

Surveillance

Dell EMC Storage with Genetec Security Center

Configuration Guide

H13476
REV 2.2



Copyright © 2014-2017 Dell Inc. or its subsidiaries. All rights reserved.

Published March 2017

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, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners.
Published in the USA.

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

CONTENTS

Chapter 1	Introduction	5
	Purpose.....	6
	Scope.....	6
	Assumptions.....	6
Chapter 2	Configuring the solution	7
	Design concepts and disclaimers.....	8
	EMC VNX.....	10
	Disk drives.....	10
	Storage pool configuration (recommended).....	10
	LUN configuration.....	11
	Fibre Channel configuration.....	12
	VNXe RAID configuration.....	12
	iSCSI initiators.....	12
	Recommended cache configuration.....	13
	Isilon (NAS).....	13
	Data protection.....	13
	OneFS 8.1 job workers (required).....	14
	Impact policy and priority configuration.....	14
	Volume limits.....	14
	Large file system, small view (SmartQuotas).....	15
	Configuring SmartQuotas (recommended).....	15
	SMB specific configuration.....	16
	Unique share naming.....	18
	Configuring SmartConnect (optional).....	18
	I/O optimization configuration.....	19
	Configuring authentication and access control.....	20
	Releases tested.....	20
	RSA SecurID environment.....	22
	Configuring Genetec for use with RSA.....	23
	Dell EMC Surveillance Lab test environment.....	24
Chapter 3	Conclusion	25
	Summary.....	26
Index		27

CONTENTS

CHAPTER 1

Introduction

This chapter presents the following topics:

- [Purpose](#).....6
- [Scope](#).....6
- [Assumptions](#).....6

Purpose

This configuration guide aims to help Dell EMC field personnel understand how to configure Dell EMC storage system offerings to simplify the implementation of Genetec Security Center. This document is not a replacement for the Genetec implementation guide nor is it a replacement for the *Dell EMC Storage with Genetec Security Center: Sizing Guide*.

Scope

This guide is intended for internal Dell EMC personnel and qualified Dell EMC and Genetec partners. It provides configuration instructions for installing the Genetec Security Center video management software using Dell EMC storage platforms.

The following Dell EMC storage systems have been tested:

- Dell EMC Isilon™
- EMC VNX™
- EMC VNXe™
- EMC VMAX™

This guide supplements the standard *EMC VNX Storage Best Practices with Video Management Systems: Configuration Guide* and *Dell EMC Isilon Storage Best Practices with Video Management Systems: Configuration Guide* and provides configuration information specific to Genetec Security Center.

Note

All performance data in this guide was obtained in a rigorously controlled environment. Performance varies depending on the specific hardware and software used.

Assumptions

This solution assumes that internal Dell EMC personnel and qualified Dell EMC partners are using this guide with an established architecture.

This guide assumes that the Dell EMC partners who intend to deploy this solution are:

- Associated with product implementation
- Genetec-certified to install Genetec Security Center services
- Proficient in installing and configuring VNX/VNXe storage solutions
- Proficient in installing and configuring Isilon storage solutions
- Familiar with installing and configuring VMware hypervisors and the appropriate operating system, such as Microsoft Windows or a Linux distribution
- Able to access the *EMC VNX Storage with Video Management Systems: Configuration Guide* and *Dell EMC Isilon Storage with Video Management Systems: Configuration Guide*

The configurations that are documented in this guide are based on tests that we conducted in the Dell EMC Surveillance Lab using worst-case scenarios to establish a performance baseline. Lab results might differ from individual production implementations.

CHAPTER 2

Configuring the solution

This chapter presents the following topics:

- [Design concepts and disclaimers](#).....8
- [EMC VNX](#)..... 10
- [Isilon \(NAS\)](#)..... 13
- [Releases tested](#).....20
- [RSA SecurID environment](#).....22
- [Configuring Genetec for use with RSA](#).....23
- [Dell EMC Surveillance Lab test environment](#).....24

