Dell EMC Storage with Genetec Security Center

Surveillance

January 2019

H13495.12

Sizing Guide

Abstract

The purpose of this guide is to help you understand the benefits of using a Dell EMC storage solution with Genetec Security Center 5.7. Use this guide to determine the requirements for a successful Genetec Security Center installation.

Dell EMC Solutions

Dell EMC Surveillance Lab Validated

Genetec

DELL EMC

Published January 2019

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL 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 DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

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

CONTENTS

CHAPTER 1

Introduction

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

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 surveillance.

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.

This document discusses Genetec Security Center. Security Center is a superset of Omnicast, although Omnicast is indirectly discussed because it is the video recording engine for Security Center.

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 Isilon®
- Dell EMC Unity®
- Dell EMC SC series®
- Dell EMC PowerEdge®
- Dell EMC ECS® Object Storage

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 Genetec Archivers
- Mix of nodes and Genetec Archivers based on the expected bandwidth in an Isilon implementation
- Mix of nodes and Genetec Archivers based on the expected bandwidth in an ECS implementation
- Storage using Fibre Channel (FC) and Internet SCSI (iSCSI) on Unity and SC series systems
- Storage using Server Message Block (SMB) on Isilon systems
- Load factors related to the use of Dell EMC storage arrays in the customer's solution

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 Surveillance 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.
- Recommend an Isilon SMB configuration.
- Calculate node maximum bandwidths.
- Recommend disk drive types.
- Determine the Archiver service's maximum bandwidth to specific Dell EMC storage arrays and clusters.
- Confirm the previous test results with lab controlled failures, such as disk rebuilds, node removals, and network path failures.

CHAPTER 2

Solution components

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

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:

- Isilon clusters
- Unity arrays
- SC series arrays
- ECS Object Storage
- PowerEdge servers

For our testing, we used both single and dual storage processors for the full range of Unity and SC series storage arrays and single- and multi-node performance testing on the Isilon storage array.

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:

- FC
- iSCSI
- SMB (CIFS)
- 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 Surveillance 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

Table 1 Security Center primary services (continued)

Service	Description
	applications on the system. From the Directory, applications can review and establish connections, and receive centralized configuration information.

Releases tested

The following table lists the Genetec Security Center releases used for our tests.

Table 2 Genetec Security Center releases

VMS	Release
Genetec Security Center	5.7 SR1, SR2, SR3, SR4
	5.6 SR3
	5.4 SR2,
	5.3 GA, SR4 plus hot fix
	5.2 SR8

RSA SecurID

This section describes the security benefits of RSA® SecurID®. In this solution, is installed with an RSA-secured domain, increasing Windows and Security Center security.

RSA authentication uses constantly changing RSA tokens to enhance the user's Security Center experience by providing a single login structure for accessing multiple Security Center applications.

RSA SecurID two-factor authentication

RSA SecurID two-factor authentication is based on something you know, a password or personal identification number (PIN), and something you have, an authenticator.

This combination provides much more reliable user authentication than reusable passwords alone.

To access resources protected by the RSA SecurID system, users combine their secret PIN with the codes generated by their RSA SecurID authenticators. The result is a unique, one-time-use passcode that is used to positively identify, or authenticate, the user. If the RSA SecurID system validates the code, the user is granted access to the protected resource. If it is not recognized, the user is denied access.

RSA SecurID two-factor authentication is based on something you know -a password or personal identification number (PIN) -and something you have-an authenticator.

RSA SecurID appliance

The RSA SecurID Appliance includes the RSA Authentication Manager, the engine behind the industry-leading two-factor user authentication technology, in an integrated, rack-mountable hardware appliance.

Used with RSA SecurID authenticators, the RSA SecurID Appliance validates the identities of users before granting access to critical company resources. Additionally, the system logs all transactions and user activities, allowing administrators to use it as an auditing, accounting, and compliance tool.

With quick setup times, a web-based management interface, streamlined credential deployment, and user self-service, you can gain greater cost savings and improved security.

RSA, Active Directory, and DNS must be integrated before integrating with Security Center.

Credentialing methods

The RSA SecurID Appliance supports authenticators in a variety of form factors.

