Virtualizing Video Management Systems with Lenovo DE Series Storage

Design and Deployment Guide

Abstract

Video surveillance solutions using Lenovo® DE Series storage offer a highly scalable repository for video recordings, supporting large camera counts, megapixel resolutions, high frame rates, and long retention periods. Architecting a video management system solution in a virtualized environment further enhances scalability and supports clustering capabilities to provide high availability to meet the demands of video surveillance deployments.

First edition (July 2020)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

As the demand for video surveillance increases, enterprise-grade video surveillance solutions (VSSs) need to support the growing bandwidth requirements of high-resolution, high-quality video images. The reliability and availability of video surveillance are necessary for security and can also be extremely important for liability, critical business processes, and other commercial needs. To meet these demands, surveillance solutions must be:

- Highly available, providing a redundant, fault-tolerant environment across all components of the solution
- Scalable, supporting growth in video management, storage capacity, and performance
- Easy to implement and use

Virtualization and Lenovo DE Series storage offers the ideal solution to support video management system (VMS) operations at any scale. The infrastructure described in this report provides scalability and availability from compute to storage. This report highlights deployments using Windows Hyper-V.

For larger video surveillance installations that require multiple recording servers, a virtualized environment reduces the number of physical servers to install, monitor, and maintain. With Lenovo DE Series storage, you can run other applications beyond a video management system on the same physical servers. With high-performance, high-read/write applications such as virtual machines (VMs), and computer vision using all-flash drives and traditional video storage on high-capacity, lower-cost drives, DE Series storage offers a cost-efficient hybrid approach or a scaled deployment to fit the needs of any solution.

This technical report describes a solution framework for those who sell, design, or implement virtualized video surveillance solutions using DE Series storage. It defines the functional components required to build a virtualized video surveillance solution, with a deep focus on the processes that affect the video storage data path. The VMA deployment examples feature Milestone XProtect software.

2 Solution Design

Architecting a video surveillance storage solution for a virtual environment starts with determining expected recording data rates and retention from cameras to storage. Figure 1 shows the video recording data flow for a typical video surveillance solution. The design discussed in this document focuses on iSCSI SAN, but deployments are flexible enough to allow Fibre Channel connectivity if desired.

Figure 1) Video recording data flow example.

Isolating and alleviating bottlenecks along the recording data path is crucial in constructing a successful solution.

The following guides can help determine the appropriate network and compute needs. The next sections cover specific video surveillance requirements.

- Milestone Systems XProtect Corporate system requirements
- Windows Hyper-V requirements

2.1 Network Requirements

There are four distinct networks that are recommended for enterprise video surveillance deployments. Placing the iSCSI SAN and camera networks on dedicated private switches is crucial to separating congestion concerns across the network infrastructure. All networks that are capable of using jumbo frames should be configured to take advantage of larger TCP packet sizes. They must be configured on all endpoints and the switches between them.

- 10Gb iSCSI storage network:
  - Two 10Gb interfaces minimum from each hypervisor to DE Series SAN storage (high availability)
- 10Gb Ethernet camera network:
  - Two 10Gb interfaces from each hypervisor to the camera network (redundancy)
  - Each camera can use a different speed uplink, but the recording connection must be able to handle the aggregate camera traffic
- Management networks:
  - 1Gb network minimum for public network access from each hypervisor
  - 1Gb network minimum for private cluster communication and live migrations
  - Windows Hyper-V Live Migration Setup

2.2 Storage Requirements

VMS virtual environments require at least two performance tiers of storage. The first is a fast tier that serves the VM infrastructure, and the second is a high-capacity recording tier for camera recording. For example, each VM requires storage for the operating system and applications installation. Volumes as small as 100GB can be dedicated to each VM installation. Lenovo recommends placing all VM operating systems and applications (such as VMS) on flash (solid state) storage using centralized DE Series storage. This allows live VMs to seamlessly migrate compute and memory between hypervisors.

Note: A fast tier might also be required for recordings needed for real-time analytics workloads.

Figure 2) Left: SSD storage with VMs using a DE4000F (AFA) and recording data on a separate HDD tier using a D4000H 4U60. Right: DE4000H 4U60 hybrid configuration combining SSD and HDD into a single enclosure.

For video storage, see *DE Series for Video Surveillance Best Practices Guide* for information about sizing DE Series appropriately. DE Series storage offers the benefit of consolidating VM and application (video) storage in a single hybrid SAN storage system.