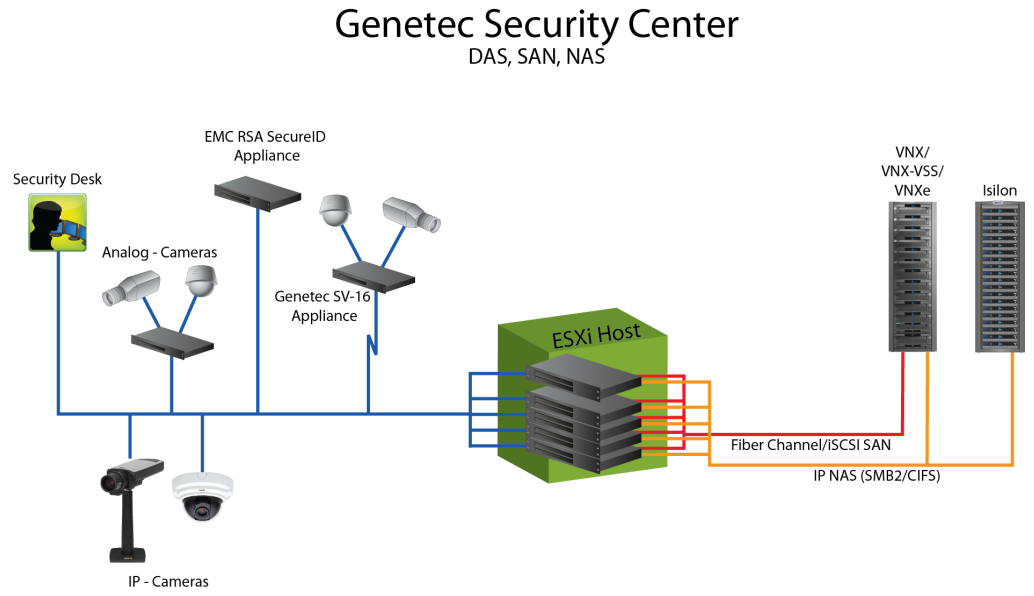
Design concepts and disclaimers

There are many design options for a Genetec Security Center implementation including Federations, Auxiliary Servers, and multicast considerations.

Genetec offers many courses that are related to design and implementation for those who require this information. These details are beyond the scope of this paper.

The following figure illustrates the Dell EMC components that were tested.

Figure 1 Genetec Security Center architecture



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 will be fully validated on Generation 5 and Generation 6 hardware.

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.

Disk drives

Although any supported drive will work, video surveillance systems typically rely on the density of the array. Dell EMC recommends NL-SAS drives of the highest available density in this solution. In general, we used one-terabyte (TB) or multi-TB NL-SAS drives when performing our tests.

Note

Because of the high percentage of sequential, large block writes, Dell EMC does not recommend using flash drives for video storage within a surveillance application.

Storage pool configuration (recommended)

The tests we conducted show how storage pools that are defined with the maximum allowable number of disks per pool perform as well as, or better than, traditional RAID groups. Therefore, Dell EMC recommends that you use storage pools rather than RAID groups. Storage pools also reduce the required array management tasks.

The VNX family array architecture is optimized for storage pools. A storage pool is a construct that is built over one, or more commonly multiple, RAID groups. LUNs are built on top of the storage pool. The read/write activity is a random distribution across all disks defined to the storage pool. This distribution results in increased and balanced per disk utilization and improved performance when compared to traditional RAID implementations.

The RAID groups underlying storage pools can be either RAID 5 or RAID 6. The default and recommended RAID configuration for a VNXe or VSS1600 array using NL-SAS drives is RAID 6. Either RAID 5 or RAID 6 can be used with VNX arrays. RAID 5 is used for optimizing the array to achieve the maximum amount of storage and RAID 6 is used for enhancing data protection. Our tests using an isolated surveillance infrastructure did not reveal any notable performance variances when using RAID 5 as compared to RAID 6.

Building a storage pool is a straightforward process. You can configure either RAID 5 or RAID 6 pools depending on the VNX or VNXe storage system restrictions and the level of risk that the customer is willing to accept. When configuring storage pools, use large storage pools with large logical unit number (LUN) sizes, and configure the LUNs as thick. Do not use thin LUN provisioning.