From the traditional hardware authenticators to software-based authenticators that install on PCs and smart phones to the SecurID On-demand Authenticator that delivers one-time codes using Short Message Service (SMS) or email. All of these credentials are centrally managed from a common interface.

Deployment and maintenance

The RSA SecurID Appliance is designed so that a customer can be up and running in as little as 30 minutes.

The built-in web server and web-based GUI provide access to the straightforward setup and management console from any web browser.

In addition to the primary setup, common tasks manageable through the web interface include:

- Adding users and assigning authenticators
- Installing and configuring agents
- Viewing the activity monitor
- Specifying the location of backup files

Native LDAP integration enables the RSA SecurID Appliance to point to a single authoritative data store in real time for user and group information. Both the Base and Enterprise editions of the RSA Authentication Manager software include RSA Credential Manager. The RSA Credential Manager is a completely integrated software module that enables user self-service (Base and Enterprise) and workflow provisioning (Enterprise only) to dramatically speed the onboarding of users to their credentials.

CHAPTER 3

Configured components

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

Dell EMC Surveillance Lab test environment

The Dell EMC Surveillance Lab is constantly being upgraded to the most recent software releases.

In order to test this solution, the Dell EMC Surveillance Lab was configured as follows:

Virtualized environment:

- 8vCPUs
- 16 GB memory
- Network adapter type: VMXNET3 (GbE and 10 GbE), E1000, or VMXNET2 (GbE only)
- Isolated VLAN for storage (if not FC)

Physical/Baremetal minimum environment:

- 8 Cores
- 32 GB memory

Network environment:

- Network adapter type: 10 GbE
- Camera user VLAN
- Storage VLAN

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). Microsoft MPIO is recommended for use with Unity and SC series arrays.

The Dell EMC Surveillance 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 6.5 host using Dell EMC PowerEdge servers. 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.

Watermarking and motion detection require additional vCPU and memory.

Isilon clustered storage system

Isilon NAS was designed and developed specifically for storing, managing, and accessing digital content and other unstructured data.

An Isilon clustered storage system is composed of three or more nodes. Each node is a self-contained, rack-mountable device that contains industry-standard hardware such as disk drives, CPUs, memory, and network interfaces. These nodes are integrated with the proprietary Isilon OneFS™ operating system, which is a distributed networked file system that unifies a cluster of nodes into a single shared resource.

Data protection

OneFS does not rely on hardware-based RAID for data protection. The Isilon system uses the Reed-Solomon algorithm for N+M protection with Forward Error Correction (FEC).

Protection is applied at the file level, enabling the cluster to recover data quickly and efficiently. Nodes, directories, and other metadata are protected at the same or a higher level as the data blocks they reference. Since all data, metadata, and FEC blocks are spread across multiple nodes, dedicated parity drives are not required. For more information about Isilon data protection, see *Dell EMC Isilon OneFS: A Technical Overview*.

Although cluster sizes as small as three nodes are possible, for surveillance applications we recommend a minimum of five nodes. Sizing calculations need to include a minimum free space calculation for proper cluster sizing. We recommend a cluster size that enables a node to be removed while retaining a minimum of 10 percent free space in the remaining capacity. This cluster size ensures that node removal and node failures have minimal or no impact on video ingestion.

The Isilon sizing tool provides an accurate calculation. You can find this tool at https://isilon-sizing-tool.herokuapp.com. Other sizing tools from video management software (VMS) and camera vendors may also be used for sizing the necessary bandwidth and storage capacity.

Cluster size

We recommend a minimum cluster size of five nodes, even if you are not writing to all of them. For example, if you are implementing a four-node Archiver solution, implement a five-node cluster. This also meets the recommended best practices for data protection.

To estimate the ideal number of nodes in a cluster, you need to consider cluster bandwidth and capacity.

Sizing by bandwidth

We recommend a cluster size with one or more additional nodes than calculated in bandwidth sizing. This ensures that failover of a node allows for redistribution of NAS connections and avoids any frame loss.

Sizing by aggregate capacity

We recommend a cluster size with enough usable capacity to handle 110 percent of the calculated space requirement, with a minimum added capacity of one full node plus 10 percent. The values are based on camera bit rate.

