Dell Technologies IoT Solution | Surveillance

August 2018

H17382

Reference Architecture

Abstract

The Dell Technologies IoT Solution | Surveillance is a hyper-converged solution purpose-built for demanding, multi-sense surveillance, such as video, sound, and barometric pressure, comprising both hardware and software.

DELL Technologies

Published August 2018

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

CONTENTS

CHAPTER 1

Overview

Business challenge

Private businesses and public entities generally respond to the rising concerns about theft, fraud, and terrorism by sharpening their focus on physical security and surveillance systems. Organizations such as retailers, casinos, financial institutions, higher education institutions, transportation companies, law enforcement, school systems, prison systems, and government agencies all need to manage and protect their ever-growing volume of physical security information.

Driven by 4K and higher cameras, denser number of cameras, sensor variety, and longer data retention times, the following transformations are happening in surveillance:

- Digital transformation of digital evidence
- Workforce transformation with 4K displays and precision desktops
- Security transformation with endpoint control, protection, and management

Today's surveillance is not just about video, it is about integrating video data with the data from all types of other sensors to paint a complete picture of events. Within the Dell Technologies IoT Division, we call this "mashing." For example, an oil rig must connect video data with data from other sensors, as well as business applications, and do so in real time. When a chemical detection sensor goes off at the same time as someone pushes a panic button, the customer must be able to send the right responder at the right time for the right reasons. Furthermore, all of this data should be stored in a data repository and analyzed holistically to discover insights that can have a significant and positive effect on the business or organization for long term decisions, as well as for compliance.

To handle all this volume and variety of streaming sensor data, customers are demanding enterprise-class surveillance solutions that not only have sufficient compute, storage, and network capacity, but also top-flight security, reliability, scalability, and overall system resilience. Linking all these demands under one solution is not a trivial task. Having it easy to deploy and understand how to recommend scaling is something that is very difficult to achieve. The Dell Technologies IoT Solution Division has years of experience in the surveillance market, with 20 to 30 years in core infrastructure design and build. With two global interoperability labs and certification teams, we stand ready to meet these demands.

Solution purpose

This reference architecture is intended to provide a high-level architecture for designing effective IoT surveillance solutions. This document focuses on a pre-integrated solution that provides a consistent foundation from edge to core to cloud, with a single management console for information technology and operational technology (IT/OT) convergence in an open, flexible architecture.

This solution represents an evolution in enterprise architectures for IoT and surveillance that includes storage, compute, networking, and software with key partnerships in the surveillance and IoT space. As a software-defined data center solution, it is engineered and tuned for real-world IoT and surveillance workloads, providing the only solution with designed-in security from camera to cloud that protects data and enables visibility of your surveillance devices.

As requirements change and become more sophisticated, the Dell Technologies IoT Solution | Surveillance architecture can be enhanced to meet any customer's individual needs. We pre-integrate, test, and validate the solution in the Dell EMC

Surveillance Lab using customer data, which helps customers reduce deployment risk, increase system reliability, reduce support costs and gain a proven, repeatable architecture.

CHAPTER 2

Key components

Introduction

Surveillance and Internet of Things (IOT) solutions have grown to the point that customers are looking for Enterprise-grade IT solutions to deliver management, security, and scale to IoT and surveillance deployments. Dell Technologies has been uniquely focused on addressing the surveillance and IoT market for over a decade with proven architectures and industry partnerships.

The Dell Technologies IoT Solution | Surveillance presents the next evolution in enterprise architectures for IoT and surveillance that includes many Dell innovations: storage, compute, networking, and software with key partnerships in the surveillance and IoT space.

Dell EMC ECS Object Storage

Dell EMC ECS is a complete software-defined cloud storage platform that supports the storage, manipulation, and analysis of video surveillance and unstructured data on a massive scale on commodity hardware. ECS is specifically designed to support the mobile, cloud, and Big Data workloads that are similar to large-scale workloads.

