Dell Technologies IoT Solution | Safety & Security with Genetec Security Center Sizing Guide

H17436.2

Abstract

The purpose of this guide is to help you understand the benefits of using a Dell Technologies Solution | Safety & Security with Genetec Security Center 5.7. Use this guide to determine the requirements for a successful Genetec Security Center installation.

Dell Technologies Solutions

Dell Technologies
Safety & Security Lab
Validated

Genetec

December 2018

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Introduction

This chapter provides information on the purpose and scope of this solution.

Topics:

Solution overview

The purpose of this guide is to help you understand the benefits of using a Dell EMC storage solution with Genetec Security Center V6.10.08. The solution includes both hardware and software elements for video safety and security.

Use this guide to determine the requirements for a successful Genetec Security Center installation. The storage platforms include VMware ESXi hosts that are running Genetec Security Center. This paper also includes information on VMware virtualization.

Scope

This guide is intended for use by internal Dell EMC sales and pre-sales personnel, and qualified Dell EMC and Genetec partners.

The guidelines presented are for storage platform positioning and system sizing. The sizing recommendations are based on performance and storage protocol conclusions derived from Dell EMC testing.

The guidelines for sizing this video storage solution describe the use of the following storage platforms:

- Dell EMC ECS Object Storage
- VMware vSAN

These guidelines include the following design considerations:

- Bandwidth recommendations for Genetec Security Center 5.7 and higher when they are attached to specific Dell EMC storage systems
- Architectural overview of Genetec Security Center
- Dell EMC storage considerations for Genetec Security Center
- Result summaries for the tests carried out by Dell EMC engineers in a VMware ESXi virtualized infrastructure

Use this guide to determine the best practices for the following:

- Number of Archivers per vSAN node
- ECS sizing
- GeoDrive configuration

NOTE: All performance data contained in this report was obtained in a rigorously controlled environment. Network topology and system environment variables can have significant impact on performance and stability. Follow the best practices as outlined in the *Dell EMC Storage with Genetec Security Center: Configuration Guide* regarding network and storage array configuration. Server and network hardware can also affect performance. Performance varies depending on the specific hardware and software, and might be different from what is outlined here. Performance results will be similar if your environment uses similar hardware and network topology.

Key objectives

The configurations documented in this guide are based on tests conducted in the Dell EMC Safety & Security Lab and actual production implementations.

These are the key objectives of this solution:

- Measure the sizing needs for specific system requirements so that an implementation can be correctly sized and the appropriate Dell EMC products can be matched to a customer's requirements.
- Calculate maximum bandwidths.
- Describe validated disk drive types.
- Illustrate lab controlled failures, such as disk rebuilds, and network path failures.

2

Solution components

This chapter provides information about storage options for video and audio data.

Topics:

Dell EMC storage

Dell EMC storage arrays are ideal for storing video and audio data.

This guide describes the tests for the following storage arrays:

- ECS Object Storage

Storage protocols

Dell EMC uses standard file protocols to enable users and applications to access data that is consolidated on a Dell EMC storage solution.

This guide provides information about these network protocols:

- S3

Genetec Security Center

A Genetec Security Center installation can consist of a single server or multiple servers in a hierarchical structure.

You can configure Security Center to handle anything from a few cameras to several thousand cameras.

NOTE: Security Center 5.5 is not supported. The Dell EMC Safety & Security Lab has validated Security Center versions up to 5.4 and Security Center 5.6 or later.

The following table describes two primary Security Center services.

Table 1. Security Center primary services

Service	Description
Archiver	Security Center records video through the Archiver service. The Archiver is responsible for dynamic discovery and status polling of units. This is where all video and multimedia streams are processed and committed to storage. "Archiving" is the term used for storing video.
Directory	The Directory is the main server application whose service is required to provide a centralized catalog for the other Security Center services and applications on the system. From the Directory, applications can review and establish connections, and receive centralized configuration information.

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.

3

Configured components

This chapter provides information about the components configured in this solution.