The Isilon sizing tool can use both the sizing by bandwidth and sizing by aggregate capacity methods when calculating ideal cluster size.

Dell EMC Unity and Dell EMC SC series

Dell EMC Unity and Dell EMC SC series storage arrays are ideal for recording and managing terabytes of video from distributed locations. This section describes best practices for configuring a Unity or SC series storage system for this solution.

The Unity and SC series arrays are designed for midtier to enterprise storage environments, are ideal for distributed environments, and can scale to handle large petabyte (PB) environments with block-only requirements at central locations.

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 Embedded Box PCs

Dell Embedded Box PCs are ruggedized, fanless, highly reliable devices for a variety of use cases, including process and discrete manufacturing, fleet management, kiosks, digital signage, surveillance and automated retail solutions. Embedded computers must run reliably 24x7 for extended deployments, and withstand higher and lower temperatures than ordinary PCs in environments that can bring high amounts of shock, vibration, moisture and high electromagnetic radiation.

Dell Embedded Box PCs are designed to MIL-STD-810G standards, building on the expertise of our rugged device engineers. Flexible, with many input/output (I/O) options, they run on powerful multicore Intel® processors. PCI/PCIe card slots provide flexible expansion for new I/O and graphics capabilities.

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 NAS clusters or block arrays are planned for surveillance storage.

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

CHAPTER 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.

Block storage (SAN, local)

We conducted validation tests to determine how Genetec works with Dell EMC block and local storage arrays.

Unity

We conducted the validation tests to determine how Genetec works with Unity™ storage arrays.

A Genetec Archiver supports up to 37.5 MB/s (300 Mb/s) and up to 300 cameras.

The test results shown in the following table are based on a conservative model to ensure that the constant-bandwidth video traffic is unaffected during a single storage processor (SP) maintenance cycle, disk rebuild, or similar performance-intensive events.

Table 3 Dell EMC Unity storage array results

Array	Security Center Version	RAID	Disks	No. of archivers	Bandwidth (MB/s)			Maximum (RAW)
					Per archiver	Array iSCSI	Array FC	
Unity300	5.7	6	80	8	37.5	300	330	2.34 PB
	5.7	6	150	15	37.5	562	618	
Unity400 [a]	5.7	6	120	12	37.5	450	495	3.9 PB
	5.7	6	250	24	37.5	900	989	
Unity500	5.7	6	64	7	37.5	262	288	7.8 PB
	5.7	6	104	13	37.5	488	536	
	5.7	6	240	30	37.5	1125	1136	
	5.7	6	500	40	37.5	1500	1649	
Unity600	5.7	6	100	16	37.5	600	660	9.7 PB
	5.7	6	200	32	37.5	1200	1320	
	5.7	6	400	64	37.5	2400	2640	
	5.7	6	500	80	37.5	3000	3300	
	5.7	6	600	80	37.5	3000	3300	
	5.7	6	1000	80	37.5	3000	3300	

[a] These values are extrapolated from Dell EMC Surveillance Lab test results.

Note

All disk drives are 6 TB NL-SAS unless otherwise noted.

SC series

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

We performed the following tests to ensure a worst-case scenario for all sizing parameters:

- Disk drive failures
- Storage controller failures
- NIC failures

We performed all tests using 5 Mb/s cameras. The total bandwidth is balanced across both controllers and provides constant bandwidth, with video traffic unaffected during single controller failure scenarios.

The following tables provide bandwidth-sizing guidelines based on our test results.

Table 4 Dell EMC SC series storage array results

Array	Security Center Version	RAID	Disks		Bandwidth (MB/s)		No. of recorders	Maximum (RAW)
			No.	Size	Per archiver	Array iSCSI		
SC5020	5.7	6 (8+2)	70	8 TB	37.5	262	7	4 PB
			140	8 TB	37.5	525	14	
			222	8 TB	37.5	825	22	
SCv3000	5.7	6 (8+2)	60	4 TB	37.5	225	6	1 PB
			120	4 TB	37.5	450	12	
			222	4 TB	37.5	825	22	

Note

All disk drives are NL-SAS 7200 RPM unless otherwise noted.

