



Technical Report

Virtualizing video management systems with NetApp E-Series storage

Design and deployment guide

Mitch Blackburn, Charles Cummins, Luis Salmeron, NetApp
October 2021 | TR-4818

Abstract

Video surveillance solutions using NetApp® E-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.

TABLE OF CONTENTS

Introduction	3
Solution design	3
Network requirements	4
Storage requirements	4
Host requirements	5
Example designs	6
Deployment guide	10
Network configuration	10
Hypervisor virtual switches	11
E-Series iSCSI SAN configuration	12
E-Series storage creation	14
E-Series storage mapping	15
Creating a VM	17
Configuring milestone video management	18
Configuring Genetec video management	23
Frequently asked questions	26
Conclusion	27
Where to find additional information	27
Version history	28

LIST OF TABLES

Table 1) VM examples.....	5
Table 2) Servers and VMs.....	8
Table 3) Physical Windows servers that host the VMs.....	9

LIST OF FIGURES

Figure 1) Video recording data flow example.....	3
Figure 2) Left: SSD storage with VMs using an EF300 and recording data on a separate HDD tier using an E2860. Right: E2860 hybrid configuration combining SSD and HDD into a single enclosure.....	5
Figure 3) VMware archiver networks.....	7
Figure 4) VMware archiver storage.....	7
Figure 5) Example of virtual network components that each Windows Server uses.....	9

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 NetApp® E-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 and VMware.

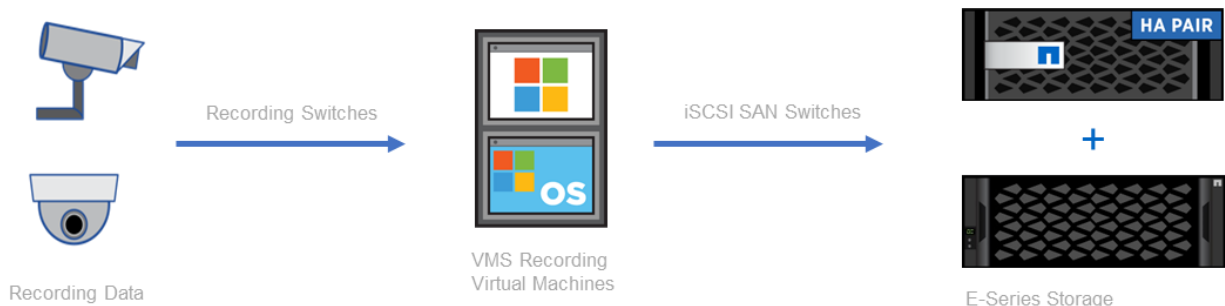
For larger video surveillance installations that require multiple recording servers, a virtualized environment reduces the number of physical servers to install, monitor, and maintain. With NetApp E-Series storage you can run other applications beyond a video management system on the same physical servers. 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, E-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 E-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 Genetec Security Center and Milestone XProtect software.

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](#)
- [Genetec Security Center system requirements](#)
- [Windows Hyper-V requirements](#)
- [VMware vSphere documentation](#)
- [NetApp Interoperability Matrix Tool](#)

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 can use 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.

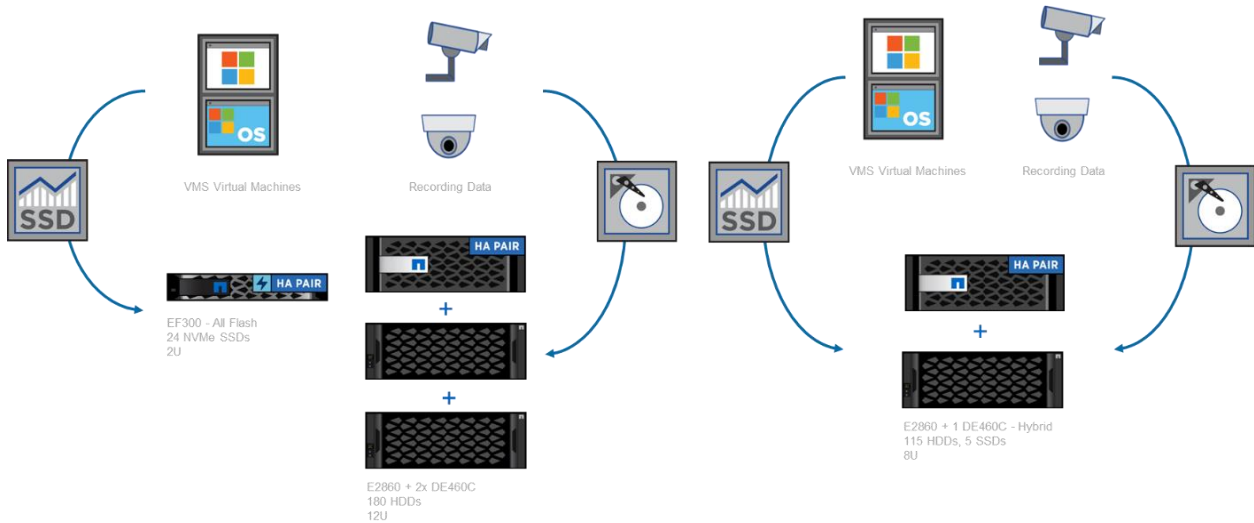
- 10Gb iSCSI storage network:
 - Two 10Gb interfaces minimum from each hypervisor to E-Series SAN storage (high availability)
- 10Gb Ethernet camera network:
 - Two 10Gb interfaces from each hypervisor to the camera network (redundancy)
 - Each camera can use a different speed uplink, but the recording 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
 - [Networking Best Practices for vSphere vMotion](#)
 - [Windows Hyper-V Live Migration Setup](#)

Storage requirements

VMS virtual environments require at least two performance tiers of storage, see Figure 2. 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. NetApp recommends placing all VM operating systems and applications (such as VMS) on flash (solid state) storage using centralized E-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 an EF300 and recording data on a separate HDD tier using an E2860. Right: E2860 hybrid configuration combining SSD and HDD into a single enclosure.