2.3 Host Requirements

For a highly available virtual solution, at least two physical servers are required. The CPU and memory required for each server must meet the requirements for the deployed VMs as well as any special requirements by the hypervisor. Section 2.4, Example Designs, outlines the server requirements for specific VMS deployments, and the general architecture can easily be extended to support additional applications and servers, such as badge readers or analytics software.

Table 1) Virtual machine examples.

VMS VMs	Security VMs	Other VMs
VMS security user interface	Security badge reader	Share network
VMS Manager	Security access control database	Domain controller
VMS management database	Security disaster management	DHCP
VMS camera recorders	Security photo database	TensorFlow
VMS logging	Security layout and planning	Ansible
VMS recording failover	–	–
VMS events	–	–

For the Windows Virtual Machine Manager, an additional system with at least 1GHz CPU, 1GB RAM, a network connection to each hypervisor, and 2GB of free space is required.

For the memory and processor requirements of the VMS VMs, see the best practices documentation for the VMS being deployed. The size and number of recording servers is based on the workload generated by the number of cameras and the maximum expected bit rate of each stream. To provide a highly available solution, each hypervisor in the cluster should be able to support the memory and processor requirements of an additional server in the installation. Lenovo recommends using identical hardware for all hypervisors.

2.4 Example Designs

This section describes some common hardware and software configurations found in enterprise video surveillance deployments. These examples are designed to be a guide for any combination of VMS and any hypervisor being deployed.

Windows Hyper-V Milestone Design Example

This subsection provides an example design for a virtualized deployment of the Milestone XProtect software. This example does not require a significant event server or log server, and it uses a local SQL instance to the management server. The example satisfies up to 600 2Mbps cameras with 60-day retention. It focuses on the video recording path, but other servers, such as a smart client, might be necessary for security personnel to monitor.

Milestone Physical Hardware

An Intel Xeon E3 or newer processor and NX/XD enablement fulfills Milestone VMS requirements and Microsoft processor requirements. Although 8GB of RAM would meet the minimum requirements for Milestone, for enterprise deployments Lenovo recommends a minimum of 32GB of memory per Windows node. This minimum requirement allows VMS components to be split into different VMs and provides full hardware redundancy across the servers. Use the following recommended server and storage requirements for a Milestone XProtect installation. A wide variety of hardware today exceeds these requirements. Here is an example of hardware selections.

Servers: Four identical Lenovo 2U servers, each with the following:

- 2x 2.0Ghz Xeon 6-core processors
- 64GB of memory
- 800GB internal storage for the Windows OS installation
- 4x 10Gb NICs (two for camera ingest, two for iSCSI SAN)
- 2x 1Gb NIC interfaces (public and private network)

Switches: Four switches that match the four virtual switches:

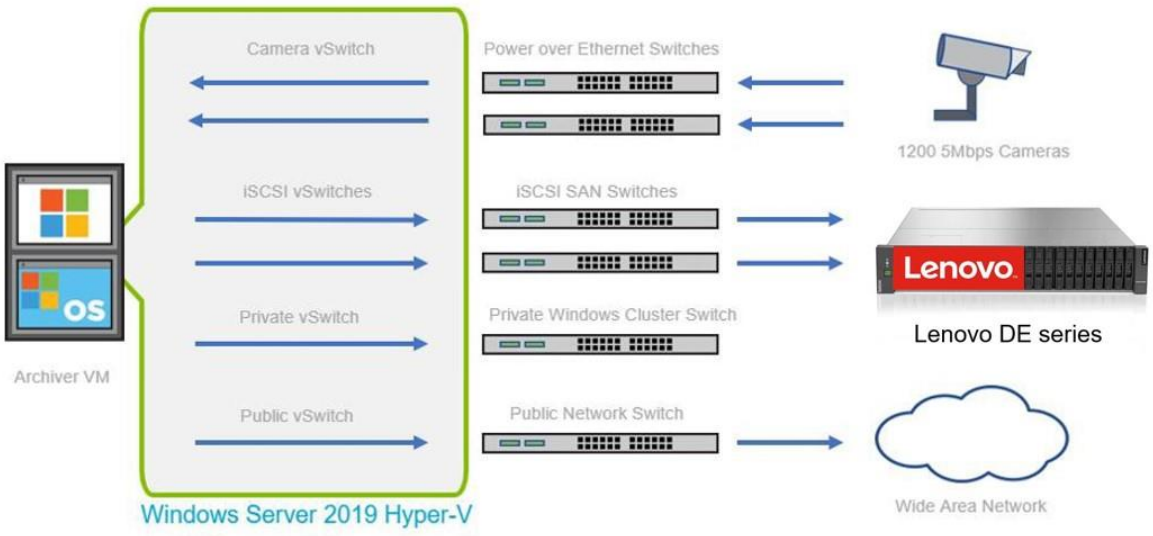
- One Power over Ethernet (PoE) switch (connecting the cameras to the Windows nodes)
- One 10Gb switch (connecting the iSCSI SAN to the Windows nodes)
- Two 1GB switches for private and public management networks