File storage (NAS)

The Dell EMC Surveillance Lab conducted validation tests to determine how Genetec works with Dell EMC file storage clusters.

To maximize performance for surveillance workloads, the Dell EMC Surveillance Lab recommends the following best practices:

- Use two SSD system drives per node in clusters where it is supported, such as the NL-Series
- Cluster utilization not to exceed 70 percent capacity

Isilon node and cluster

The test results are based on a model in which the constant-bandwidth surveillance video traffic remained unaffected during a single node maintenance cycle, disk rebuild, SP failure, or non-disruptive upgrade.

Sizing guidelines are based on a combination of storage capacity and per node bandwidth. When sizing a cluster, make sure to evaluate the number of servers that write and read from nodes in addition to overall storage capacity.

We used 1 GbE interfaces with no more than two SMB connections per interface. A 10 GbE interface can accommodate up to four Archiver connections at the maximum Genetec-supported values.

We performed all tests with a per-camera bandwidth of 4 Mb/s, so a single Archiver that handles 37.5 MB/s can support 75 such cameras.

We performed all tests with node or drive failures in place in the cluster (for example, with Isilon FlexProtect™ running) to ensure a worst-case scenario for all sizing parameters.

Note

HD400 Only — node reboot and node hardfail test has a video loss of 50 seconds on the recorders writing to the failed node.

Note

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

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

Table 5 Dell EMC Isilon node and cluster (SMB) test results

Cluster	OneFS version	Archivers per node	Bandwidth (MB/s)		Drives Size	Maximum Cluster Raw
			Per node	Per host		
A200	8.1 [a]	1	37.5	37.5	4 TB [b]	17 PB
A2000	8.1.1.1 [a]	1	37.5	37.5	10 TB	28 PB
		2	75	37.5	10 TB	
H400	8.1 [a]	1	37.5	37.5	8 TB	17 PB
		2	60	30	8 TB	
		3	75	25	8 TB	
		4	60	15	8 TB	
HD400	8.1 [a]	1	37.5	37.5	6 TB	50.9 PB
		2	75	37.5	6 TB	
	8.0.x	1	37.5	37.5	6 TB	
		2	75	37.5	6 TB	
		3	112.5	37.5	6 TB	

Table 5 Dell EMC Isilon node and cluster (SMB) test results (continued)

Cluster	OneFS version	Archivers per node	Bandwidth (MB/s)		Drives Size	Maximum Cluster Raw
			Per node	Per host		
NL410	8.1 [a]	1	37.5	37.5	4 TB	30.2 PB
		2	75	37.5	4 TB	
	8.0.x	1	37.5	37.5	4 TB	
		2	75	37.5	4 TB	
		3	112.5	37.5	4 TB	
X410	7.2.x	1	37.5	37.5	1 TB	20.7 PB
		2	75	37.5	1 TB	
		3	112.5	37.5	1 TB	
NL400	7.0.x	1	37.5	37.5	1 TB	30.2 PB
		2	40	20	1 TB	
		4	40	10	1 TB	

a. See Dell EMC Storage with Genetec Security Center Configuration Guide for additional information regarding OneFS 8.1 installations.

b. Uses SATA drives.

Note

All disk drives are NL-SAS 7200 RPM unless otherwise noted.

Dell EMC ECS

The test results are based on a model in which the constant-bandwidth surveillance 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 or 15k rpm SAS drives for the CIFS-ECS 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 6 Dell EMC ECS Object Storage test results

Cluster	ECS Version	Recorders per node	Bandwidth (MB/s)		No. drives/ ECS node	ECS Node Drives	
			Recorder	Node		Size	Type
ECS U400	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

Servers

We conducted functional tests to determine how Genetec works with Dell EMC servers.

Dell EMC PowerEdge servers

The test results are based on a model in which the constant-bandwidth surveillance video traffic remained unaffected during select storage failure scenarios, such as disk rebuild, failing processors, 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.

Multiarchiver tests were conducted with a single instance of Security Center running multiple Archiver services.

We used 10 GbE interfaces with up to four Archiver connections at the maximum Genetec supported values. We performed all tests with a per Archiver bandwidth of 37.5 MB/s with a combination of 1 Mb/s and 5 Mb/s cameras.

