Surveillance
Dell EMC Storage with Genetec Security Center

Sizing Guide

H13495

REV 2.2

DELL EMC

Published March 2017

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. 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.

This guide also provides information on tests that were carried out on the Genetec SV-16v2 and SV-32v1 appliances. The Genetec SV-16 and SV-32 are small form factor devices that are intended for minimal standalone implementations or as remote entities in a large federated corporate or government implementation.

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™
- EMC VNX™
- EMC VNXe™
- EMC VMAX™

These guidelines include the following design considerations:

- Bandwidth recommendations for Genetec Security Center 5.4 SP4 and higher when they are attached to specific Dell EMC storage systems
- Dell EMC storage array configurations that are ideal for physical security solutions with Security Center
- Configuration guidelines for the Genetec SV-16v2 and SV-32v1 appliances
- 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 configuration for the following:

- Number of Genetec Archivers
- Mix of nodes and Genetec Archivers based on the expected bandwidth in an Isilon implementation

- Storage using Fibre Channel (FC) and Internet SCSI (iSCSI) on VNX 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:

- Determine the Archiver service's maximum bandwidth to specific Dell EMC storage arrays and clusters.
- 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.
- Determine the Genetec SV-16v2 and SV-32v1 performance properties.
- Recommend VNX cache configuration.
- Determine the VNX, VNXe, and VSS LUN bandwidth within the storage pool.
- Recommend an Isilon SMB configuration.
- Calculate array or node maximum bandwidths.
- Recommend disk drive types.
- Confirm the previous test results with lab controlled failures, such as disabled storage processors, disk rebuilds, node removals, and network path failures.

CHAPTER 2

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:

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

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). In addition, Dell EMC PowerPath™ was used for block storage (FC and iSCSI) and is recommended for block storage implementations.

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 6.0 host using Cisco UCS B230 Blade Servers with a 20-core ESXi host at 2.2 GHz and 256 memory. 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.

EMC VNX

VNX storage is ideal for recording and managing terabytes of video from distributed locations. This section describes best practices for configuring a VNX or VNXe storage system for this solution.

The VNX family includes the VNX, VNXe, and VNX-VSS series arrays. The VNXe series is designed for small to midsize environments. The VNX series is designed for midtier to enterprise storage environments, is ideal for distributed environments, and can scale to handle large petabyte (PB) environments with block-only requirements at central locations.

SV-16 and SV-32 appliance configuration

The SV-16 and SV-32 are fixed-configuration appliances. The operating system and Genetec Security Center are pre-installed and configured. These appliances are suited for back office or remote location implementations.

You can use iSCSI arrays, NAS arrays, or clusters for storage if they are available at the remote site.

CHAPTER 3

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
- VNX arrays
- VNXe arrays
- VMAX arrays

Note

The solution also supports VMAX arrays but we have not fully benchmarked this system. Consult with the Dell EMC Physical Security Solution Development team for VMAX array configuration recommendations.

For our testing, we used both single and dual storage processors for the full range of VNX, VNXe, and VSS 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)

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.

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

Table 1 Security Center primary services (continued)

Service	Description
	and establish connections, and receive centralized configuration information.

Genetec SV-16 and SV-32 appliances

Genetec SV-16 and SV-32 are IP video physical security appliances composed of the Dell EMC software preloaded on a small form factor (SFF) Windows 7 Embedded computer.

The SV-16v2 compact fixed-hardware appliance is designed to accommodate up to 16 cameras, or up to 4 MB/s (32 Mb/s) total throughput. The SV-32v1 can handle up to 32 cameras, or up to 8 MB/s (64 Mb/s) total throughput.

If an Dell EMC iSCSI storage array is already available, or is being considered for the site, then that storage array may have enough remaining overhead to support video from the SV-16v2 or SV-32v1.

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 .

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 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:

VNX and VNXe

We conducted the functional tests to determine how Genetec works with VNX and VNXe 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 pool (SP) maintenance cycle, disk rebuild, or similar performance-intensive events.

Table 2 EMC VNX/VNXe storage array results

Storage Protocol	Array	Array Bandwidth (MB/s)	Disks	Maximum (RAW)
iSCSI	VNXe1600**	300	35	400 TB
		300	200	
	VNXe3200*	210	120	500 TB
		210	150	
	VNX-VSS100*	390	90	360 TB
	VNX5200	446	75	500 TB
	VNX5400*	536	120	1 PB
		536	250	
	VNX5600*	616	120	2 PB
		985	240	
		985	500	
	VNX5800*	739	120	3 PB
		1182	240	
		1774	360	
		1774	750	
	VNX7600*	887	120	4 PB
		1419	240	
		2128	360	
		2838	480	
		2838	1000	
	VNX8000*	1064	120	6 PB
		1703	240	
		2554	360	
		3405	480	
		3405	600	

Table 2 EMC VNX/VNXe storage array results (continued)

Storage Protocol	Array	Array Bandwidth (MB/s)	Disks	Maximum (RAW)
		3405	1000	

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.