ECS provides UI, RESTful API, and CLI interfaces for provisioning, managing, and monitoring storage resources. Storage services provided by the unstructured storage engine (USE) ensure that video is available and protected against data corruption, hardware failures, and data center disasters. The USE enables global namespace management and replication across geographically dispersed data centers and enables the following storage services:

Object service

Enables you to store, access, and manipulate video and unstructured data. The object service is compatible with existing Amazon S3, Dell EMC Centera™ content addressable storage (CAS), and Atmos™ APIs.

Hadoop Distributed File System (HDFS)

Helps you use your ECS infrastructure as a Big Data repository against which you can run Hadoop analytic applications.

The provisioning service manages the provisioning of video surveillance storage resources and user access. Specifically, it handles user management, authorization, and authentication for all provisioning requests, resource management, and multitenancy.

You can scale up, scale out, and add users, applications, and services, as well as manage your local and distributed storage resources for your surveillance data through a single view.

Dell EMC CIFS-ECS

CIFS-ECS is a lightweight application that allows you to upload and download files to a Dell EMC ECS storage platform. It creates a Windows virtual drive to ECS cloud storage and transfers data from a Windows platform to an ECS using REST S3 API. CIFS-ECS is designed as an easy access to data in the cloud by allowing Windows applications to interface with an ECS storage server through standard file system APIs.

ECS combined with CIFS-ECS provides applications and users efficient access to content in the cloud from a Windows platform.

Dell EMC PowerEdge servers

Dell EMC PowerEdge™ servers are ideal for recording and managing terabytes of video from distributed locations.

PowerEdge 1U servers are used where external network-attached storage (NAS) clusters or block arrays are planned for surveillance storage.

PowerEdge 2U rack servers are used for local video storage where external surveillance storage is not used.

VMware vSphere

VMware vSphere is a virtualization platform that is used across thousands of IT environments around the world. VMware vSphere can transform or virtualize computer hardware resources, including CPU, RAM, hard disk, and network controller, to create a fully functional virtual machine (VM) that runs its own operating systems and applications like a physical computer.

The high-availability features of VMware vSphere coupled with VMware vSphere Distributed Resource Scheduler (DRS) and VMware vSphere Storage vMotion enable the seamless migration of virtual desktops from one ESXi server to another with minimal or no impact to the customer's usage.

VMware vSAN

VMware vSAN aggregates local or direct-attached data storage devices to create a single storage pool shared across all hosts in the vSAN cluster. vSAN eliminates the need for external shared storage, and simplifies storage configuration and virtual machine provisioning.

vSAN is a distributed layer of software included in the VMware ESXi hypervisor, and it is fully integrated with VMware vSphere. vSAN supports vSphere features that require shared storage, such as High Availability (HA), vMotion, and Distributed Resource Scheduler (DRS). VM storage policies enable you to define VM storage requirements and capabilities.

Each host in a vSAN cluster contributes storage to the cluster. These storage devices combine to create a single vSAN datastore. A hybrid vSAN cluster uses flash devices for the cache tier and magnetic drives for the capacity tier. creating a flash-optimized, resilient shared datastore designed for surveillance environments.

VMware vRealize Operations Manager

VMware vRealize Operations Manager delivers intelligent operations management with application-to-storage visibility across physical, virtual, and cloud infrastructures. Using policy-based automation, operations teams automate key processes and improve IT efficiency.

Using data collected from system resources (objects), vRealize Operations Manager identifies issues in any monitored system component, often before the customer notices a problem. vRealize Operations Manager also frequently suggests corrective actions you can take to fix the problem right away. For more challenging problems, vRealize Operations Manager offers rich analytical tools that allow you to review and

manipulate object data to reveal hidden issues, investigate complex technical problems, identify trends, or analyze to gauge the health of a single object.

VMware Pulse IoT Center

VMware Pulse IoT Center is a secure, enterprise-grade IoT device management and monitoring solution. Integrate, manage, monitor and secure IoT use cases from the edge to the cloud, bridge the gap between Information Technology and Operational Technology organizations and simplify IoT device management with Pulse IoT Center.