Dell EMC recommends using RAID 6 with local storage to accommodate the disk rebuild duration. For example, in the Dell EMC Surveillance Lab, a disk rebuild in a 16 x 10 TB disk system takes at least 36 hours to complete when 10TB of data and 37.5 MB/s of write are in place.

PowerEdge servers with local storage

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

Specification	R740xd	R540	R740xd-2
Security Center Version	5.7	5.7	5.7
CPU	2 X 12 Cores Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz	2 X 12 Cores Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz	2 X 12 Cores Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz
RAM GB	128	96	128
Drive type	NL-SAS	NL-SAS	NL-SAS
Storage Controller	H740P	H740P	H730P

Specification	R740xd		R540	R740xd-2
No of drives X Drive size TB	18 X 10tb		12 X 10tb	26 X 10tb
RAID	6		6	6
HotSpare	1		1	1
Host Operating system	Windows 2012 R2	Esxi	Windows 2012 R2	Windows 2012 R2
No of Instances	3 Archiver roles per server	3 VM Archivers per Esxi host. 1 Archiver role per VM	2	3 Archiver roles per server
Write BW per Archiver (MBps)	37.5	37.5	37.5	37.5
Total Write BW per server (MB/s)	112.5	112.5	75	112.5
Total IOPS	800	874	667	1551
Disk Rebuild duration Days	11	10	14	11
Video Data storage	Local	Local	Local	Local
Nic speed	2X10 Gb	2 X 10 Gb	2X10 Gb	2X10 Gb

Note

All tests performed with local storage are Genetec certified.

PowerEdge servers with external storage

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

Table 7 Dell EMC PowerEdge server with external storage

Option		R740	R730xd	R630 [a]	R530	R430
Security Center Version		5.7	5.5	5.5	5.5	5.5
Write BW (MB/s)		75	75	75	37.5	37.5
Archivers per host		2	2	1	1	1
Video data storage		HD400, NL410	HD400, NL410	HD400, NL410	HD400, NL410	HD400, NL410
RAM (GB)		96	64	64	64	64
NIC speed		10 Gb	10 Gb	10 Gb	10 Gb	10 Gb
CPU	Cores Processor GHz	2 X 12 Intel Xeon Gold 6126 2.60	2 X 12 Intel Xeon E5-2650 v4 2.20	2 X 10 Intel Xeon E5-2640 v4 2.40	2 X 6 Intel Xeon E5-2603 v3 1.60	2 X 6 Intel Xeon E5-2640 v4 2.40

Table 7 Dell EMC PowerEdge server with external storage (continued)

a. These values are extrapolated from Dell EMC Surveillance Lab test results.

Note

- Ensure that all external storage options are sized appropriately to support the specified workload before integrating PowerEdge servers into the surveillance solution.
- Servers that are used for external storage must meet Genetec's minimum requirements.

Dell EMC PowerEdge FX chassis

The PowerEdge FX architecture is based on a modular, building-block concept that makes it easy for enterprises to focus processing resources where needed.

The FX2 is a 2U rack-based, converged computing platform that combines the density and efficiencies of blades with the simplicity and cost advantages of rack-based systems. The FX2 hosts flexible blocks of server and storage resources while providing outstanding efficiencies through shared power, networking, I/O, and management within the chassis itself.

Server blocks

Server sled options are FC830, FC640, FC630, FC430.

Storage block

The PowerEdge FD332 storage block provides dense, highly scalable, direct attached storage for most FX infrastructures (it does not support the FM120 microserver). It is a critical component of the FX architecture, enabling future-ready scale out infrastructures that bring storage closer to compute for accelerated processing.

IO Blocks

The FX2 chassis comes with 1Gb or 10Gb pass through IO modules, or optional IO aggregator modules. The FN410s, FN410t, and the FN2210s are powerful IO aggregators that provide plug and play network switch Layer 2 functions.

For more details about the FX chassis, see the Dell Products page. For networking best practices, see the Dell EMC Surveillance Networking Reference Architecture.