DE Series hybrid storage system:

- 1 DE Series DE4000H 4U60, expansion shelf (DE600S), 115x 12TB HDD drives (video storage), 5x 800GB SSD drives (OS, application storage)

Additionally, a maximum of 200 PoE cameras per VM should be connected. Figure 3 shows an example of the components that each Windows Server is exposed to.

Figure 3) Example of virtual network components that each Windows Server uses.



Hyper-V VMs

Physical Windows servers host the VMs described in Table 2. This subsection focuses on VMs along the recording data path.

Table 2) Physical Windows servers that host the VMs.

Server	CPU	Memory	OS/Application Storage	Video Storage
Management	4 cores	8GB	DE Series 200GB SSD	None
Recording 1	8 cores	12GB	DE Series 200GB SSD	DE Series 300TB HDD
Recording 2	8 cores	12GB	DE Series 200GB SSD	DE Series 300TB HDD
Recording 3	8 cores	12GB	DE Series 200GB SSD	DE Series 300TB HDD

Note: Recording server considerations:

- Approximately four CPU cores per 100 cameras without motion detection.
- Memory starts at 4GB and increases by about 4GB per 100 cameras.
- Raw video storage requires 2Mbps at 60-day retention. 1.296TB of storage is required per camera.

Hyper-V and Milestone Software

- Microsoft Windows Server 2019 Datacenter
- Hyper-V Manager 10.0.17763.1
- Failover Cluster Manager 10.0
- Windows Server 2019 Datacenter (VM)
- Active Directory Domain Controller (DNS/DHCP recommended)
- Milestone XProtect Corporate 2020 R1

3 Deployment Guide

After the video surveillance requirements have been evaluated and the solution design is complete, the solution is ready for deployment. This section describes the configuration steps to deploy the VMS in a virtual environment, using Hyper-V examples and featuring Milestone deployment steps.

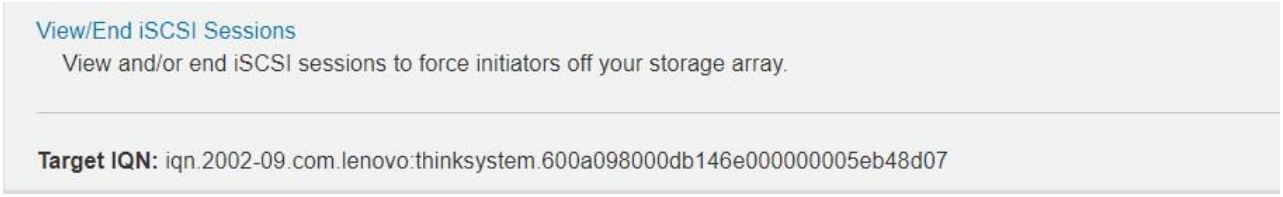
3.1 Network Configuration

Configure the appropriate switches, including SAN switches, camera ingest switches, and host management switches. Here are a few general switch recommendations prior to deployment.

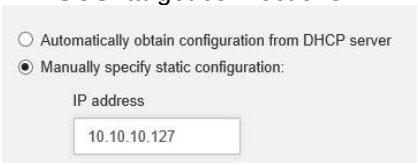
- Lenovo recommends separate switches for SAN, camera ingest, and host management.
- The camera switches usually require Power over Ethernet capability.
- Priority flow control must be disabled across the SAN network.
- Lenovo recommends enabling jumbo frames (MTU 9000) across all networks if possible.

Configuring DE Series Storage Networking

1. To configure DE Series storage networking, select and configure IPv4 iSCSI ports from Lenovo ThinkSystem System Manager system settings.
2. Save the Target IQN for later hypervisor iSCSI connection.



3. Next, select Configure iSCSI Ports to populate the network addresses. Repeat to enable at least two iSCSI target connections.



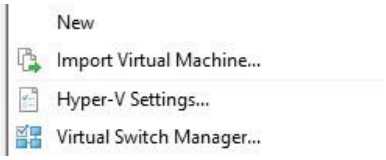
3.2 Hypervisor Virtual Switches

Virtual switches provide a logical extension of all the physical networks in the virtualization infrastructure. This infrastructure includes SANs, camera networks, and public networks. Each VM can then be mapped to any or none of these networks as the deployment requires.