CHAPTER 3

Architectural overview

IOT engine architecture

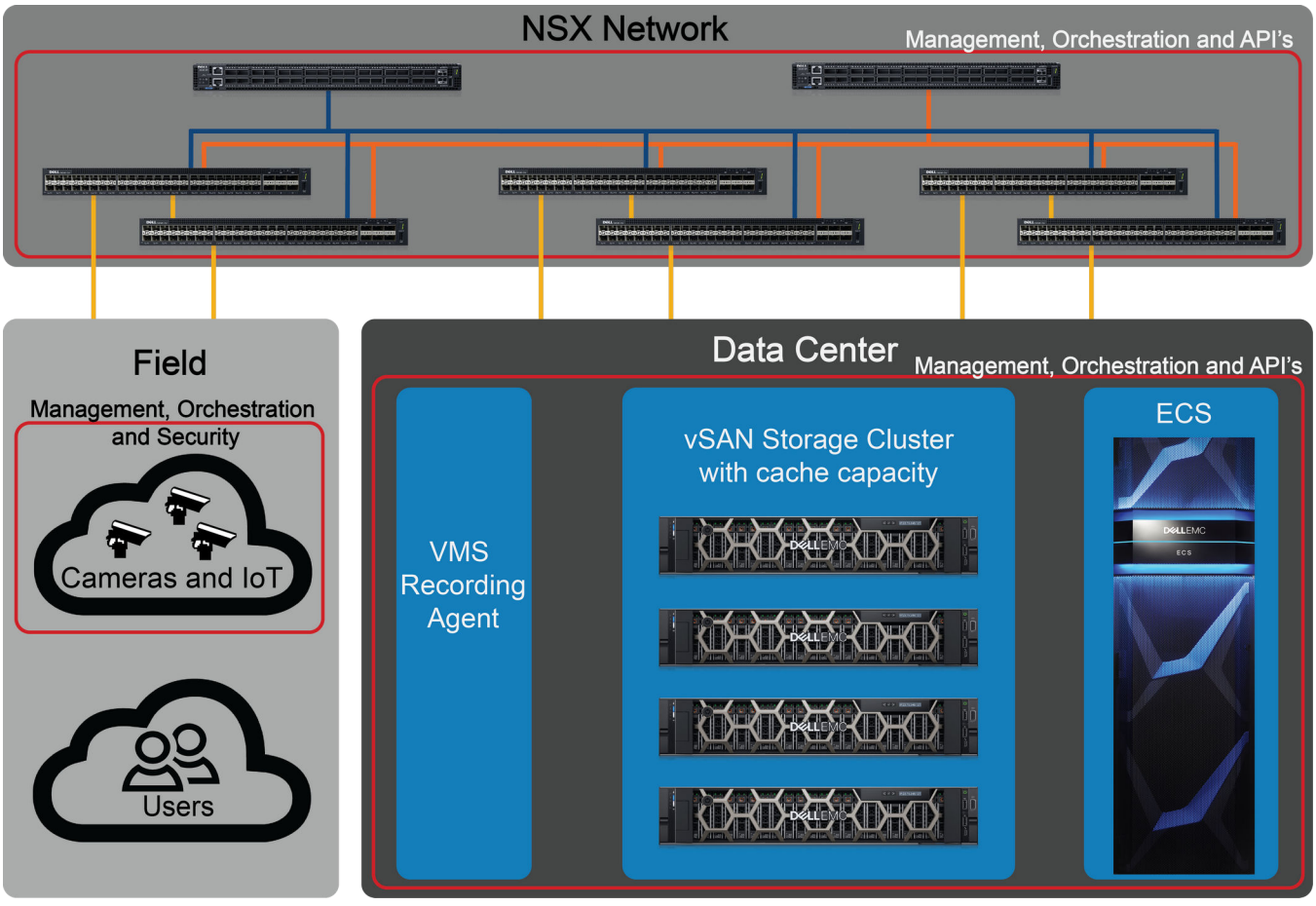
Dell Technologies has engineered a pre-integrated enterprise-class hyper-converged solution that provides a consistent foundation from edge to distributed core to cloud. The IoT surveillance solutions uses a full leaf-spine architecture that can span multiple networks to move distributed surveillance camera video from edge switches through a central switching infrastructure to distributed servers and storage.

VMware NSX provides the networking and security foundation for software-defined data center to protect data from camera to cloud, enabling the three key functions of micro-segmentation: isolation, segmentation, and segmentation with advanced services.