Dell EMC recommends the following RAID configurations for VNX arrays:

- RAID 5 or RAID 10 with SAS drives
- RAID 6 with NL-SAS drives

Procedure

1. In Unisphere, select **Storage > Storage Pools** for block.
2. Click **Create** under **Pools** in the **Pools** section.
3. Set the following options for the storage pool:
 - Storage pool name
 - RAID type
 - Number of SAS drives
 - Number of NL SAS drives
4. Choose a method for selecting disks to include in the storage pool:
 - **Automatic:** Provides a list of available disks.
 - **Manual:** Enables you to select specific disks to include in the storage pool from a list of available disks. Be sure to clear the automatic disk recommendation list before you select new disks from the list.
5. Select **Perform a Background verify on the new storage** and set the priority to medium.
6. Click **Apply**, and then click **YES** to create the storage pool.

LUN configuration

A VNX pool LUN is similar to a classic LUN. Pool LUNs comprise a collection of slices. A slice is a unit of capacity that is allocated from the private RAID groups to the pool LUN when it needs additional storage. Pool LUNs can be thin or thick.

Thin LUNs typically have lower performance than thick LUNs because of the indirect addressing. The mapping overhead for a thick LUN is less than for a thin LUN.

Thick LUNs have more predictable performance than thin LUNs because they assign slice allocation at creation. Because thick LUNs do not provide the flexibility of oversubscribing like a thin LUN, use thick LUNs for applications where performance is more important than saving space.

Thick and thin LUNs can share the same pool, enabling them to have the same ease-of-use and benefits of pool-based provisioning.

Procedure

1. In Unisphere, right-click a storage pool and then click **Create LUN**.
2. Type the user capacity for the LUN.
3. Type the starting **LUN ID**, and then select the number of LUNs to create.

For example, if the selected LUN ID is 50, and the selected number of LUNs to create is 3, the names for the LUNs are 50, 51, and 52.
4. Select **Automatically assign LUN IDs as LUN names**.
5. Click **Apply**.

Fibre Channel configuration

To transfer traffic from the host servers to shared storage, the serial-attached network (SAN) uses the Fibre Channel (FC) protocol that packages SCSI commands into FC frames.

Note

iSCSI is prevalent for video security implementations because it often provides a lower-cost option when compared to FC.

To restrict server access to storage arrays that are not allocated to the server, the SAN uses zoning. Typically, zones are created for each group of servers that access a shared group of storage devices and LUNs. A zone defines which HBAs can connect to specific service providers (SPs). Devices outside a zone are not visible to the devices inside the zone.

Zoning is similar to LUN masking, which is commonly used for permission management. LUN masking is a process that makes a LUN available to some hosts and unavailable to other hosts.

Zoning provides access control in the SAN topology. Zoning defines which HBAs can connect to specific targets. When you use zoning to configure a SAN, the devices outside a zone are not visible to the devices inside the zone.

Zoning has the following effects:

- Reduces the number of targets and LUNs presented to a host
- Controls and isolates paths in a fabric
- Prevents non-ESXi systems from accessing a particular storage system and from possible virtual machine file system (VMFS) data loss
- Optionally, separates different environments, such as test and production environments

With VMware ESXi hosts, use single-initiator zoning or single-initiator-single-target zoning. The latter is the preferred zoning practice because it is more restrictive and prevents problems and misconfigurations that can occur on the SAN.

VNXe RAID configuration

VNXe offers RAID 5, RAID 6, and RAID 10 configurations. Different configurations offer different types of protection against disk failures.

Dell EMC recommends the following RAID configurations:

- RAID 5 or RAID 10 with SAS drives
- RAID 6 with NL-SAS drives

iSCSI initiators

Software or hardware initiators may be used with VMware ESXi server or a non-virtualized server.

Microsoft Internet SCSI (iSCSI) initiators

For both physical servers and VMware ESXi server, the Dell EMC Surveillance Lab uses Microsoft iSCSI initiators with excellent results.

Hardware iSCSI initiators

Hardware iSCSI initiators can be used. There are many iSCSI initiators available on the market, and results might vary.

Microsoft Windows Server 2008 R2 or later supports the iSCSI initiators natively in the OS. Our tests were conducted using Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. The increased performance that is associated with the 2012 releases not been significant enough to warrant including release-specific results in this document.

Recommended cache configuration

EMC VNX generation 2 systems, such as VNX5200 or VNX5400, manage the cache. If the array is shared with other applications, you can use a lower write cache value, but avoid excessive forced flushes.