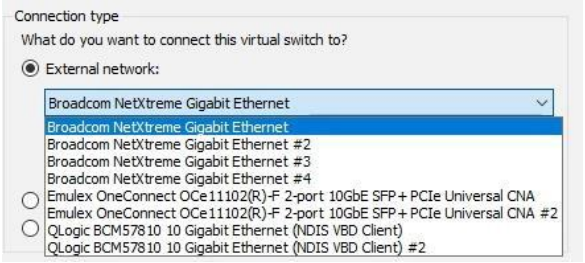
Configuring Windows Virtual Switches

Each network connection being used by any VM must have its own virtual switch. There should be a public and private network as well as a network for iSCSI and camera traffic. See Create a Virtual Network.

1. Open the Hyper-V Manager. In the Actions pane, select Virtual Switch Manager.



2. Select New Virtual Network Switch > External. Click Create Virtual Switch.
3. Select a network port from the drop-down list to connect to the virtual switch.
4. Set the virtual switch name at the top of the window and use the same name for shared networks across the multiple servers in the cluster.



Note: If multiple ports need to be teamed for additional bandwidth, this must occur in the normal Windows Adapter Settings interface before setting up the virtual switch. See NIC Teaming.

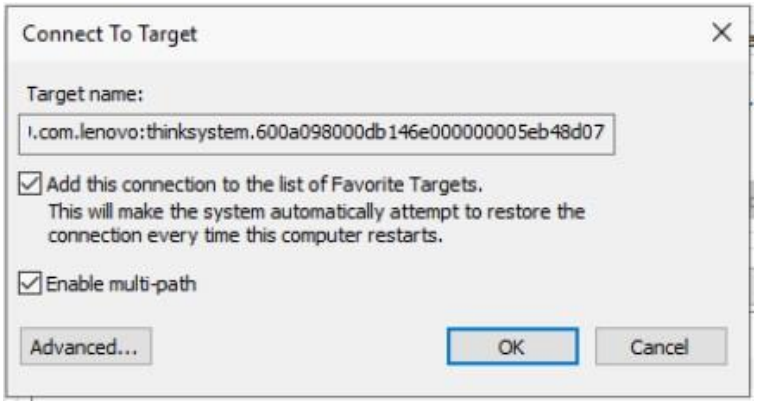
3.3 DE Series iSCSI SAN Configuration

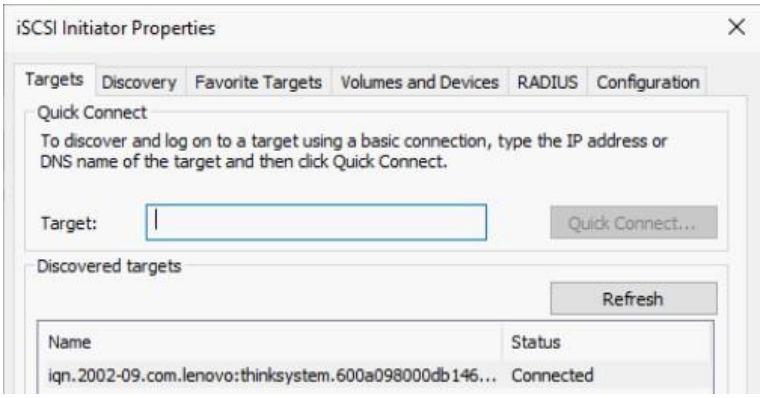
This section is a brief overview of iSCSI express configuration for Windows. For additional information, see *ThinkSystem DE Series Hardware Installation and Maintenance Guide for 2U and 4U Enclosures*, and *ThinkSystem DE Series Software Deployment and Configuration Guide* which describes both operating system configurations in more detail. Both guides and more support resources can be found on DE support center. For connection troubleshooting, see section 4, Frequently Asked Questions.

Configuring Windows iSCSI

Windows requires DE Series DSM for multipathing. See Storage Manager for the downloadable package.

1. Follow the executable instructions to enable multipathing on Windows.
2. Use the iSCSI Initiator UI (or PowerShell cmdlets) to create a discovery portal to a single DE Series target IP address.
3. Make sure that your host's initiator name in the Configuration tab is the same initiator set on your host in ThinkSystem Storage Manager.
4. In the Targets tab, select the IQN of your storage array. Under Properties, create your iSCSI sessions to the controllers. Make sure that the Enable Multipath box is checked.





3.4 DE Series Storage Creation

Provisioning VMs and Video Storage

To provision the VMs, follow these steps.