VMware Pulse enables management of IT/OT with a single console providing visibility of all devices, as well as facilitating over-the-air (OTA) updates for security patches.

ESXi Enterprise Plus enables High Availability (HA) and Distributed Resource Scheduler (DRS) to provide automatic monitoring and load balancing across all host servers.

Figure 1 Dell Technologies IoT Solution | Surveillance architecture



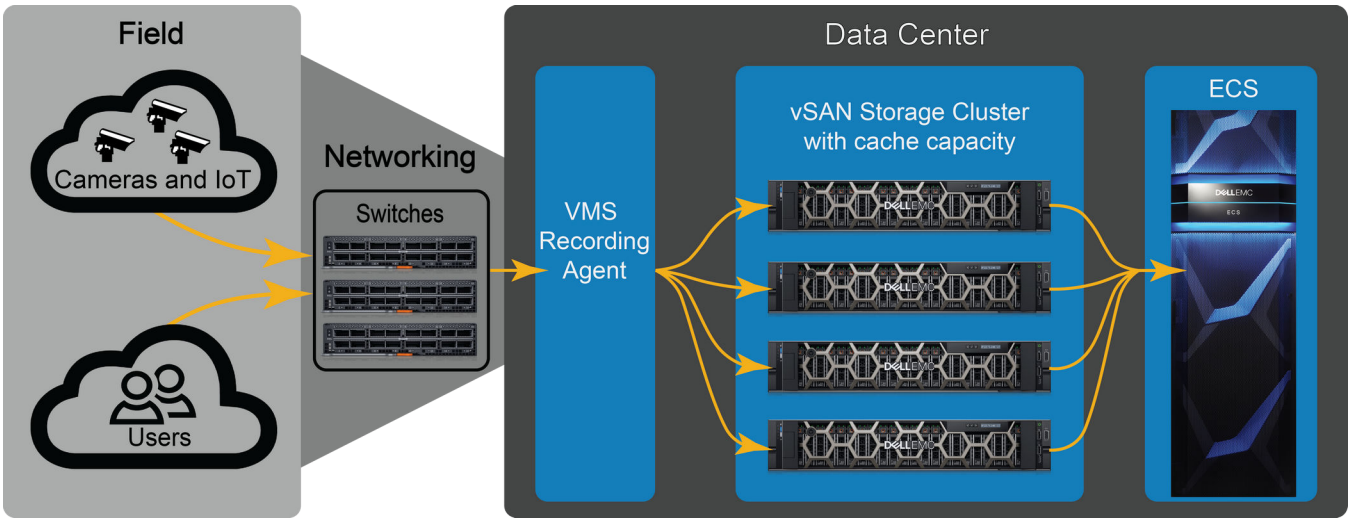
This solution provides an automated, fault-tolerant approach to scaling for private, on-premises, off-premises, or hybrid needs:

- Tier I storage: from 100 TB to 500 TB

- Tier II storage: from 500 TB to 50 PB
- Cameras: from 100 s to 1000 s of cameras/sensors

The following figure shows a two-tier implementation where the surveillance data traffic flow is using a vSAN storage cluster and ECS Object Storage.

Figure 2 Data flow in a Dell Technologies IoT Solution | Surveillance environment



The surveillance data flow is initiated at the edge with cameras and IoT sensors and initially flows through the network to the VMS Recording Agent. The VMS moves the surveillance data to the vSAN storage cluster. A more detailed description of the virtual appliance storage flow is provided later in this document.

CIFS-ECS then moves the surveillance files from the storage cluster to the ECS storage tier at regular intervals, providing one pool of storage that each VM can draw on for local provisioning. ECS stores the surveillance files until the file's full retention time has expired.

Replacing traditional physical servers and SAN with a software-defined data center provides an extensible framework for certain expansion in the future. Software-defined data centers also allow you to leverage the latest innovations in software-defined infrastructure.

vSAN overview

VMware vSAN is enterprise-class storage for Hyper-Converged Infrastructure (HCI). Included in the VMware vSphere hypervisor, vSAN delivers flash-optimized, secure storage.

vSAN is the first native HCI data-at-rest encryption solution and a highly available control plane that helps customers evolve their systems without risk. vSAN is designed to help customers modernize their infrastructure by addressing three key IT needs: higher security, lower costs, and faster performance. Stretched clusters provide resiliency with simplicity and lower costs against entire site failure compared to traditional stretched clustering solutions.