For video storage, see [TR-4825 Video Surveillance Best Practices](#) for information about sizing E-Series appropriately. E-Series storage offers the benefit of consolidating VM and application (video) storage in a single hybrid SAN storage system.

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. The Example Designs section below 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, see Table 1.

Table 1) VM 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 VMware vSphere client or 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. NetApp recommends using identical hardware for all hypervisors.

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.



VMware Genetec design example

This subsection provides an example design for a 1,200 camera Genetec Security Center 5.9 deployment on VMware ESXi 6.7u3. This example does not require a significant event server or log server and uses local SQL instances for each archiver. The example satisfies 5Mbps cameras with 30-day retention. It focuses on the video recording path. Other servers, such as a Security Center server, might also be necessary, but they are not covered at length.

Genetec physical hardware

An Intel Xeon E3 or newer processor and NX/XD enablement fulfills the directory server requirements. Although 8GB of RAM would meet the minimum requirements, for enterprise deployments NetApp recommends a minimum of 32GB of memory per ESXi node. This minimum requirement allows VMS components to be split into different VMs and provides hardware redundancy across the servers. A wide variety of hardware today meets these requirements. Here is an example of hardware selections.

Servers: Three identical Fujitsu PRIMERGY RX4770 M4 2U servers, each with the following:

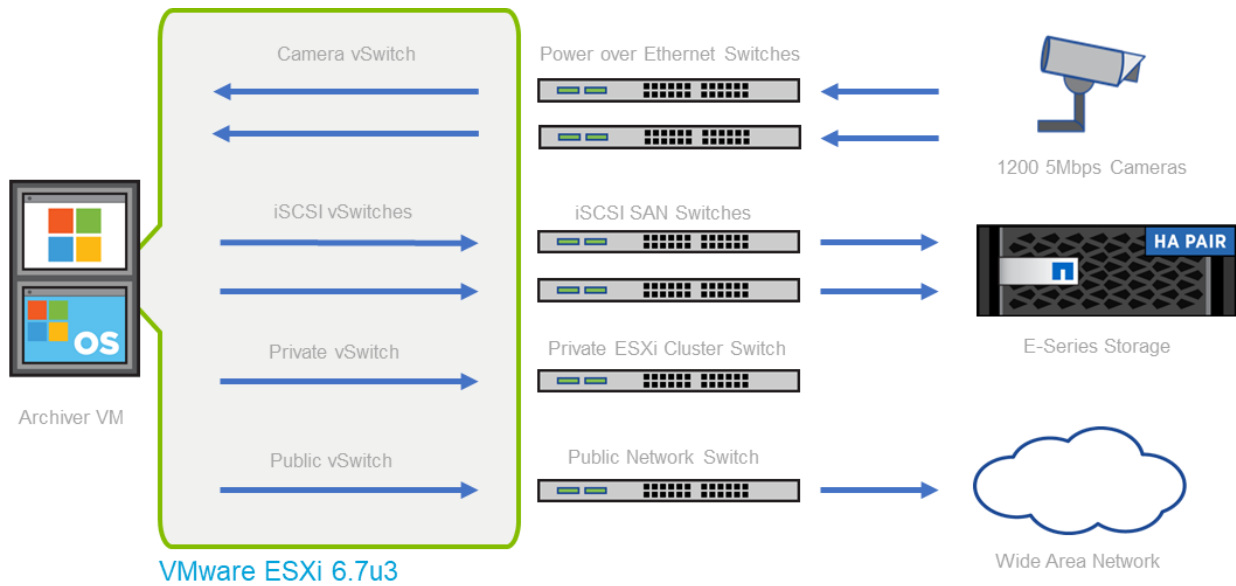
- 4x Xeon 2.7Ghz 24 core processors
- 128GB of internal ECC memory
- 1x 800GB internal storage for the ESXi OS installation
- 4x 10Gb NICs (two for camera ingest, two for iSCSI SAN)
- 2x 1Gb NIC interfaces (public and private VMware network)

Switches: Six switches, attached to each server:

- 2x Cisco Power over Ethernet (PoE) switches, 10G uplink capable
- 2x Cisco 10Gb iSCSI SAN switches
- 1x Cisco 1Gb private network switch
- 1x Cisco 1Gb public network switch

The switch configuration has symmetric camera ingest and archiving output to sustain the expected 6Gbps bandwidth requirements and headroom to withstand any single point of failure. The same SAN network also manages VM storage for this example, see Figure 3. This might be necessary to separate SAN networks if VMs exercise heavy analytic workloads.

Figure 3) VMware archiver networks.