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.

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

Table 3 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		
X410	7.2.x	1	37.5	37.5	1 TB	20.7
		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
		2	40	20	1 TB	
		4	40	10	1 TB	
NL410	8.0.x	1	37.5	37.5	4 TB	30.2
		2	75	37.5	4 TB	
		3	112.5	37.5	4 TB	
HD400	8.0.x	1	37.5	37.5	6 TB	50.9
		2	75	37.5	6 TB	
		3	112.5	37.5	6 TB	

Note

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

Symmetrix VMAX

We tested the Symmetrix VMAX as part of the server sizing test.

The test was functional in scope and was not intended to maximize the capabilities of the Symmetrix VMAX storage array or provide extensive benchmarking. The following table displays the results.

Table 4 Symmetrix VMAX results

Array	Array bandwidth	LUN bandwidth (MB/s)	Storage protocol
VMAX	N/A	37.5	FC

Genetec SV-16 and SV-32 servers

The Genetec SV-16 and SV-32 are small form factor, fixed-configuration appliances intended for low bandwidth. with a maximum of 16 and 32 cameras respectively.

The following table shows the testing results for maximum bandwidth and maximum number of cameras for the Genetec SV-16v2 and SV-32v1 appliances.

Table 5 Appliance test results

	Array	Bandwidth (MB/s)	Maximum cameras
SV-16v2	Any Dell EMC storage	4	16
SV-32v1	Any Dell EMC storage	8	32

ESXi host class comparison

The following table displays the ESXi host class comparison results from various host classes (processor chips) across multiple server vendors.

Note

The purpose of the following table is to illustrate that varying the processing power and memory affects server density and aggregate bandwidth. The following table is not intended to provide a comprehensive comparison.

Table 6 ESXi 5.1 test results

Host Class	Cores	Memory	Maximum Archivers	Maximum bandwidth MB/s
Xeon E7-8830	80	1 TB	34	1,275
Xeon E7-2800	20	256 GB	6	225
Xeon 7500	24	128 GB	6	225
Xeon 7400	24	64 GB	3	112

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 Isilon and VNX storage options.
- Determine best video storage performance requirements for use with Isilon scale-out storage clusters and VNX storage arrays.
- Determine the maximum bandwidth with multiple Archivers.
- Determine all factors with a lab-controlled failure, such as disabling a storage processor, rebuilding disks, removing a node, or network path failures.

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. We also conducted tests on the Genetec Security Center SV-16v2 and SV-32v1 appliances and RSA SecurID.
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 VNX and VNXe arrays
   - Use of only one VNX or VNXe storage processor
   - 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.

SV-16 and SV-32

We tested the SV-16v2 and SV-32v1 preloaded Genetec Security Center applications stack against the Genetec bandwidth and camera specifications.

Procedure

1. Configured the target storage array.
2. Applied a camera load representing the maximum allowed SV-16 or SV-32 bandwidth.
3. Determined the optimum LUN or share performance within the scope of the SV-16 or SV-32 operating parameters.
4. Tested with the maximum number of cameras allowed in an SV-16 or SV-32 environment.

Results

Test results are provided in the Configuring the SV-16 and SV-32 section of this document.

SV-16 and SV-32 scenario 2

We verified the granularity of user permissions indicated by the users' Security Center access rights to the Config Tool and Securtiy Desk clients.

Procedure

1. Removed the user from the Security Center Group in Active Directory.
2. Logged in to the Windows domain using an RSA passcode created by combining a PIN with a token generated by an RSA authenticator.
3. Double-clicked the Security Center client icon to start the application.
4. Selected the **Use Windows credentials** option and pressed **Enter**.

Results

The user successfully accesses the Windows domain but is denied access to the Security Center client application.

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 VNX and VNXe 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.

We tested the SV-16v2 and SV-32v1, intended as standalone back-office systems or as edge appliances for more robust video surveillance implementations. The low bandwidth, low camera count SV-16v2 and SV-32v1 were tested at their maximum bandwidth and camera count levels without issues.

EMC VNX arrays

The use of storage pools to create LUNs within the EMC VNX 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.

EMC VNX-VSS arrays

The VNX Video Surveillance Storage (VSS) is a storage solution that is purpose built to meet the unique demands of the video surveillance environment.

We found that this high availability, low-cost array performs comparably to other arrays in the VNX family.

EMC VNXe arrays

An iSCSI-connected VNXe array, implemented with storage pools, provides a cost-effective implementation while maintaining the expected performance. Many mid-sized deployments can use VNXe.

Low-bandwidth implementations can use a NAS-connected VNXe, but ideally NAS implementations should be based on Dell EMC Isilon scale-out storage.

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.