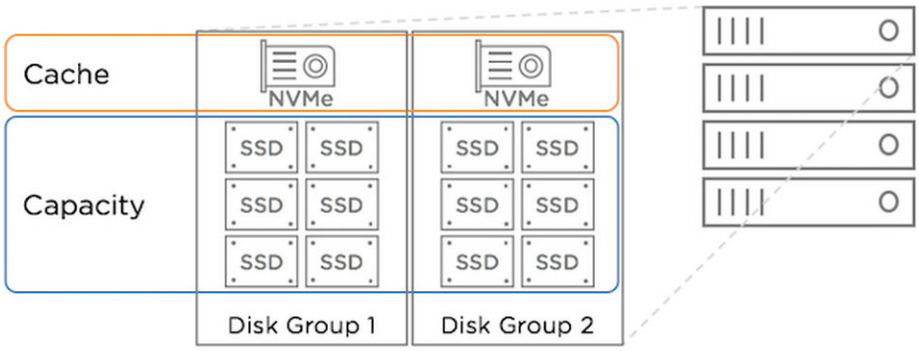
Servers with local storage

A wide variety of deployment and configuration options make vSAN a flexible and highly scalable HCI storage solution. A single vSAN cluster consists of any number of

physical server hosts from two to 64. Organizations can start with what is needed today and implement a "just-in-time" provisioning model for additional compute and storage capacity. Additional hosts can easily be added to an existing cluster in a matter of minutes. This method of purchasing, expanding, and refreshing an IT infrastructure is more efficient and less costly than provisioning large "blocks" of capacity every few years.

Each host contains flash devices (all-flash configuration) or a combination of magnetic disks and flash devices (hybrid configuration) that contribute cache and capacity to the vSAN distributed datastore. Each host has one to five disk groups. Each disk group contains one cache device and one to seven capacity devices, as shown in the following figure.

Figure 3 vSAN storage cluster

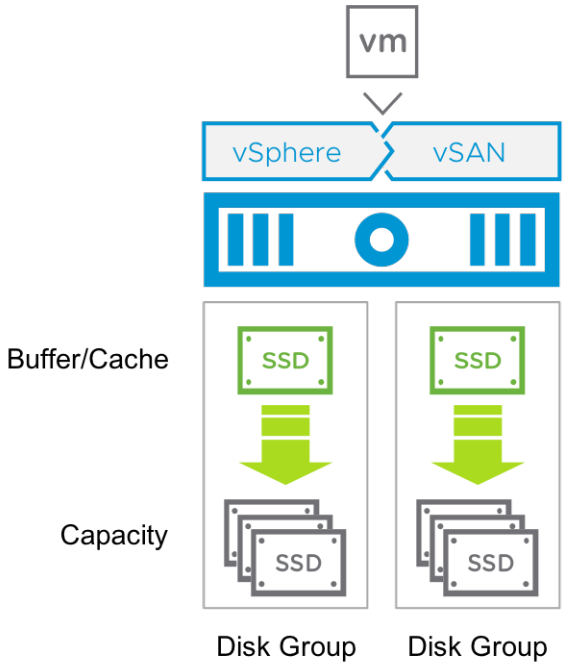


In all flash configurations, the flash devices in the cache tier are used for buffering writes. There is no need for read cache as performance from the capacity flash devices is more than sufficient. Two grades of flash devices are commonly used in an all-flash vSAN configuration: Lower capacity, higher endurance devices for the cache layer; more cost effective, higher capacity, lower endurance devices for the capacity layer. Writes are performed at the cache layer and then destaged to the capacity layer, as needed. This helps maintain performance while extending the usable life of the lower endurance flash devices in the capacity layer.