Dell EMC recommends that you configure the cache as 90 percent write and 10 percent read if the storage array does not automatically adapt to the write characteristics of video surveillance (for example, EMC VNX5500 or EMC VNX-VSS100).

Isilon (NAS)

The Isilon scale-out network-attached storage (NAS) platform combines modular hardware with unified software to harness unstructured data. Powered by the distributed Isilon OneFS™ operating system, an Isilon cluster delivers a scalable pool of storage with a global namespace.

The platform's unified software provides centralized web-based and command-line administration to manage the following features:

- A symmetrical cluster that runs a distributed file system
- Scale-out nodes that add capacity and performance
- Storage options that manage files and tiering
- Flexible data protection and high availability
- Software modules that control costs and optimize resources

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 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.

Isilon protection with OneFS

New or upgraded clusters, starting with OneFS 7.2, provide a data protection level that meets Dell EMC Isilon guidelines for mean time to data loss (MTTDL) for large capacity nodes. Current releases of OneFS offer a new protection option, `+3d:1n1d`, which means the cluster can survive three simultaneous disk failures or one entire node failure plus one disk. OneFS also provides an option that continually evaluates the cluster and sends an alert if the cluster falls below the suggested protection level.

OneFS 8.1 job workers (required)

OneFS can be tuned to provide optimal bandwidth, performance, or operating characteristics. Starting with OneFS 8.1 the Dell EMC Surveillance Lab achieved optimum resilience when the number of job workers slowly increased their number per job phase.

From the CLI to modify the job works to 0 per core:

```
isi_gconfig -t job-config impact.profiles.medium.workers_per_core=0
```

Impact policy and priority configuration

The impact policy defines the number of parallel tasks or workers that can run at one time within OneFS. Leave the impact policy as it is, unless Isilon directs you to change one or more policies.

Releases with OneFS 7.0 or greater

Dell EMC recommends using OneFS 7.0 or later to maximize bandwidth and minimize video review response times. You can use the default impact policy with Isilon X400, Isilon X410, Isilon NL410, and greater. For less powerful nodes, such as the Isilon X200 and earlier running OneFS 7.0 or greater, modify all jobs to use an impact policy of **Low**.

Releases prior to OneFS 7.0

For releases prior to OneFS 7.0, the best I/O performance is obtained by configuring all background jobs with the impact policy set to **Low**. To set the impact policy select **Operations > Jobs and Impact Policies**.

Priority configuration

Even if the impact policy is modified, for example, by changing the settings of all the jobs to **Low**, the priority of the jobs remains at their default settings.

Volume limits

Implementations greater than 8 TB are common when video is stored on high-end storage, such as Isilon scale-out NAS storage and VNX block storage. The clustered file system OneFS uses enables Isilon to handle these large volumes.

Genetec provides best practices that are based on in-house testing and customer experiences. For video storage with Security Center 5.2, Genetec recommends limiting volumes to 16-20 TB. Based on lab tests and customer experiences, Genetec

realizes that an Isilon cluster performs extremely well with video storage shares much greater than 8 TB. Genetec fully supports these larger shares with Dell EMC Isilon.

Large file system, small view (SmartQuotas)

Although it is possible to assign the full Isilon cluster file system to a single Genetec Archiver, the Dell EMC best practice is to use SmartQuotas™ to segment the single Isilon file system so that each Archiver has a logical subset view of storage.

There are three directory-level quota systems:

Advisory limit

Lets you define a usage limit and configure notifications without subjecting users to strict enforcement.

Soft limit

Lets you define a usage limit, configure notifications, and specify a grace period before subjecting users to strict enforcement.

Hard limit (recommended)

Lets you define a usage limit for strict enforcement and configure notifications. For directory quotas, you can configure storage users' view of space availability as reported through the operating system.

Use the **Hard limit** quota system to set the video storage as a defined value.

If necessary, both Isilon and the Genetec Archiver can add or subtract storage, even if a hard quota is set.

Configuring SmartQuotas (recommended)

The SmartQuotas feature enables you to limit the storage that is used for each Genetec Archiver. It presents a view of available storage that is based on the assigned quota to the Archiver. SmartQuotas enables each Archiver to calculate its available disk space and react appropriately.