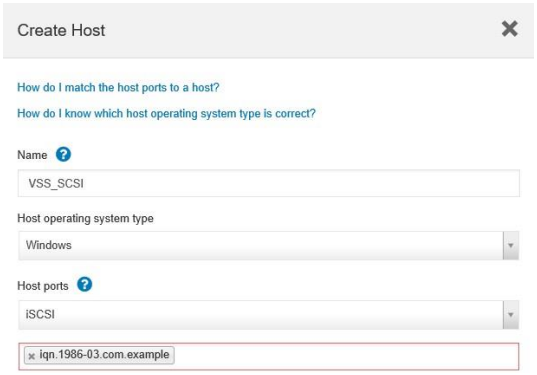
1. Create a RAID 6 group with five SSDs and then select Volume Group > Create Volumes.
2. Create a single volume and then select Map Later.

To provision the video storage, follow these steps.

1. Create a pool with all HDDs and then select Pool > Create Volumes.
2. Create an appropriate number of volumes based on the sizing guidelines and then select Map Later.

Mapping Hosts

1. In ThinkSystem System Manager, go to the Hosts tile and select Create Host.
2. Complete this operation on each hypervisor: Select Create Host, supply the host name, and select host type and host identifier.



3. After creating all hosts, complete the following steps:
   a. Select Create > Host Cluster and then add all hypervisors to the host cluster.
   b. Enter a name for the cluster and complete the operation.
   c. Assign volumes to the cluster object.
   d. Select the cluster object from the table and then select Assign Volumes.
   e. Select the SSD volume and all VSS volumes.

The storage configuration is complete. All the mapped volumes are available to each hypervisor.

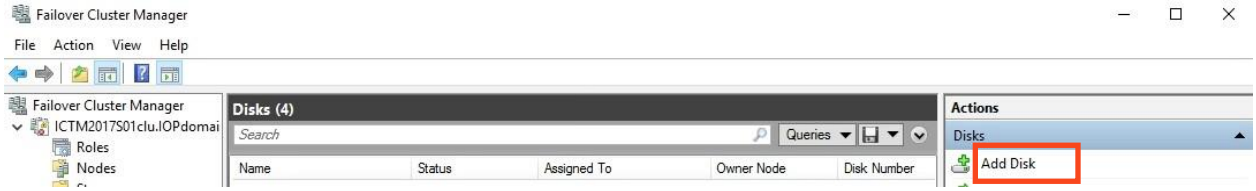
3.5 DE Series Storage Mapping

Windows

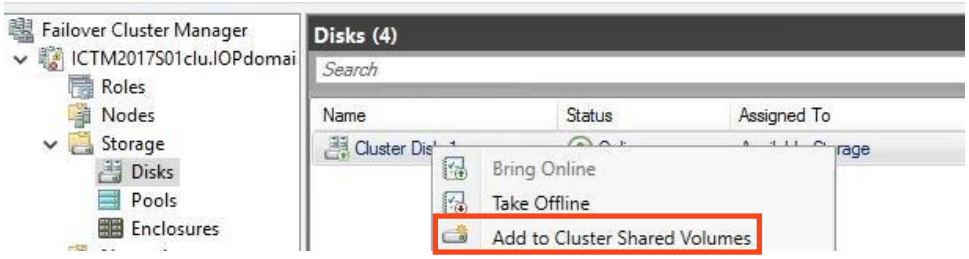
Windows might need to rescan storage before the newly mapped volumes will be accessible by the operating system. This can be done by using disk management.

Adding Cluster Shared Volumes

1. Before adding a VM SSD or VSS HDD to the cluster, format it as NTFS. In the Failover Cluster Manager under Disks, choose Add Disk on the far right.



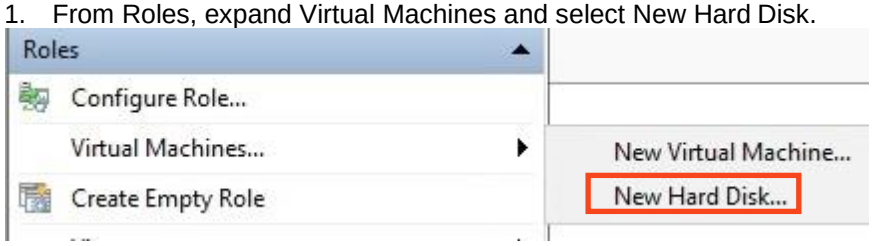
2. Select a disk from the list. After it is added to the disk list, right-click it and select Add to Cluster Shared Volumes.



