Surveillance
Dell EMC Storage with LENSEC Perspective VMS

Configuration Guide

H14767

REV 1.1

CONTENTS

CONTENTS

CHAPTER 1

Introduction

This chapter presents the following topics:

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 LENSEC Perspective VMS. This document is not a replacement for the LENSEC implementation guide nor is it a replacement for the *Dell EMC Storage with LENSEC Perspective VMS: Sizing Guide*.

Scope

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

The following Dell EMC storage systems have been tested:

- Dell EMC Isilon™

This guide supplements the standard *Dell EMC Isilon Storage Best Practices with Video Management Systems: Configuration Guide* and provides configuration information specific to LENSEC Perspective VMS.

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
- LENSEC-certified to install LENSEC Perspective VMS services
- 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 *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

There are many design options for a LENSEC Perspective VMS implementation. These design details are beyond the scope of this paper.

This guide is intended for systems integrators and architects, network IT planners, and system administrators. The guides assume that readers know what LENSEC Perspective VMS does and how it works, and know how to deploy and configure Windows IP networks.

A LENSEC Perspective VMS installation can consist of a single web server with single or multiple Archiver servers. You can configure Perspective VMS to manage a few cameras or thousands of cameras.

The following table describes the primary Perspective VMS services.

Table 1 Perspective VMS primary services.

Service	Description
Administration Service	Responsible for monitoring disk utilization and moving old archives to different offsite locations. It also ensures user synchronization between Active Directory and Perspective VMS.
Streaming Service	An intermediate agent between Perspective VMS and system cameras. It is responsible for handling streams and passing them to the system.
Archiving Service	Responsible for archiving image and video streams from cameras. It handles image and live recording requests from Perspective VMS users to capture video streams.
Health Monitor Service	Checks if system cameras defined in Perspective VMS are up and running. If not, the service notifies the user about the offline status of the camera in question. Generates health report that is related to cameras, servers, and other system components.
External System Service	Acts as an intermediary communication agent between Perspective VMS and third party software and hardware applications. This service is installed using a stand-alone, independent package from the main Perspective VMS setup.

The single web server runs the Administrative, Health Monitoring and External System services, while the Archiving and Streaming services runs on the Archiver and Reviewer servers.

The following figure represents the basic configuration that was tested in our lab for this solution.

Figure 1 LENSEC Perspective VMS architecture
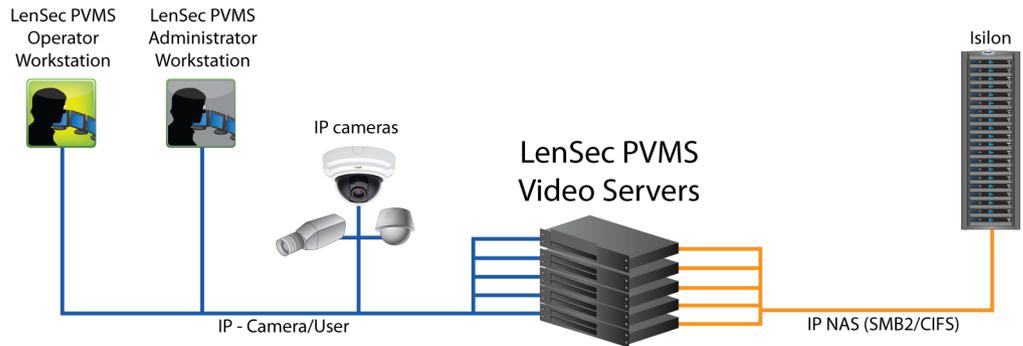
Isilon (NAS)

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

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. The clustered file system OneFS uses enables Isilon to handle these large volumes.

Large file system, small view (SmartQuotas)

Although it is possible to assign the full Isilon cluster file system to a single LENSEC 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 LENSEC 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 LENSEC 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 LENSEC Perspective VMS 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.

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.

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 LENSEC 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 LENSEC 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 LENSEC.

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 LENSEC Perspective VMS server and the Isilon cluster are part of the same Windows domain.

Partial Active Directory

> Where the LENSEC Perspective VMS servers are part of the Windows domain, but the Isilon cluster is administered locally.

Fully locally administered control

> Where the LENSEC Perspective VMS servers and the Isilon cluster are administered locally.

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 LENSEC 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 Perspective VMS 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 Perspective VMS 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 2 Isilon OneFS releases

Model	Firmware
X410	7.2.1
NL410	7.2.1
HD400	7.2.1

Table 3 LENSEC Perspective VMS releases

Release	Subrelease
LENSEC Perspective VMS	2.3.0.1

CHAPTER 3

Conclusion

This chapter presents the following topics:

Summary

We performed comprehensive testing with LENSEC Perspective VMS on a number of Dell EMC Isilon clusters. Depending on the implementation needs, you can use Dell EMC storage for LENSEC Perspective VMS. The LENSEC Perspective VMS architecture and product suite enables extreme scaling from a few cameras to tens of thousands of cameras using Dell EMC storage.

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 LENSEC Perspective VMS as a best practice.