Without SmartQuotas, the Security Center administrator must anticipate the total write rate to the cluster and adjust the **Min Free Space** on each Archiver accordingly. A miscalculation can result in lost video. SmartQuotas resolves the issues that can be caused by manual calculations.

Configure SmartQuotas when more than one Archiver is writing to the Isilon cluster, or when other users share the cluster. Enable SmartQuotas and define a quota for each share or directory.

Configure the SmartQuotas setup with the following settings:

- Configure a hard share limit threshold to the Archiver video files.
- Define OneFS to show and report the available space as the size of the hard threshold.
- Set the usage calculation method to show the user data only.

Procedure

1. From the OneFS GUI, select **File System Management > SmartQuotas**.
2. For each listed share, select **View details**.
3. Under **Usage Limits**, select **Edit usage limits**.
4. Define the SmartQuotas limit and set the threshold:

- a. Select **Specify Usage Limits**.
 - b. Select **Set a hard limit**.
 - c. Type the hard limit value.
 - d. Select the size qualifier, typically **TB**.
 - e. Select the size of the hard threshold.
5. Click **Save**.
 6. Repeat the process for the remaining shares.

SMB specific configuration

The Dell EMC Surveillance Lab has discovered a File Open issue with some failure test scenarios. If the TCP socket connections that were made previously between the video server and the Isilon node do not close, then the server writing video to the Isilon share might not be available for up to 20 minutes, which is the SMB default.

As a preventative measure we recommend adding two timeout values: *keepidle* and *keepintvl*. Set the *keepidle* to 61 seconds and the *keepintvl* to 5 seconds, which resets the default 20 minute timer to 61 seconds allowing the shares to be re-opened between 1 and 2 minutes.

To make a `sysctl` configuration change persistent, add to or change the desired parameter in the `sysctl.conf` file.

Procedure

1. Open an SSH connection on a node in the cluster and log on using the `root` account.
2. Run the following command to back up the `/etc/mcp/override/sysctl.conf` file:

```
touch /etc/mcp/override/sysctl.conf && cp /etc/mcp/override/
sysctl.conf /etc/mcp/override/sysctl.conf.bk01
```

3. Run the following command, where `<sysctl_name>` is the parameter you want to add or change and `<value>` is the value assigned to the parameter.

```
isi_sysctl_cluster <sysctl_name>=<value>
```

The following output is displayed:

```
Value set successfully
```

For example:

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

4. Run the following command to verify that the change was successfully added to the `/etc/mcp/override/sysctl.conf` file:

```
cat /etc/mcp/override/sysctl.conf
```

Output similar to the following is displayed:

`<sysctl_name>= <value> #added by script`

For example:

```
cat /etc/mcp/override/sysctl.conf
efs.bam.layout.disk_pool_global_force_spill=1 #added by script
net.inet.tcp.keepidle=61000 #added by script
net.inet.tcp.keepintvl=5000 #added by script
```

5. If you need to revert the `sysctl.conf` file to the backup version created previously:
 - a. Open an SSH connection on any node in the cluster and log on using the root account.
 - b. Run the following command to copy and then rename the original backup of the `sysctl.conf` file:

```
cp /etc/mcp/override/sysctl.conf.bkul /etc/mcp/override/
sysctl.conf
```

Refer to the KB Library topic: 000089232 for further information about configuring these parameters.

Frame loss reduction

In our testing we discovered there might be some video loss when adding or removing a node from the cluster. OneFS is a scale-out, single namespace, clustered file system. To maintain coherency, OneFS implements a distributed lock manager that marshals locks across all nodes in the cluster. When a node is added or removed from the cluster, all operations must be temporarily suspended until all existing locks are rebalanced across the resulting node set. The system must then recalculate the cluster write plan. The time required for this group change to occur depends on the size of the cluster, individual node performance, and cluster workload.

We optimized the parameters on the cluster to reduce the frame loss duration as much as possible.