		FX2 Chassis
Storage Block used		FD332
Video Data storage		Local, FD332
Drive type and Size		SAS, 14 X 1.2 TB
RAID Used		6
Server block used		FC640
CPU	Cores Processor GHz	2 X 12 Intel Xeon Gold 6126 2.60

	FX2 Chassis
RAM GB	64
Network speed	2 X 10 Gb
Security Center Version	5.7
No. of Archivers per server	2
Write BW per Archiver	37.5
Total Write BW per server (MB/s)	75
Total Read (MBps)	15

Dell Embedded Box PCs

We conducted functional tests to determine how Genetec works with Dell Embedded PCs.

Table 8 Dell Embedded PC test results

Option	Dell Embedded Box PC 5000
Video Data storage	Local
Drive type and Size	2 TB, SATA Flash drive
RAID Used	0
CPU	Intel Core i7 Processor
RAM GB	32
Network speed	2 X 1 Gb
Security Center Version	5.7
Archiver write BW	10 MBps
OS	Windows 10 Enterprise 64Bit

ESXi host class servers

The ESXi host can run on various host classes (processor chips) across multiple servers. For more information about server comparisons, see the Dell EMC servers tested section of the Dell EMC Surveillance Validation Matrix.

Bandwidth sizing guidelines

All solution tests were performed in a lab environment. The storage system, cameras, and VLANs in the lab environment were dedicated to these tests.

Connections to the storage system under test conditions were restricted to Security Center Archiver, monitoring, and web management stations. Expect some variance between the lab results and a production environment.

CHAPTER 5

Testing and validation

This chapter describes the testing used to validate this solution.

Test objectives

Many factors must be considered when designing your solution.

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

- Determine the bandwidth for various Dell EMC storage arrays using FC and iSCSI.
- Determine the bandwidth for various Dell EMC storage clusters using SMB.
- Determine the best configuration parameters for Unity and SC series storage options.
- Determine the best configuration parameters for Isilon storage options.
- Determine best video storage performance requirements for use with:
  - Isilon scale-out storage clusters
  - Unity storage arrays
  - SC series storage arrays
  - ECS Object Storage
- Determine the maximum bandwidth with multiple Archivers.
- Determine all factors with a lab-controlled failure, such as rebuilding disks, removing a node, 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:

- All test measurements were based on active failure scenarios. Failure scenarios include drive failures and recovery, forced Isilon node failures, and storage processor failures. These scenarios generally caused background jobs to run, such as Isilon's FlexProtect. Testing with these realistic scenarios helps ensure a successful implementation that is able to withstand various types of failures.
- 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 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.

The Unity and SC series block storage arrays were protected using RAID with hot spare disks. For the test, disk failure scenarios were induced and the data rebuild to the hot spare disks was observed with effect to write bandwidth.

The Isilon cluster was protected using a +2 protection scheme that allows for two simultaneous disk failures. For the test, two disks are failed and then recovered. The SmartFail process started and the CPU utilization of the node increased with no observed effect to the write streams.

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.

The Unity and SC series block storage arrays were protected using RAID with hot spare disks. For the test, disk failure scenarios were induced and the data rebuild to the hot spare disks was observed with effect to write bandwidth.

The Isilon cluster was protected using a +2 protection scheme that allows for two simultaneous disk failures. For the test, two disks are failed and then recovered. The SmartFail process started and the CPU utilization of the node increased with no observed effect to the write streams.

NIC failure test

The Unity and SC series block storage arrays were configured with multiple paths to the recorders using Microsoft MPIO. Multiple NICs were configured with the recorders and controllers for redundancy. The Unity and SC series hard NIC failure test removes one nic cable from the array. Recorders that were configured with multipathing reconnected to the volume across another available path. To reduce the reconnection time and eliminate video loss, adjust the TCP retransmission timers. For more information, see the .

The Isilon hard NIC failure test removes one NIC cable from the active node that was involved in active recording. After the NIC failure, writing to the same node failed. When the network fails, the server must recognize the failure, then it must establish a new connection. Also, when the network fails TCP socket connections are left open and remain open on the cluster until Isilon's OneFS forces them closed, which allows the server to continue writing.

We can force the open TCP sockets to close for a duration of less than 2 minutes by reducing the `TCP keep idle` and `TCP keep interval` timeout to the optimum values recommended by Isilon Engineering.