The disk is now mounted on all nodes in the cluster to a directory in `C:\ClusterStorage`.

Creating a Virtual Hard Disk

1. From Roles, expand Virtual Machines and select New Hard Disk.



2. The maximum size for a VHDX is 64TB. Use all the available space from your cluster storage volumes located at `C:\ClusterStorage`.

3.6 Virtual Machine Creation

1. Create a new VM for the management, recording, archiving, and any other desired components that have the recommended compute, memory, and storage capacities. The VM configuration is deployed using the design requirements recommended.
2. See the Windows document Create a Virtual Machine in Hyper-V.

3. Complete this operation for each server being deployed.

3.7 Milestone Video Management Configuration

For more information about the workflows used in the deployment, see the following documentation:

- Milestone Systems Administrator Manual
- Milestone Systems Getting Started Guide

1. Use the Milestone Systems Administrator Manualto install the Milestone XProtect Management Client software.
2. Attach and use the domain account for all Milestone installations.

   When the management server completes installation, the Management Server task becomes viewable in the task bar, and a Client Launcher shortcut is added to the desktop and the Start menu. The Milestone Systems web interface becomes available at http://<management server>/installation/admin/default-en-us.htm.

The web interface provides downloads for Milestone software on additional servers, such as the smart client and recording server software.

Scaling the Recording Server

The recording server is the most likely server to require scaling (that is, deployments of multiple recording server virtual machines). First, clone the archiver (template or export) by using the virtual machine manager.

For Windows Hyper-V, see Export and Import Virtual Machines. Use import type Copy the Virtual Machine.

Attaching Storage to Recording Servers

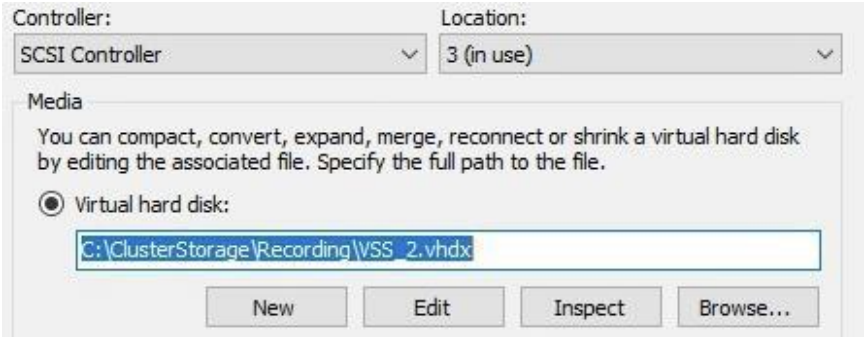
Before you begin, make sure that the VM is powered down. To attach all the hypervisor volumes to the archivers, follow these procedures.

Windows Recording Storage

1. In Failover Cluster Manager, right-click the recording server VM and select Settings. Under Hardware,

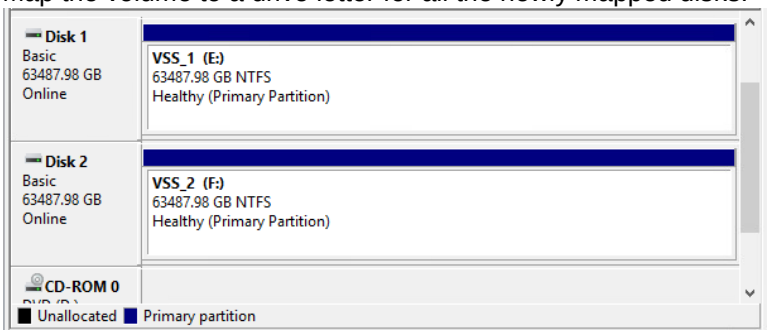
select SCSI Controller. Select Hard Drive and click Add.

2. Browse for the VHDX drives in the cluster shared volume. Add as many disks as required by the recording server.



Formatting Recording Server Drives

From the archiver server disk manager, right click the new disks, select Initialize, and create a volume. Map the volume to a drive letter for all the newly mapped disks.



Installing a Recording Server

1. To install a recording server, open a browser and connect to http://<management server>/installation/admin/default-en-us.htm.