Procedure

1. Set the parameters in the `sysctl` configuration file using the following commands:

```
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.data.lock.initiator.lazy_queue_goal=
$MDS
```

2. Verify the changes are logged in `sysctl.conf` file:

```
cat /etc/mcp/override/sysctl.conf
net.inet.tcp.keepidle=61000 #added by script
net.inet.tcp.keepintvl=5000 #added by script
kern.maxvnodes=10000 #added by script
kern.minvnodes=10000 #added by script
efs.lin.lock.initiator.lazy_queue_goal=10100 #added by script
efs.ref.initiator.lazy_queue_goal=10100 #added by script
efs.mds.block_lock.initiator.lazy_queue_goal=7500 #added by
script
efs.bam.data_lock.initiator.lazy_queue_goal=7500 #added by
script
```

Unique share naming

When working with a single file system, each Archiver uses the time and date as part of its directory and file-naming conventions.

To avoid corruption caused by overwriting or grooming (deleting) files prematurely, create a unique share for each Archiver. The share uses the form `\video_repository\archiver n` , where n represents the sequential number for a unique Archiver.

In the Genetec Configurator Tool, you can change the default directory that the Archiver uses for video storage. By default, Genetec Archivers all use a subdirectory called `videoarchive`.

Configuring SmartConnect (optional)

SmartConnect™ uses the existing Domain Name Service (DNS) Server and provides a layer of intelligence within the OneFS software application.

The resident DNS server forwards the lookup request for the delegated zone to the delegated zone's server of authority, which is the SmartConnect Service IP (SIP) address on the cluster. If the node providing the SmartConnect service becomes unavailable, the SIP address automatically moves to a different node in the pool.

Connections are balanced across the cluster, which ensures optimal resource utilization and performance. If a node goes down, SmartConnect automatically removes the node's IP address from the available list of nodes, ensuring that a connection is not tried with the unavailable node. When the node returns to service, its IP address is added to the list of available nodes.

The delegated server authority is always the node with the lowest ID, unless it has surrendered its authority status, either voluntarily or involuntarily. This node should always be available, but if the status of the node changes and becomes unavailable, it voluntarily surrenders its role as server of authority.

You must add a delegation Name Server (NS) entry to the resident DNS server for the SmartConnect name, which points to the SIP address as the Name Server. In your DNS Manager, create a **New Delegation** using your SmartConnect zone name. In the Microsoft DNS wizard, a New Delegation record is added in the forward lookup zone for the parent domain.

SmartConnect balances connection loads to the Isilon cluster and handles connection failover. With SmartConnect, all Genetec Archivers use a single fully qualified domain name (FQDN) or universal naming convention (UNC) path for video storage access. Using this network name provides load balancing when the connection to the cluster is made and simplifies installations.

SmartConnect Basic can use a round-robin-type connection allocation, which is based on DNS load balancing.

SmartConnect Advanced can include multiple pools for each subnet, Dynamic IP addresses for NFS, and the following load-balancing options (Connection policy and Rebalance policy):

Round-robin (recommended)

Sequentially directs a connection to the next Isilon IP address in the cycle. Based on field reports, this option works well with 20 servers or more.

Connection count

Provides uniform distribution of the Genetec Archiver servers to specified nodes in the Isilon cluster. Use a unique IP address pool for video recording and Archiver read/write access.

Network throughput

Based on NIC utilization. Use of throughput requires that each Archiver is activated, configured, and recording video after it connects to Isilon.

CPU usage

Uses the node CPU utilization to determine which Isilon IP address to assign to the next connection request.

Ensure that no other service uses the Archiver IP address pool. Define additional pools for management (such as Isilon InsightIQ™ or administrative access), evidence repository, post process, or other use.

Procedure

1. Select **Networking Configuration**.
2. Under **Subnet > Settings**, define the SmartConnect service IP (SSIP) address. The SSIP address is the IP address that the DNS uses for the Isilon Authoritative name service.
3. Under **Pool settings**:
 - a. Define the SmartConnect zone name, which is the name to which clients connect.
 - b. Define the SmartConnect service subnet (the subnet that has the SSIP configured on the DNS server).
 - c. Define the connection balancing policy to **Round Robin**.
 - d. Set the IP allocation strategy to **Static**.
4. Verify this configuration on the SmartConnect dashboard.

I/O optimization configuration

As of OneFS 7.0.x, no changes are necessary to the I/O profiles for the directories that are used for Genetec.

Note

This setting does not require a SmartPool license.

Configuring authentication and access control

We conducted authentication and access control tests to determine the best method for shared access.