Topics:

Dell EMC IoT Solution | Safety & Security environment

The Dell EMC Safety & Security Lab recommends the following base configuration for a successful implementation:

Virtualized environment	• 8 vCPUs • 16 GB memory • Network adapter type: VMXNET3 (GbE and 10 GbE)
R740xd vSAN Ready node (vSAN certified storage)	• Dual Intel Xeon gold 6126 2.6G, 12C/24T • 192 GB memory • 10x 3.84 TB SSD SAS Read Intense • 2x 800 GB SSD SAS Write Intense • Intel X710 Quad Port 10 Gb DA/SFP+ Ethernet, Network Daughter Card

vSAN cluster	• 4 R740xd vSAN Ready nodes
	• 40 total capacity drives
	• 8 Disk Groups (1 vSAN cache to 5 capacity SSD_
	• 10 GbE NIC connections for:
	  ○ vSAN
	  ○ Administration
	  ○ vMotion
	  ○ vSAN Managment

Management cluster	• 4 R440 vSAN Ready nodes
	• 128 GB memory
	• 5 1.92 TB cluster drives
	  ○ 1 flash cache drive
	  ○ 4 storage drives

Switching	• Dual DellS4048s (leaf) vSAN cabinet: vSAN, vMotion, Camera/User • DualDell Z9100s network core (spine) - optional
External storage	• ECS U4000 • 8 node with 60 drives per node
Supporting Servers	• Review stations: Dell PowerEdge servers - various models • Work stations: Dell Precision - various models

Refer to the following network and design guides for more information on configuring vSAN for your environment, or contact ProDeploy Plus for vSAN configuration assistance:

- VMware Storage and Availability Technical Documents
- VMware vSAN Design and Sizing Guide
- VMware vSAN Network Design

All storage and server tests are conducted using 10 GbE NICs unless otherwise noted.

For all the tests, the virtual CPU (vCPU), memory, and network were configured according to Genetec best practices. The VMware vSphere configuration was in accordance with the VMware Compatibility Guide (www.vmware.com/resources/compatibility/search.php).

The Dell EMC Safety & Security Lab's host hardware met and exceeded the minimum system requirements for an ESXi/ESX installation. The Genetec Archiver VM was running on an ESXi 6.0 host using Cisco UCS B230 Blade Servers, and various Dell EMC servers, such as the Dell EMC FC630s, FC430s, and R730xd. For more information about VM configuration, see the General recommendations for storage and sizing section of the *Using EMC VNX storage with VMWare VSphere* guide.

Dell EMC ECS Object Storage

Dell EMC ECS is a complete software-defined cloud storage platform that supports the storage, manipulation, and analysis of safety and security video 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 safety and security video 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 safety and security 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.

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.

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.

4

Sizing the solution

This chapter provides information to enable you to quickly determine the correct storage array based on your customer's bandwidth requirements.

Topics:

Overall bandwidth and capacity guidelines

The test results are based on a model in which the constant-bandwidth safety and security video traffic remained unaffected during select storage failure scenarios, such as disk rebuild, node failures, and failing network paths.

The following table provides bandwidth-sizing guidelines based on the desired number or recorders. The table begins with 16 recorders, as the IOT solution requires a minimum of 4 vSAN nodes.

Table 2. Bandwidth sizing guidelines

Number of recorders	Nodes required		Bandwidth (MB/s)	
	vSAN	ECS	Per recorder	Total
16	4	8	37.5	600
20	5	10	37.5	750
24	6	12	37.5	900
28	7	14	37.5	1050

The following table provides capacity guidelines based on our test results.

Table 3. Capacity sizing details

Disks per vSAN node	Disk type	Disk Size	No. of disks	Storage policy [a] (RAID)	Usable space		Retention time [b]
					Per VSAN Node	Per recorder [c]	
Minimum number	SSD	4 TB	10	5	18 TB	4.25 TB	31 Hours
Maximum number	SSD	4 TB	24	5	40 TB	10 TB	3 days

a. Defines the number of host and device failures that a virtual machine object can tolerate, including using RAID 5 or RAID 6.
b. In local cache at 37.5 MBps write BW
c. Four Recorders per node

Dell EMC ECS

The test results are based on a model in which the constant-bandwidth safety and security video traffic remained unaffected during select storage failure scenarios, such as disk rebuild, node failures, and failing network paths.

We performed all tests with disk drive failures, node failures, storage process failures, or NIC failures to ensure a worst-case scenario for all sizing parameters.

Genetec Archivers use a default file size of 500 MB. While using the default file size we observed spikes in the ECS upload bandwidth. Reducing the file size to 100 MB provides a constant upload bandwidth to ECS.

Dell EMC recommends:

- Using SSD, 10k, or 15k rpm SAS drives for the GeoDrive cache disks.
- Calculating drive space requirements for local disk and ECS buckets based on the retention times used.