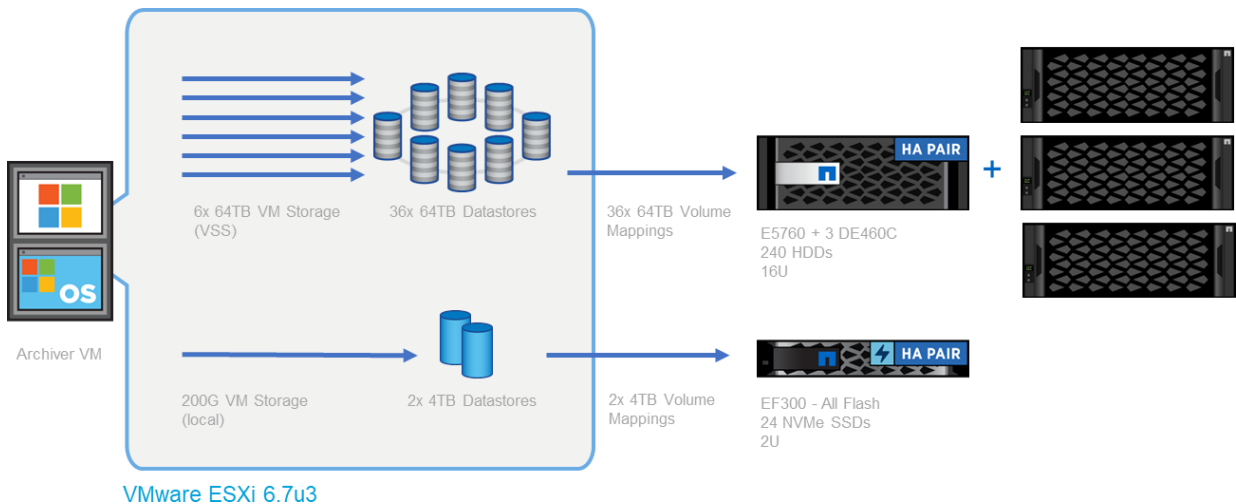


Storage: Two NetApp E-Series storage systems (Figure 4):

- 1x E-Series E5760, 3 expansion shelves (DE460C), 240x 12TB HDD drives (video storage)
- 1x E-Series EF300, 12x 1.9TB NVMe SSD drives (OS, application storage)

VMware limits a single hard disk at 64TB requiring multiple volume mappings from storage into each VM. For each archiver instance, six 64TB disks are mapped into VMware, with each VM mapping consuming the entire datastore. A separate datastore contains flash storage from the EF300 and presents only 200GB for the VMs OS or application to consume.

Figure 4) VMware archiver storage.



In addition to servers, network, and storage, 1,200 PoE cameras and a VMware vSphere client host are required. Figure 3 and Figure 4 show a single archiver instance. The deployment consists of six archiving VMs that function identically.

VMware VMs

Physical ESXi servers host the VMs, such as the examples in Table 2. This section focuses on VMs along the recording data path and their requirements for Genetec Security Center to accommodate 1,200 high-definition cameras.

Table 2) Servers and VMs.

Server	CPU	Memory	OS or Application Storage	Video Storage
Directory	8 cores	8GB	E-Series 200GB SSD Volume	None
Archiver 1	8 cores	12GB	E-Series 200GB SSD Volume	6x 64TB HDD Volumes
Archiver 2	8 cores	12GB	E-Series 200GB SSD Volume	6x 64TB HDD Volumes
Archiver 3	8 cores	12GB	E-Series 200GB SSD Volume	6x 64TB HDD Volumes
Archiver 4	8 cores	12GB	E-Series 200GB SSD Volume	6x 64TB HDD Volumes
Archiver 5	8 cores	12GB	E-Series 200GB SSD Volume	6x 64TB HDD Volumes
Archiver 6	8 cores	12GB	E-Series 200GB SSD Volume	6x 64TB HDD Volumes

Archiving server additional information:

- Approximately four CPU cores per 100 cameras without motion detection
- Memory starts at 4GB and increases by about 4GB per 100 cameras
- 200 cameras on each archiver
- Approximately 33 cameras are mapped to every 64TB VSS storage drive

Genetec software

- VMware ESXi 6.7U3
- vSphere Client 6.7.0.40000
- VMware Tools 10.2.5
- Windows Server 2019 Datacenter (VMs)
- Active Directory Domain Controller (DNS/DHCP recommended)
- Genetec Security Center 5.9

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 NetApp 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 Dell 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:

