMS to warn you that you need to migrate the cameras to another volume. You then need to spend time adding disks, configuring the array with an additional volume that has the right LUN, and formatting for RAID 6. Afterward, the VMS needs to accommodate associating the video feeds to the new LUN and volume, which can take up to 12 hours and affect playback.

Adding capacity and performance capabilities to a PowerScale cluster is significantly easier than with other storage systems—requiring only three simple steps for the storage administrator: adding another node into the rack, attaching the node to the InfiniBand network, and instructing the cluster to add the additional node. Because a PowerScale cluster contains a single, global volume, the problem of one volume filling up faster than another does not occur. A single volume also reduces the likelihood that you will need more capacity because there is no static association between a small set of disks and a volume.

If the cluster does require additional capacity to handle more cameras, it takes less than two minutes to have a node added to a cluster and appear as part of the single volume in a usable manner. When you add a node, OneFS automatically rebalances the data across the new node, with no effect on playback and recording, as verified in tests at Dell EMC labs. More importantly, no changes are necessary on the VMS, where the target volume does not have to change and remains \\video_repository.

The AutoBalance feature of OneFS will automatically move data across the InfiniBand network in an automatic, coherent manner so existing data that resides on the cluster moves onto this new storage node. This automatic rebalancing ensures the new node will not become a hot spot for new data and that existing data is able to gain the benefits of a more powerful storage system. The AutoBalance feature of OneFS is also completely transparent to the end user and can be adjusted to minimize impact on high-performance workloads. This capability alone allows OneFS to scale transparently, on-the-fly, from 10's of terabytes to 10's of petabytes with no added management time for the administrator, or increased complexity within the storage system. For safety and security systems, many of which undergo constant change, the operating costs of PowerScale scale-out NAS may be even lower.

Failure handling

There are two primary points of infrastructure failure in a safety and security system: VMS and storage. Most video management systems include a failover mechanism that transfers the video feeds from a VMS that fails to a secondary VMS, which receives the feeds. With a traditional storage system, when the VMS remaps the camera feeds to the new server, the recordings for the cameras associated with the failed VSM's volumes become unreachable. With a PowerScale storage system, there is no loss of playback for the recorded video.

Disks can present another point of failure in the storage system. If two or more disks fail in the volume of a traditional system, the cameras associated with the volume lose the capability to make new recordings and play back existing content. Even when one disk fails in a volume, frame loss typically occurs because rebuilds affect the safety and security system's bandwidth and processing.

By comparison, a PowerScale storage system can handle two simultaneous disk failures as well as the failure of a node with as many as 36 disks without affecting new video recordings and without affecting playback. New recordings are unaffected if a node fails because the SmartConnect module's automated load balancing of video streams minimizes frame loss in-flight. Dell EMC PowerScale SmartConnect software allows IT managers to meet the demands of an always-on, 24x7 world by providing the highest levels of performance and industry-leading data availability. With intelligent, automatic client connection load balancing and failover capabilities, SmartConnect simplifies and optimizes scale-out storage performance and data availability.

Conclusion

A Dell EMC PowerScale cluster solves many common storage problems for safety and security systems by providing capabilities that traditional storage systems lack:

- **Simplicity.** Dell EMC PowerScale OneFS operating system enables a single volume to be shared by all the cameras streams—thus saving enormous amounts of time in initial set up. With PowerScale's single volume, single file system architecture, storage systems are simple to install, manage, and scale to virtually any size.
- **Massive scalability and extreme performance.** With PowerScale's scale-out architecture, organizations can easily scale performance and capacity based on the specific requirements of their business. Organizations can increase cluster capacity to PB's of storage by simply adding another node—with no downtime or disruption of their safety and security solution.
- **High availability and reliability.** PowerScale is highly resilient, with up to N+4 redundancy and offers proven enterprise-grade data back-up, replication and disaster recovery options. OneFS distributes data across the cluster to guard the data with parity blocks instead of parity disks to ensure there is no video loss even in drastic failure states.
- **High-velocity video ingestion.**For performance, OneFS load balances 1 GbE and 10 GbE network connections among all the nodes in a cluster to eliminate bottlenecks and to accept video streams using network protocols such as NFS, SMB, HTTP, and REST.

Dell EMC PowerScale is enterprise-grade, resilient, scalable and reliable solutions for demanding and data intensive safety and security workloads. PowerScale enables organizations to keep up with growing safety and security data and envision a safer and smarter world by protecting what matters most.

Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell EMC storage platforms.

Related resources

Provide a list of documents and other assets that are referenced in the paper; include other resources that may be helpful.

- Top reasons to choose Dell EMC PowerScale for safety and security
- Traditional storage vs Dell EMC PowerScale for safety and security
- Simplified safety and security for a complex world
- ESG solution showcase: Dell EMC Isilon makes its efficiency story even stronger
- Dell Technologies IoT solution for safety and security