The following table provides bandwidth-sizing guidelines based on our test results.

Table 4. Dell EMC ECS Object Storage test results

Cluster	ECS Version	Archivers per node	Bandwidth (MB/s)		No. drives/ ECS node	ECS node drives	
			Archiver	Node		Size	Type
ECS U4000	3.2.0.0	1	37.5	37.5	30	8 TB	NL-SAS
		2	37.5	75	30	8 TB	NL-SAS
		3	26	78	30	8 TB	NL-SAS
		4	20	80	30	8 TB	NL-SAS

VMware vSAN

The test results are based on a model in which the constant-bandwidth safety and security video traffic remained unaffected during select storage failure scenarios, such as disk rebuild, node failures, and failing network paths.

Dell EMC recommends:

- Keep some RAM (16GB) for the virtualization OS
- Do not run more than 6 VMs total
- Do not exceed VM designs above 1200 Mbps per server

The following table provides bandwidth-sizing guidelines based on our test results.

Table 5. Dell EMC ECS Object Storage test results

Server node	VMware version	Archivers per node	Disk groups	Bandwidth (MB/s)		No. capacity drives/ VMware node	ECS Node Drives		Max. drive (usable)
				Archiver	Node		Size	Type	
PowerEdge R740xd Ready Node	6.7	1	2-4	37.5	37.5	10-24	3.8 TB	NL-SAS	70-170 [a]
		2	2-4	37.5	75	10-24	3.8 TB	NL-SAS	
		3	2-4	37.5	112.5	10-24	3.8 TB	NL-SAS	
		4	2-4	37.5	150	10-24	3.8 TB	NL-SAS	

a. Usable drive size varies depending on configuration.

5

Testing and validation

This chapter describes the testing used to validate this solution.

Topics:

Test objectives

Many factors must be considered when designing your solution.

The Dell EMC Safety & Security Lab tests focus on storage-related factors with the following objectives:

- Determine best video storage performance requirements for use with:
  - ECS Object Storage
- Determine the maximum bandwidth with multiple Archivers.
- Determine all factors with a lab-controlled failure, such as rebuilding disks, or network path failures.

Test parameters

All test parameters and scenarios reflect standard production behavior for Genetec Security Center under storage-intensive conditions, including typical storage functions and failures. We followed best practices for recovery and break-fix issues for normal situations that might arise in a standard production environment.

We used the following parameters to perform the tests:

- The IP network (Layer 2) is a flat, high-availability network with plenty of capacity, which enabled us to focus on the products we were testing.
- All tests assumed uniform distribution of bandwidth from the Genetec Archiver.

Tests conducted

We ran tests with the SmartConnect™ configuration in place and the SMB shares were mounted using the SmartConnect zone name.

Video playback test

As video is being written to the storage, video is simultaneously recalled or reviewed at a rate equal to 20 percent of the write rate. Tests are run with the SmartConnect™ configuration in place and the SMB shares are mounted using the SmartConnect zone name.

The review did not affect the write rate, video quality, or result in dropped video.

Disk group failure test

A single disk failure is the most common failure affecting storage systems today. When a disk fails, that disk is removed and replaced. The replacement disk is then reconstructed.

For the test, disk failure scenarios were induced and the data rebuild to the hot spare disks was observed with effect to write bandwidth. There was no video data loss during recovery.

Disk failure test with ECS

A single disk failure is the most common failure affecting storage systems today. When a disk fails, that disk is removed and replaced. The replacement disk is then reconstructed.

ECS employs a hybrid model of triple mirroring data, metadata, and indexing. Erasure coding is also used for enhanced data protection and reduction of storage overhead. For data integrity, ECS uses checksums.

When the system labels a drive as `FAILED`, the data protection logic rebuilds the data on that drive on other drives in the system. The `FAILED` drive no longer participates in the system in any way. ECS requires a minimum of four nodes to be able to conduct the default erasure coding and six nodes for the cold archive option.

The disk rebuild operation did not affect the write rate, video quality, or result in dropped video.

NIC failure test with ECS

The ECS hard NIC failure test removes one NIC cable from the active node that was involved in active recording to simulate the NIC failure scenario.