To reduce the video loss duration due to the `TCP Socket Open` condition, set the persistent values in the `sysctl.config` file as follows to reduce the impact duration time significantly:

```
 isi_sysctl_cluster
net.inet.tcp.keepidle=61000
 isi_sysctl_cluster
net.inet.tcp.keepintvl=5000
```

Refer to the KB Article 89232, *Configuring sysctls and making sysctl changes persist through node and cluster reboots and upgrades* for further information about how to configure these parameters.

Note

NIC failure impact can be overcome by using NIC aggregation in Active/Passive Failure aggregation mode, which is explained in the next test case. Connectivity to the nodes that are not affected by the network outage continues to be available throughout the test scenario and no impact was observed.

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 Surveillance 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.

NIC Failure test with NIC aggregation in Active/Passive

The hard NIC failure test with Active/Passive aggregation was run by removing the active NIC port cable. After the network failure, writing to the same node continued and the NIC that was passive was immediately changed to the active NIC. The NIC failure caused no apparent loss.

TCP transmission timers can be adjusted to reduce the reconnection times during Nic failures on recorders that use Microsoft MPIO. For more information, see the .

Note

NIC aggregation in Active/Passive mode remedies only a network disconnection/NIC failure that happens on the Isilon node or the corresponding switch port where it is connected.

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.

During the tests, the servers on the failed node reconnected to a new node, but did not start writing again for an aggregate (reconnect and start writing) duration of up to 52 seconds while waiting for writing to the SMB share to be re-started.

Also, the removal or addition of a node causes an interrupt to the cluster. Therefore, video servers writing to the other nodes might experience a short interruption. The duration of the interruption can be reduced by modifying the OneFS environment variables.

The following changes are required to modify the remove or add node interruption:

```
declare -i COUNT MDS
BASE=10000
COUNT=$((1.01 * $BASE))
MDS=$(($BASE * 0.75))
isi_sysctl_cluster kern.maxvnodes=$BASE
isi_sysctl_cluster kern.minvnodes=$BASE
isi_sysctl_cluster efs.lin.lock.initiator.lazy_queue_goal=$COUNT
isi_sysctl_cluster efs.ref.initiator.lazy_queue_goal=$COUNT
isi_sysctl_cluster efs.mds.block_lock.initiator.lazy_queue_goal=$MDS
isi_sysctl_cluster efs.bam.datalock.initiator.lazy_queue_goal=$MDS
```

Note

During an abrupt failure of a node, the recorders writing to that node reconnect to SmartConnect and can buffer the video during reconnection. Data tat was already written to the disk cannot be recovered which can range from about 4 to 5 seconds.

⚠WARNING

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

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.

Procedure

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:
   - Disk failures and rebuilds on Isilon nodes
   - Initiation of Isilon node failures and recoveries
   - Initiation of Isilon node removals (downsizing a cluster)
   - Initiation of Isilon node additions (scaling up)
   - NIC failures with active/active and active/passive configurations
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.

CHAPTER 6

Conclusion

This chapter summarizes the testing for this solution.

Summary

The Dell EMC Surveillance Lab performed comprehensive testing with Genetec Security Center against a large number of Unity and SC series arrays and Isilon clusters.

In addition to these performance tests, we conducted tests to illustrate the use of RSA SecurID user authentication.

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.

We demonstrated how RSA SecurID seamlessly provides enhanced user logon and permission capabilities.

Note

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

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.

Dell EMC Unity and SC series arrays

The use of storage pools to create LUNs within the Dell EMC Unity or SC series arrays greatly simplifies the configuration and increases the performance when compared to traditional block-level storage. Either iSCSI or FC can be implemented. FC performs better than iSCSI.

Dell EMC Isilon scale-out storage

Dell EMC Isilon scale-out storage is ideal for midtier and enterprise customers. An Isilon cluster is based on independent nodes working seamlessly together to present a single file system to all users.

Licensed SmartQuotas options can be configured so that each Archiver view of the storage is based on the assigned quota and not the entire file system. We recommend using SmartQuotas with Genetec Security Center as a best practice.