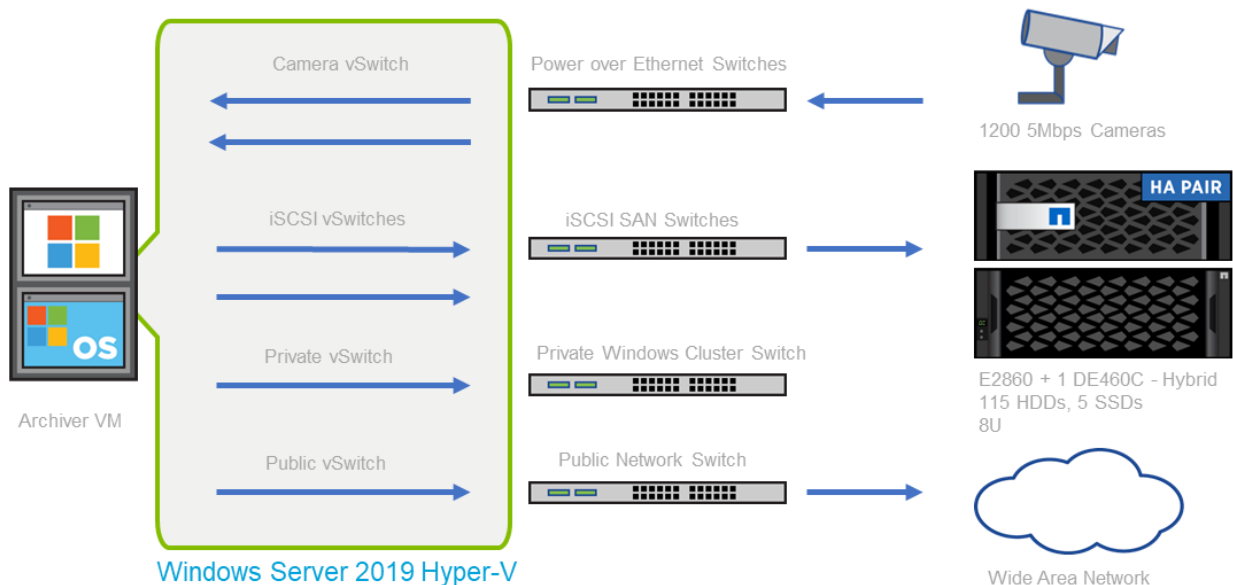
- 1x Cisco Power over Ethernet (PoE) switch (connecting the cameras to the Windows nodes)
- 1x Cisco 10Gb switch (connecting the iSCSI SAN to the Windows nodes)
- 2x Cisco 1GB switches for private and public management networks

Storage: One E-Series hybrid storage system, Figure 5:

- 1x E-Series E2860, expansion shelf (DE460C), 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 5 shows an example of the components that each Windows Server is exposed to.

Figure 5) Example of virtual network components that each Windows Server uses.



Hyper-V VMs

Physical Windows servers host the VMs described in Table 3. This subsection focuses on VMs along the recording data path.

Table 3) Physical Windows servers that host the VMs.

Server	CPU	Memory	OS/application storage	Video storage
Management	4 cores	8GB	E-Series 200GB SSD	None
Recording 1	8 cores	12GB	E-Series 200GB SSD	E-Series 300TB HDD
Recording 2	8 cores	12GB	E-Series 200GB SSD	E-Series 300TB HDD
Recording 3	8 cores	12GB	E-Series 200GB SSD	E-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

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 and VMware examples and featuring both Genetec and Milestone deployment steps.

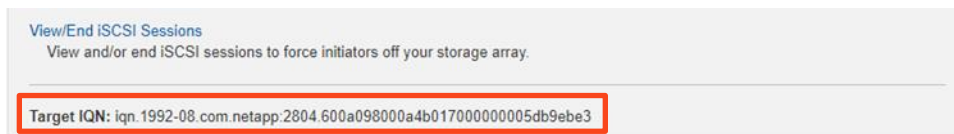
Network configuration

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

- NetApp 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.
- NetApp recommends enabling jumbo frames (MTU 9000) across all networks if possible.

Configuring E-Series storage networking

1. To configure E-Series storage networking, select and configure IPv4 iSCSI ports from NetApp SANtricity® 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.



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 VMware vSwitches

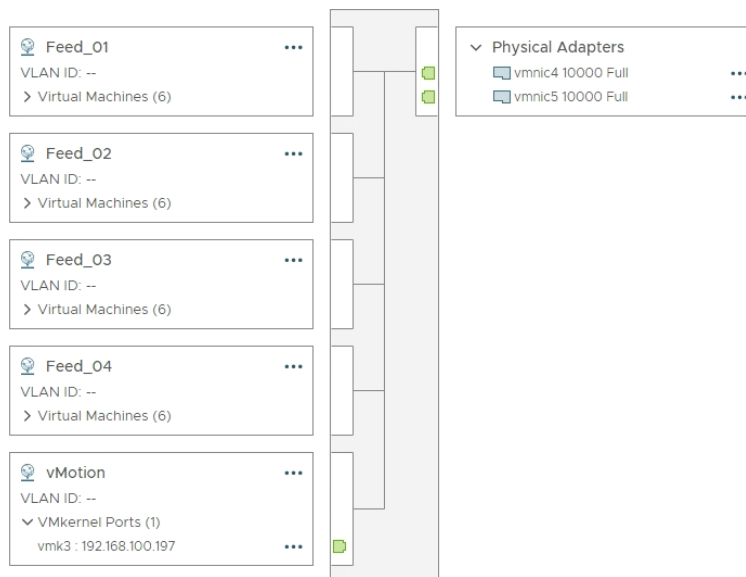
1. Configure at least four VMware vSwitches. Some of these switches might already be configured by the hypervisor. See [Create a vSphere Standard Switch](#).
2. Check that at least one physical adapter is present on this vSwitch for public access. A management vSwitch services public or local networks. This vSwitch is typically already created.



3. Check that a management vSwitch exists to service private VMware needs (for example, vMotion). This vSwitch also typically has one physical adapter but might require more, depending on expected traffic load.