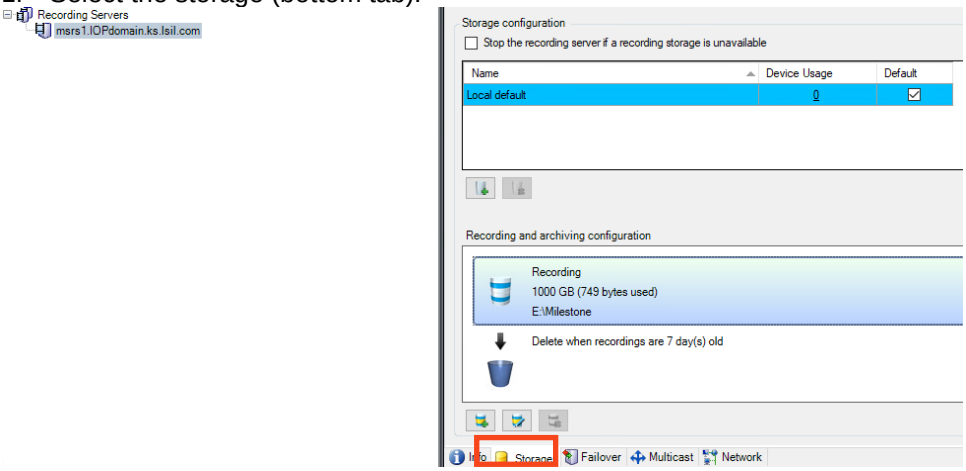
2. Download and install the recording server software. Use the same domain account as the installed management server. The recording server should be installed with up to four instances, using unique network adapters. When the installation is complete, a recording server task becomes available in the task bar in which you can view the running status and configuration of the software.

Enabling Management Server Camera Storage and Retention

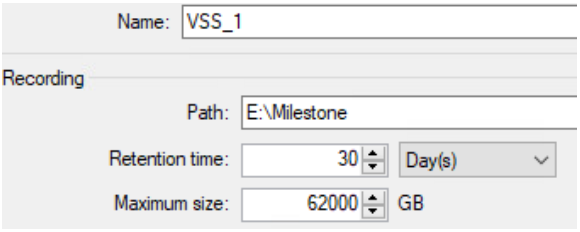
To enable management server camera storage and retention, log into the XProtect Management Client, select Recording Servers (left), and then select a recording server.

Perform these steps on all recording servers.

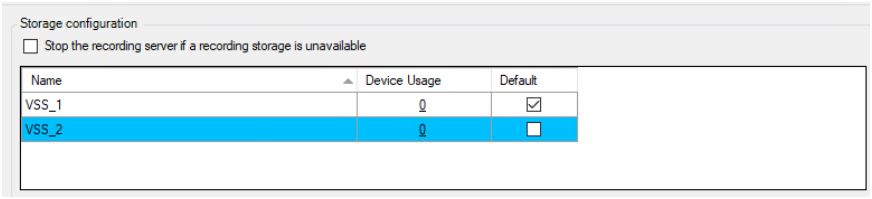
1. Select the storage (bottom tab).



2. Edit the default disk to increase the size to maximum (62TB). Change the retention to 90 days.



3. (Optional) Change the name to match the disk name.
4. Add the remaining VSS volumes in the same way.

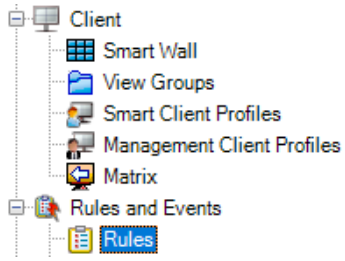


The recording storage is now set. Storage is selected to accommodate the expected retention period as cameras are added.

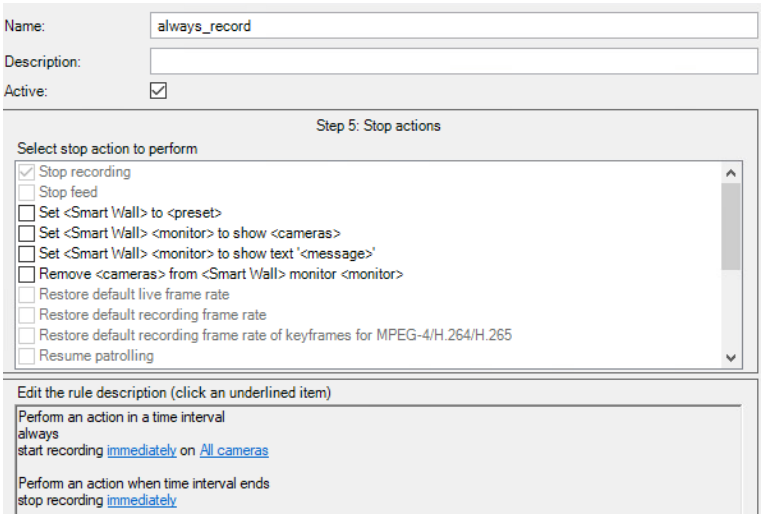
Adding a Recording Rule

To make every camera begin recording when added, you must set a rule.