In hybrid configurations, one flash device and one or more magnetic drives are configured as a disk group. A disk group can have up to seven drives for capacity. One or more disk groups are used in a vSphere host depending on the number of flash devices and magnetic drives contained in the host. Flash devices serve as read cache and write buffer for the vSAN datastore while magnetic drives make up the capacity of the datastore. vSAN uses 70 percent of the flash capacity as read cache and 30 percent as write cache.

The following figure shows the disk configuration in a vSAN hybrid storage cluster.

Figure 4 vSAN hybrid storage cluster



VMware is always looking for ways not only to improve the performance of vSAN but to improve the consistency of its performance so that applications can meet their service level requirements. vSAN 6.7 continues this drive for better performance and consistency through optimizations made in the data path.

vSAN 6.7 optimizes the destaging mechanism, resulting in data that drains more quickly from the write buffer, to the capacity tier. The ability to destage this data more quickly allows for the buffer tier to be available to accept new incoming I/Os, which will reduce periods of congestion.

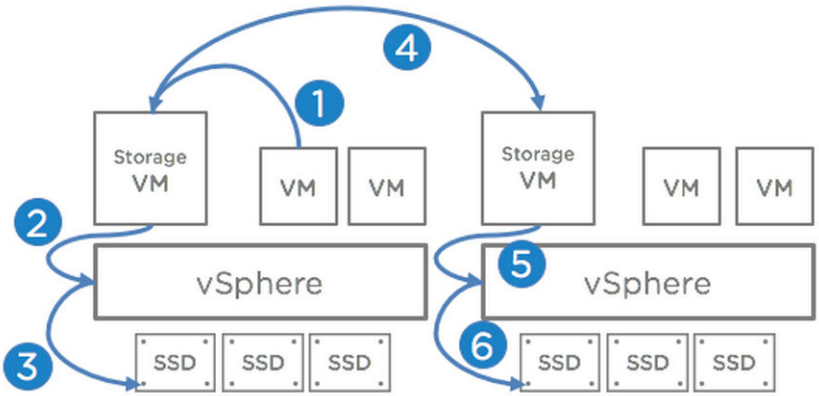
Storage Controller Virtual Appliance Disadvantages

Storage in an HCI requires computing resources that have been traditionally offloaded to dedicated storage arrays. Nearly all other HCI solutions require the deployment of storage virtual appliances to some or all hosts in the cluster. These appliances provide storage services to each host. Storage virtual appliances typically require dedicated CPU or memory, or both, to avoid resource contention with other virtual machines.

Running a storage virtual appliance on every host in the cluster reduces the overall amount of computing resources available to run regular virtual machine workloads. Consolidation ratios are lower and total cost of ownership rises when these storage virtual appliances are present and competing for the same resources as regular virtual machine workloads.

Storage virtual appliances can also introduce additional latency, which negatively affects performance. This is due to the number of steps required to handle and replicate write operations as shown in the following figure.

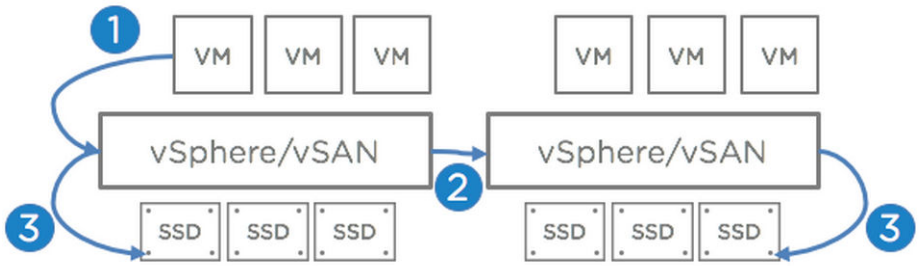
Figure 5 Virtual appliance storage flow



vSAN is included in the vSphere Hypervisor

vSAN does not require the deployment of storage virtual appliances or the installation of a VMware vSphere Installation Bundle (VIB) on every host in the cluster. vSAN is included in the vSphere hypervisor and typically consumes less than 10 percent of the computing resources on each host. vSAN does not compete with other virtual machines for resources and the I/O path is shorter, as shown in the following figure.