4. Check that there is a camera vSwitch to service camera ingest. NetApp recommends a minimum of two 10Gb-capable physical adapters, if not for expected ingest, then for redundancy. Internal connections require up to four VM ports to service VM requirements.



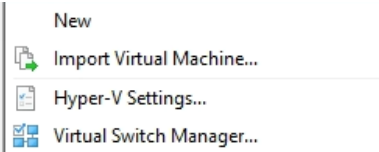
- Check that there are two iSCSI vSwitches to service SAN requirements. At least one 10Gb-capable physical adapter is required for each vSwitch to provide dual controller access.



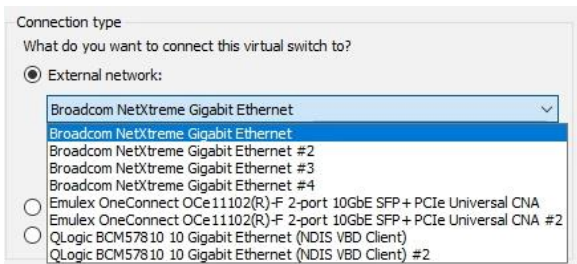
Configuring Windows virtual switches

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](#).

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



- Select New Virtual Network Switch > External. Click Create Virtual Switch.
- Select a network port from the drop-down list to connect to the virtual switch.
- 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.



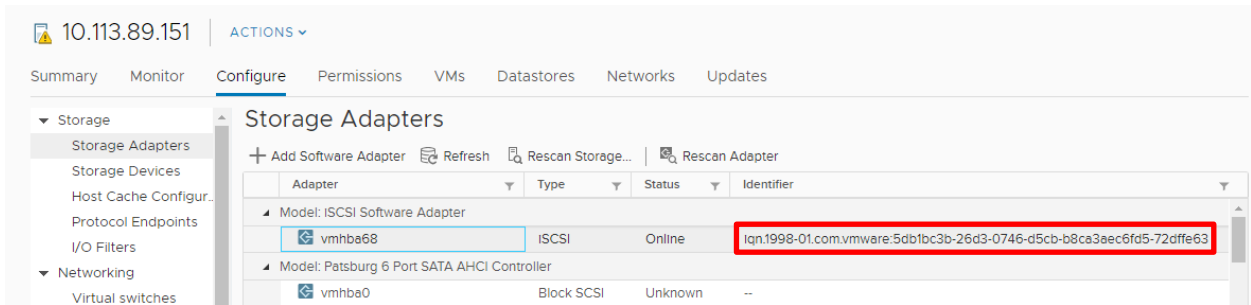
Note: If multiple ports need to be teamed for additional bandwidth, this must occur in the normal Windows Adapter Settings interface before setting up the virtual switch. See [NIC Teaming](#).

E-Series iSCSI SAN configuration

This section is a brief overview of iSCSI express configuration for VMware and Windows. For additional information, see [OS Express Configuration](#), which describes both operating system configurations in more detail. For connection troubleshooting, see [Frequently asked questions](#).

Configuring VMware iSCSI

- To configure VMware iSCSI to access an ESXi Host, select the Configure tab and select Storage Adapters in the left pane. Perform this step on each host.



2. Select iSCSI vmhba and then select Static Discovery in the lower tab.

Note: Write down vmhba 'Identifier Column'.

3. Add Static Target Server (repeat for four connections). To add a target iSCSI port address, use Target IQN as the iSCSI target name.

Add Static Target Server | vmhba68 X

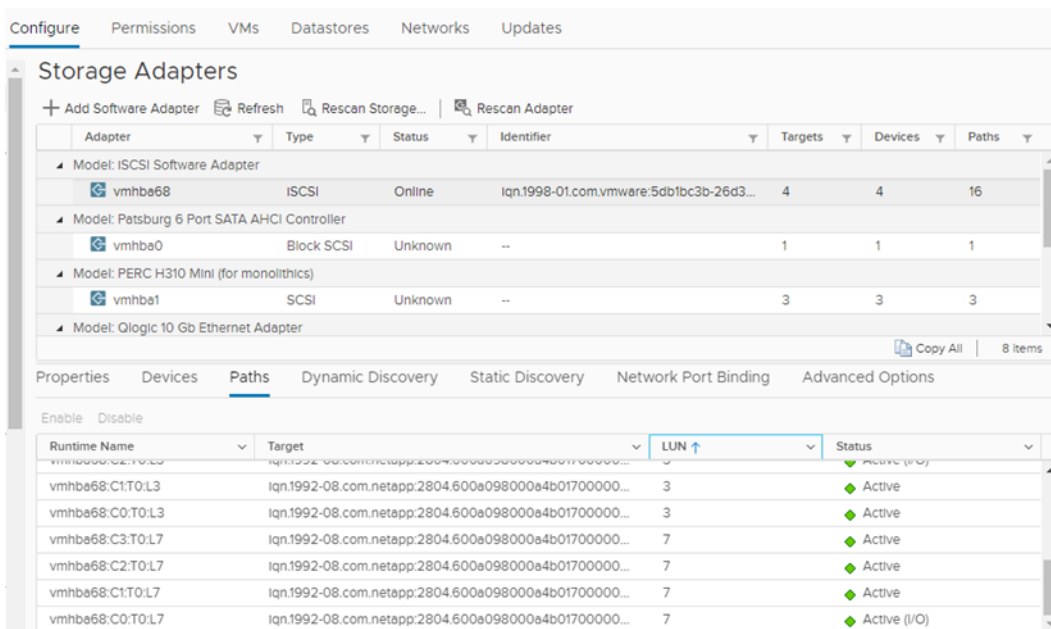
iSCSI Server: 10.10.10.127

Port: 3260

iSCSI Target Name: tapp:2804.600a098000a4b017000000005db9ebe3

☐ Inherit authentication settings from parent

4. Click the Rescan Storage button on the top left. Target LUN 7, vmhba##:C#:T#:L7, is displayed in the Paths tab.



Note: When configured properly, at least two paths per LUN are displayed, labeled Active and Active (I/O).