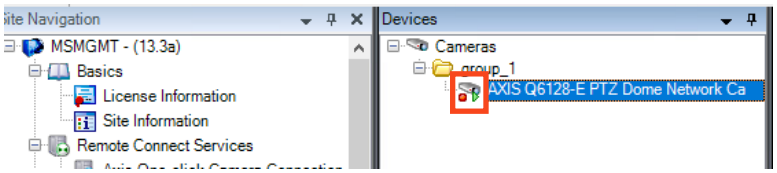
1. Under Rules and Events, select Rules.



2. Make a rule with a time interval that always occurs, starts immediately, and executes to a device. Set the device to All Cameras.



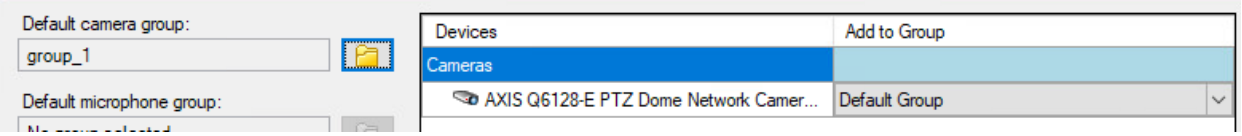
A recording symbol (red circle) is applied to each camera that is recording.



Connecting Cameras

To connect cameras, from the Milestone XProtect Management Client, select Recording Servers in the left pane. Right-click the recording server to add the camera to and select Add Hardware.

Some workflows allow multiple cameras. Use the one that fits your needs. The camera addition process allows cameras to be grouped as desired. This grouping can be used to describe which storage destination the camera is assigned to. Each camera can change its target if necessary. About 30 cameras should be assigned to each VSS volume, so that there is enough storage to archive the desired 90-day retention period.



If the camera is active, a view is displayed in the Preview pane.

4 Frequently Asked Questions

The following questions and answers address some issues you might encounter when setting up or using this solution.

Can I use ReFS instead of NTFS in Windows?

Answer: Both within the VMs and as part of Hyper-V, there is no limitation from storage about which file system is chosen. However, some file systems might support features that others do not. For instance, ReFS does not have support for removable media and cannot be used as a root disk. For more differences between ReFS and NTFS, see ReFS Overview. Additionally, VMS providers might have requirements and limitations.

Milestone does not support ReFS.

What file system can I deploy on video recording volumes?

Answer: The video management vendor supports any file system. The storage is presented to the VM as a block device, such as a hard drive, and should be formatted with a file system before using.

I don’t see any LUNs mapped during host discovery. What can I do to troubleshoot?

Answer: From the host, you should verify that you can properly ping the storage system, both with the default (usually 1500 byte) MTU and a jumbo frame (MTU 9000). If a ping succeeds with the default MTU, but fails with a jumbo frame, there is a component in your network that does not support jumbo frames and needs to be addressed. If a ping fails, there is a disconnection along the network path. If iSCSI fails to discover or connect, check the CHAP settings on the initiator (host) and target (storage). A one-way or bidirectional password might be required.

Windows using the command prompt:

```
ping -S <src> <dst>
ping -S <src> -l 9000 <dst>
```

5 Conclusion

A virtualized video surveillance solution using Lenovo DE Series storage systems is a highly available solution with redundant server and storage hardware. Virtualized deployments also offer the benefit of fewer physical servers to manage and monitor. With the explosion of growth in video bandwidth, a virtualized environment makes it easy to add surveillance capabilities with additional recoding servers and video storage. The solution also offers the flexibility to support other applications in addition to the VMS solution on the same hardware, reducing the total cost of ownership.

Where to Find Additional Information

To learn more about the information that is described in this document, review the following websites:

- DE series and SAN OS software Resources
  https://datacentersupport.lenovo.com/
- ThinkSystem Storage Documentation
  https://thinksystem.lenovofiles.com/storage/help/index.jsp
- Milestone
  https://www.milestonesys.com/support/
- DE series support center
  https://datacentersupport.lenovo.com/us/en/solutions/de-series-support-home

Contacting Support

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to https://datacentersupport.lenovo.com/serviceprovider and use filter searching for different countries. For Lenovo support telephone numbers, see https://datacentersupport.lenovo.com/supportphonelist for your region support details.

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.

8001 Development Drive

Morrisville, NC 27560

U.S.A.

Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT,

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