The following three tests were conducted:

Full Active Directory (recommended)

Where the Security Center server and the Isilon cluster are part of the same Windows domain.

Partial Active Directory

Where the Security Center servers are part of the Windows domain, but the Isilon cluster is administered locally.

Fully locally administered control

Where the Security Center servers and the Isilon cluster are administered locally.

See the **Security Center Installation and Upgrade Guide** specific to the Security Center release you are configuring.

Alternatives to the previous methods might exist, but the Dell EMC Surveillance Lab team does not plan to derive or support other methods.

Procedure

1. Select **Cluster Management > Access Management**.
2. Select **Access zone** and ensure that the **System access zone** has the provider status **Active Directory, Local, and File** marked with a green dot.
3. Under **Active Directory**, select **Join a domain** and add the Windows domain and appropriate users using one of the following options:
 - When the Isilon cluster and Genetec are not part of the same domain, set the shares to **Run as Root**. This setting is not ideal from a security perspective.
 - When the Isilon cluster and Security Center server are part of the same domain, configure the **DVM Camera** service to use the Domain account with read/write permissions to the Isilon cluster share. During the initial installation of the camera server, use the Security Center administrator account specification wizard to configure the camera service. Specify the recording location for the camera server using the full UNC path of the Isilon share.

Releases tested

The following tables list the firmware builds and software releases used for our tests.

Table 1 Firmware builds

Model	Firmware
VNXe1600	VNXe OE 3.1.3.5754151
VNXe3100	VNXe OE 2.1.0.14097
VNXe3150	VNXe OE 2.4.0.20932

Table 1 Firmware builds (continued)

Model	Firmware
VNXe3200	VNXe OE 3.1.3.5754151
VNXe3300	VNXe OE 2.1.0.14097
VNX-VSS100	VNX OE 5.32.000.5.215
VNX5100	VNX OE 5.31.000.5.006
VNX5200	VNX OE 5.33.008.5.119
VNX5300	VNX OE 5.31.000.5.006
VNX5400	VNX OE 5.33.000.5.015
VNX5500	VNX OE 5.31.000.5.720

Table 2 OneFS releases

Model	Firmware
X410	7.2.1
NL410	7.2.1, 8.0
HD400	7.2.1, 8.0

Table 3 Genetec Security Center releases

Release	Subrelease
Genetec Security Center	5.2 sr8, 5.3 GA, 5.3 sr4 plus hot fix, 5.4 SR2

For an Isilon implementation, Dell EMC recommends using Genetec Security Center 5.3 sr4 plus hot fix, or 5.4.

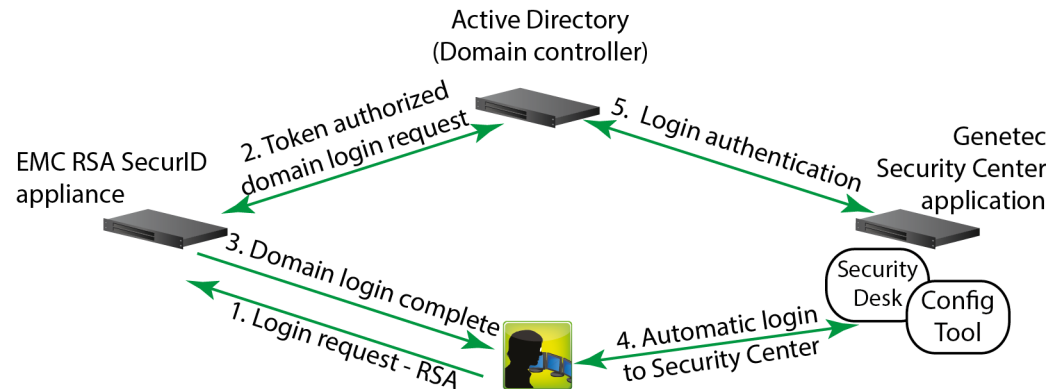
Note

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 will be fully validated on Generation 5 and Generation 6 hardware.

RSA SecurID environment

The following figure provides an overview of the process that is used to log in to the Genetec Security Center applications in an RSA® SecurID® environment that includes Microsoft Active Directory.

Figure 2 RSA login process



Note

After integrating Security Center into Active Directory, all preexisting Security Center users and user groups that have no match in Active Directory are deleted. So before integration, create these users and user groups in Active Directory.