Configuring Windows iSCSI

Windows requires E-Series DSM for multipathing. See [Configure the multipath software](#) 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 E-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 SANtricity 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.

Target name:

.992-08.com.netapp:5700.600a098000af5ca4000000005e5a149b

☒ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

☒ Enable multi-path

Targets | Discovery | Favorite Targets | Volumes and Devices | RADIUS | Configuration

Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target: Quick Connect...

Discovered targets

Refresh

Name	Status
iqn.1992-08.com.netapp:5700.600a098000af5ca40000...	Inactive

E-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.

Note: VMware limits volume sizes to 64TB.

Mapping hosts

To map the hosts, complete the following steps:

1. In SANtricity 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.

Name 

Host operating system type


VMware







Host ports 



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.

HOSTS

[Learn More >](#)

Filter 

Create	Assign Volumes	Unassign Volumes	View/Edit Settings				Delete
Name	Type	Associated Objects	Total Assigned Volumes	Reported Capacity (GiB)	Host Type	Edit	
ictm0708s02	 Cluster	2 Host(s)	0	0.00	VMware		
ictm0708s02h1	 Host Member	ictm0708s02	0	0.00	VMware		
ictm0708s02h2	 Host Member	ictm0708s02	0	0.00	VMware		

Total rows: 3  

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

E-Series storage mapping

VMware

For storage convenience, configure your system by using VMware datastore. The process begins with scanning for mapped storage.

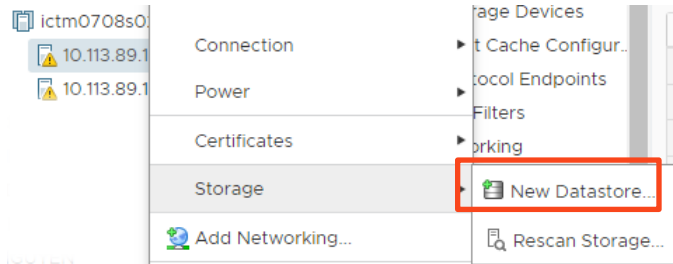
1. To rescan volumes, choose a server, select the Configure tab, and then click the iSCSI vmhba.
2. Click Rescan Storage. Perform this step for each hypervisor in the cluster.

vmhba68:C3:T0:L1	Iqn.1992-08.com.netapp:2804.600a098000a4b01700000...	1	Active (I/O)
vmhba68:C3:T0:L2	Iqn.1992-08.com.netapp:2804.600a098000a4b01700000...	2	Active
vmhba68:C3:T0:L3	Iqn.1992-08.com.netapp:2804.600a098000a4b01700000...	3	Active (I/O)
vmhba68:C3:T0:L7	Iqn.1992-08.com.netapp:2804.600a098000a4b01700000...	7	Active
vmhba68:C2:T0:L1	Iqn.1992-08.com.netapp:2804.600a098000a4b01700000...	1	Active (I/O)
vmhba68:C2:T0:L2	Iqn.1992-08.com.netapp:2804.600a098000a4b01700000...	2	Active

3. New disks discovered that were assigned volumes from host mapping are displayed. Each disk should have at least two paths, labeled Active and Active (I/O).

Creating a datastore

1. To create a datastore, right-click ESXi node and select Storage > New Datastore.
2. Create a datastore for each new disk. For more information, see [Create a VMFS Datastore](#).



Note: Be sure to create datastores for VSS volumes and VM storage. If there is an issue matching SSD versus HDD volumes, use the LUN number, which you can view from the datastore creation as well as in SANtricity System Manager on the Volumes tile.

Datastore name: VSS_1

Name	LUN	Capacity	Hardware...	Drive T...
Local DELL Disk (naa.6b8...	0	558.38 GB	Not suppor...	HDD
NETAPP ISCSI Disk (naa.6...	2	64.00 TB	Supported	HDD
NETAPP ISCSI Disk (naa.6...	3	64.00 TB	Supported	HDD

3. Complete the datastore creation for all VSS volumes mapped from storage.

New Datastore

✓ 1 Type
 ✓ 2 Name and device selection
 ✓ 3 VMFS version
 ✓ 4 Partition configuration
 5 Ready to complete

Ready to complete
 Review your settings selections before finishing the wizard.