Figure 6 vSAN resource flow



A shorter I/O path and the absence of resource-intensive storage virtual appliances enables vSAN to provide excellent performance with minimal overhead. Higher virtual machine consolidation ratios translate into lower total costs of ownership.

vSAN cluster

A standard vSAN cluster consists of a minimum of three physical nodes and can be scaled to 64 nodes. All the hosts in a standard cluster are commonly located at a single location and are well-connected on the same Layer-2 network. You must use 10 Gb network connections for all-flash configurations, and we recommend using them for hybrid configurations.

vSAN Witness Host

It is important to understand the use of a vSAN Witness Host in 2-node and stretched cluster vSAN deployments. This vSAN Witness Host stores metadata commonly called "witness components" for vSAN objects. Virtual machine data such as virtual disks and virtual machine configuration files are not stored on the vSAN Witness Host. The

purpose of the vSAN Witness Host is to serve as a "tie-breaker" in cases where sites are network isolated or disconnected.

A vSAN Witness Host may be a physical vSphere host, or a VMware provided virtual appliance, which can be easily deployed from an OVA. When using a physical host as a vSAN Witness Host, additional licensing is required, and the host must meet some general configuration requirements. When using a vSAN Witness Appliance as the vSAN Witness Host, it can easily reside on on another or an existing vSphere infrastructure, with no additional need for licensing.

When using 2 Node clusters for deployments, such as remote office branch office (ROBO) locations, it is a common practice for vSAN Witness Appliances to reside at a primary data center. They may be run at the same ROBO site but require additional infrastructure at the ROBO site.

vSAN Witness Hosts providing quorum for stretched clusters can only be located in a tertiary site that is independent of the preferred and secondary stretched cluster sites.

One vSAN Witness Host is required for each 2-node or stretched cluster vSAN deployment.

Bandwidth requirements to the vSAN Witness Host are determined by the number of vSAN components on a cluster. During failover scenarios, ownership of vSAN components must be moved to the surviving site over a five-second period. The rule of thumb is 2 Mb/s for every 1,000 vSAN components. Maximum latency requirements to and from the vSAN Witness Host depend on the number of hosts in the cluster. Two node configurations are allowed up to 500 milliseconds (ms) and stretched clusters are allowed 200 milliseconds (ms) or 100 milliseconds (ms) depending on the number of hosts in the stretched cluster.

We recommend using the vSAN Witness Appliance as a better option for the vSAN Witness Host than using a physical vSphere host. The use of a vSAN Witness Appliance is relatively low during normal operations. It is not until a failover process occurs that a vSAN Witness Host will have any significant utilization. Because of this, especially in large 2 Node deployments to ROBO sites, you can run multiple vSAN Witness Appliances on the same shared vSphere infrastructure. VMware supports running the vSAN Witness Appliance on any VMware vSphere 5.5 or higher infrastructure, which can include a standalone ESXi host, a typical vSphere infrastructure, in OVH (the service formally known as vCloud Air), any vCloud Air Network Partner, or any service provider, shared, or co-location where vSphere is used.

When using a vSAN Witness Appliance, you can patch it in the same way as any other ESXi host. It is the last host updated when performing 2 Node and Stretched Cluster upgrades and should not be backed up. If it becomes corrupted or deleted, it should be redeployed. vSAN 6.6 introduced a quick and easy wizard to change the associated vSAN Witness Host.

The Change Witness Host is available in the vSphere Web Client and the vSphere Client based on the Clarity UI framework.

CHAPTER 4

Conclusion

Summary

Dell Technologies IoT Solution | Surveillance is enabled by Dell EMC storage arrays and VMware vSAN These hyper-converged solutions are purpose-built for demanding, multi-sense surveillance, such as video, sound, and barometric pressure. The IoT solutions include both hardware and software.

This document focuses on a pre-integrated solution that delivers a consistent foundation from edge to distributed core to the cloud, in an open, flexible architecture, providing the only solution with designed-in security from camera to cloud that protects data and enables visibility of your surveillance devices.

By pre-integrating, testing and validating the solution in our labs using customer data customers can reduce deployment risk, increase system reliability, reduce support costs and gain a proven, repeatable architecture.

As requirements change and become more sophisticated, Dell Technologies IoT Solution | Surveillance architectures can be enhanced to meet any customer's individual needs.