The Dell EMC Safety & Security Lab uses two 10 GbE, 24-port or 52-port Arista switches that are used to transfer data to and from customer applications as well as internal node-to-node communications. These switches are connected to the ECS nodes in the same rack and employ the Multi-Chassis Link Aggregation (MLAG) feature, which logically links the switches enabling active-active paths between the nodes and customer applications. This configuration results in higher bandwidth while preserving resiliency and redundancy in the data path. Any networking device supporting static LAG or IEEE 802.3ad LACP can connect to this MLAG switch pair. Because the switches are configured as MLAG, these two switches appear and act as one large switch.

The NIC failure tests did not affect the write rate, video quality, or result in dropped video.

Node poweroff test

An unexpected single node hard failure was simulated, which causes the servers that were writing to that node to reconnect to a new node.

Server rebalancing is based on the rules of the HA cluster that the vSAN nodes are a member of. When a vSAN node is failed, the Archivers running on that node are rebooted across the remaining three nodes.

Initially, the four Archivers run across three nodes. Upon recovery of the failed node, VMware vSphere vMotion can then rebalance the cluster.

Node poweroff test with ECS

ECS employs a hybrid model triple mirroring data, metadata, and indexing. Erasure coding is also used for enhanced data protection and reduction of storage overhead.

Erasure coding provides enhanced data protection from a disk or node failure that is storage efficient as compared to conventional protection schemes. The ECS storage engine implements the Reed Solomon 12+4 erasure-coding scheme, in which a chunk is broken into 12 data fragments and 4 coding fragments for parity. These 16 fragments are then dispersed across nodes at the local site. The data and coding fragments for each chunk are equally distributed across nodes in the cluster. For example, with 8 nodes, each node stores 2 of the 16 fragments. The storage engine can then reconstruct a chunk from any 12 fragments of the original 16.

One of the ECS nodes was manually shutdown. The GeoDrive tool load balanced the traffic across all the available nodes and the recorders bypassed the failed node. The node failure did not affect the write rate, video quality, or result in dropped video.

WARNING:

If running a mixed workload, these changes can adversely affect the other workloads that might be present on the cluster.

Node reboot test with ECS

One of the ECS nodes was manually restarted to simulate a node reboot. The GeoDrive tool load balanced the traffic across all the available nodes and the recorders bypassed the failed node. The node reboot did not affect the write rate, video quality, or result in dropped video.

Storage bandwidth and configuration

The purpose of the storage bandwidth test was to evaluate video storage and its application to the various Dell EMC storage arrays and nodes.

About this task

Additional tests evaluated ESXi host hardware in relationship to virtual CPU settings and the resulting bandwidths.

During all the tests, we assumed that Genetec Security Center is correctly configured according to Genetec's best practices and operates within the bandwidth, camera count, and other Genetec parameters.

Steps

1. Configured video storage for a Dell EMC storage system.
2. Configured Genetec Archivers
3. Set up camera simulators (traffic generators) to produce a traffic load to each Genetec Archiver at the desired bandwidth.
4. Verified that motion detection was in the **On** state for all cameras.
5. Evaluated the network and video storage to ensure an error-free environment at the induced bandwidth.
6. Introduced storage device errors including:
   - NIC failures with active/active and active/passive configurations
   - Disk failures
   - Node failures
7. Captured the storage system and host statistics.
8. Based on the test results:
   - If no issues were detected, incremented the bandwidth.
   - If issues were detected, decreased the bandwidth.

   This procedure was repeated until the maximum error-free bandwidth was determined.

Results

Archivers for the storage protocol to be tested (FC, iSCSI, SMB2).

The test results associated with the previous procedure, for each tested Dell EMC storage array or cluster, are presented in *Dell EMC Storage with Genetic Security Center Configuration Guide*. The test results provide information about the maximum expected bandwidth per array or node, the disk configuration, as well as recommendations for various configuration parameters derived from extensive testing.

6

Conclusion

This chapter summarizes the testing for this solution.

Topics:

Summary

The Dell EMC Safety & Security Lab performed comprehensive testing with Genetec Security Center against ECS Object Storage and VMware vSAN.

Depending on the implementation needs, you can use Dell EMC storage for Genetec Security Center.

The Genetec architecture and product suite allows extreme scaling from a few cameras to tens of thousands of cameras using Dell EMC storage.

ECS storage

Dell EMC ECS is a software-defined, cloud-scale, object storage platform that combines the cost advantages of commodity infrastructure with the reliability, availability and serviceability of traditional arrays. With ECS, any organization can deliver scalable and simple public cloud services with the reliability and control of a private-cloud infrastructure.