General

Name: VSS_2
 Type: VMFS
 Datastore size: 64.00 TB

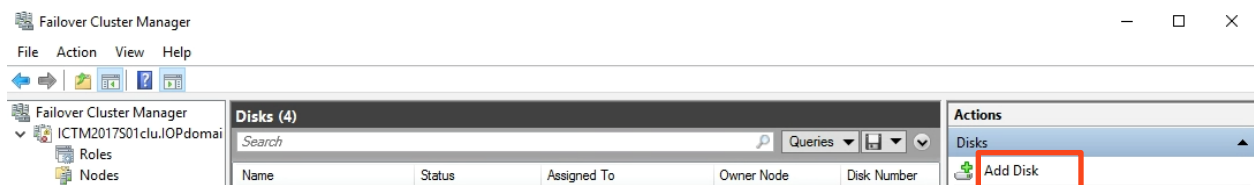
Windows

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.

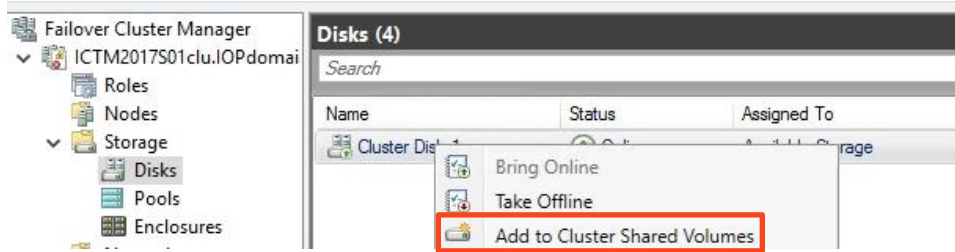
Adding cluster shared volumes

To add cluster shared volumes, complete the following steps:

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

To create a virtual hard disk, complete the following steps:

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.



Creating a VM

To create a VM, complete the following steps:

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 VMware document [Create a Virtual Machine with the New Virtual Machine Wizard](#).

New Virtual Machine

1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete

Customize hardware
Configure the virtual machine hardware

Virtual Hardware VM Options

ADD NEW DEVICE

> CPU *	4	
> Memory *	8	GB
> New Hard disk *	200	GB

3. See the Windows document [Create a Virtual Machine in Hyper-V](#).
4. Complete this operation for each server being deployed.

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

Name:	Recording VM 1
Generation:	Generation 2
Memory:	12288 MB
Network:	Virtual
Hard Disk:	C:\ClusterStorage\Recording\Recording_VM.vhdx (VHDX, dynamically expanding)
Operating System:	Will be installed from C:\Users\administrator.IOPDOMAIN\Downloads\en_window

Configuring milestone video management

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

[Milestone Systems Administrator Manual](#)

[Milestone Getting Started Guide](#)

1. Use the Milestone Systems Administrator Manual to 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 VMware, see [Clone a Virtual Machine to a Template in the vSphere Web Client](#).

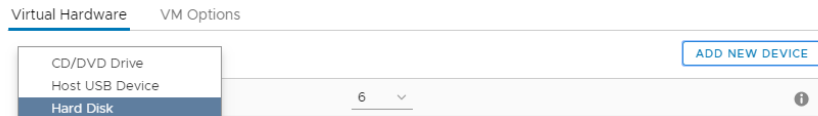
For Windows Hyper-V, see [Export and Import Virtual Machines](#). Use import type Copy the Virtual Machine.

Attaching storage to recording servers

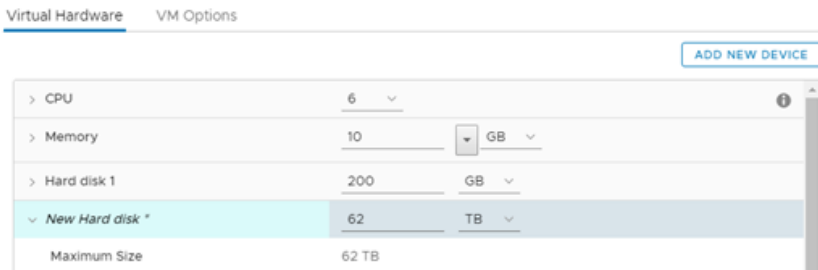
Before you begin, make sure that the VM is powered down. To attach all the hypervisor volumes to the archivers, follow these procedures.

VMware recording storage

1. In vSphere, right-click the recording server VM and select Edit Settings. At the top right, select Add New Device > Hard Disk.



2. Browse for a new location and then select the VSS volume. Increase the size of the hard disk to its maximum capacity. Add as many disks as required by the recording server.

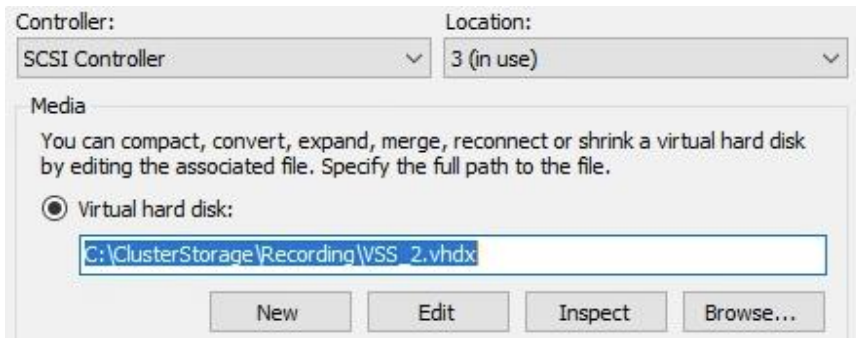


Windows recording storage

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.