The login process for Security Center in an RSA SecurID environment consists of the following five phases.

Login request—RSA token

The user types a login request that includes a one-time-use passcode.

The user's secret PIN is combined with a token code that their RSA authenticator generates to create the passcode.

The login request is sent to an RSA SecurID Appliance.

Token authorized

If the user's credentials are correct, the RSA SecurID Appliance proxies the login to Active Directory.

Domain login complete

Active Directory authenticates the login to the requested Windows domain.

Automatic login to Security Center

The user does not need to type credentials again. The client application automatically connects to the Security Center Directory.

Login authentication

To ensure that the user has access rights for the requested application, the Security Center Directory service proxies the login request to Active Directory for authentication.

The user is then able to use the chosen Security Center application.

Configuring Genetec for use with RSA

You must configure Genetec for use with SecurID.

Procedure

1. Install Genetec Security Center.
 - a. Follow the detailed instructions that are provided in the Genetec product documentation.

The default service login user (OmnicastSvcUsr) created during the Security Center Server installation is a local user and is not eligible to access Active Directory.
 - b. Change the service login user to a domain user.
 - c. After the integration of Security Center with Active Directory is complete, change the service login user to a domain user with the necessary rights to access Active Directory.

Note

Users in the same Windows domain as Security Center can log in to the Security Center server. Only the users in the user groups that are added to Security Center groups in Active Directory have the access to run the application.

2. Change the service login user from a local user to a domain user.
3. Integrate Genetec Security Center with Active Directory.

The purpose of integrating Security Center with Active Directory is to establish a unified user management system within the organization, and to simplify the initial Security Center setup. The system administrator can import any user groups that are defined in the Active Directory as Security Center users and user groups. After you enable Active Directory, only the imported users can run Security Center applications.

The Directory Service user must be a part of the same domain as Security Center and must have access to Active Directory. This user must also be a part of the local Administrators group on the server running the Security Center Directory.

For more information about this process, refer to the Genetec Security Center product documentation.

 - a. Launch Security Center Directory.
 - b. Browse to **Security Center Server Admin > Directory > Active Directory** and click **Activate**.
 - c. Select the Active Directory user groups that require access to Security Center.
 - d. Click **Activate**.
 - e. After integrating Security Center with Active Directory, add or delete Security Center users by using Active Directory.
4. Set Security Center permissions and privileges.

- a. Launch the Genetec Security Center Configuration tool.
- b. Set the credentials for each of the new entities that were imported from Active Directory.

The recommended best practice is to set credentials on the associated Active Directory group. Users who are members of the group inherit the group's credentials. In this way, no intervention is required when a new user is added to Active Directory.

User single sign-on for the associated Active Directory structure should not include Security Center.

If this is an Security Center implementation, after this configuration is complete, users no longer need to type their username and password when launching the following Security Center client applications:

- Configuration Tool
- Security Desk

- c. Select the **Use Windows credentials** option.

This option ensures that the username and password are inherited from the user's initial Windows domain login, and disables the username and password fields.

Dell EMC Surveillance Lab test environment

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

To test this solution, the Dell EMC Surveillance Lab uses the following solution components:

- 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)

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).

Watermarking and motion detection require additional vCPU and memory.

CHAPTER 3

Conclusion

This chapter presents the following topics:

- [Summary](#).....26

Summary

The Dell EMC Surveillance Lab performed comprehensive testing with Genetec Security Center against many EMC VNX and EMC VNXe arrays and Dell EMC 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.

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 will be fully validated on Generation 5 and Generation 6 hardware.

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

We demonstrated SecurID and seamlessly provided enhanced user login and permissions capabilities.

EMC VNX

Compared to traditional block-level storage, the use of storage pools to create LUNs within the VNX arrays greatly simplifies the configuration and increases the performance. Either iSCSI or FC can be implemented. FC performs better than iSCSI.

EMC VSS

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

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.

Dell EMC Isilon scale-out storage

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. Dell EMC recommends using SmartQuotas with Genetec Security Center as a best practice.

SV-16 and SV-32

The low-bandwidth, low-camera-count SV-16v2 and SV-32v1 were tested at their maximum bandwidth and camera count levels and succeeded without issues.