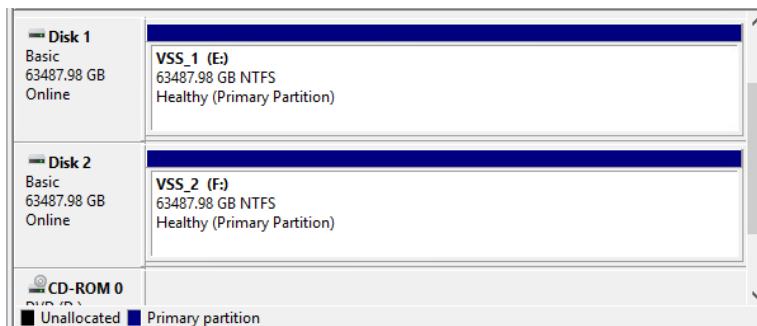


2. Browse for the VHDX drives in the cluster shared volume. Add as many disks as required by the recording server.



Formatting recording server drives

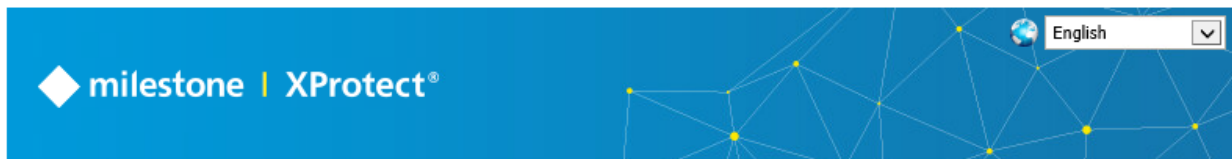
From the archiver server disk manager, right click the new disks, select Initialize, and create a volume. Map the volume to a drive letter for all the newly mapped disks.



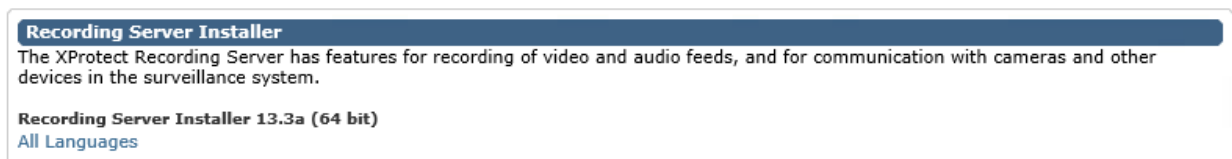
Installing a recording server

To install a recording server, complete the following steps:

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



Milestone XProtect VMS contains a set of administrative applications which are downloaded and installed from this page. User applications can be found on the default download page. If you want to view this page in another language, use the language menu in the top right corner.



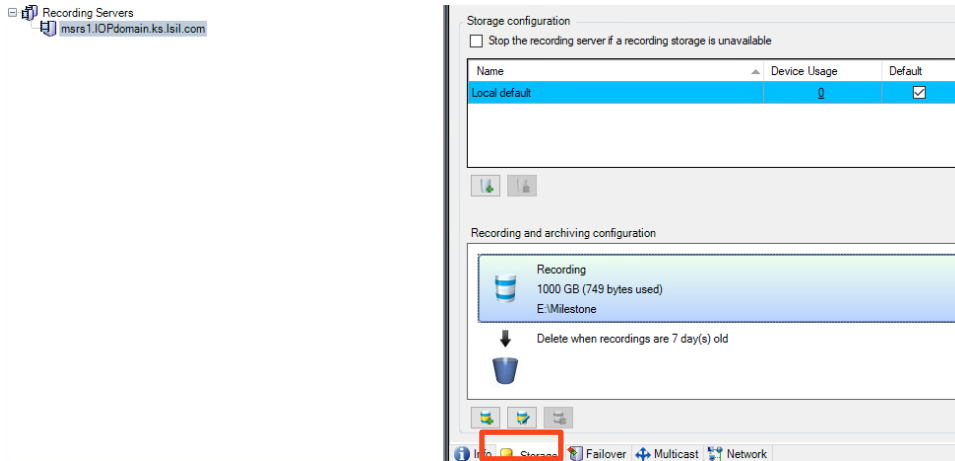
2. Download and install the recording server software. Use the same domain account as the installed management server. The recording server should be installed with up to four instances, using unique network adapters. When the installation is complete, a recording server task becomes available in the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

Name:

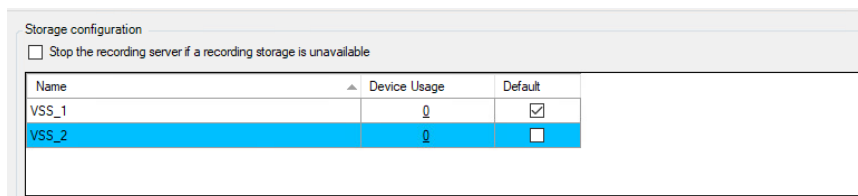
Recording

Path:

Retention time:

Maximum size:

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

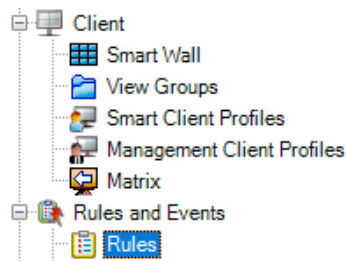


The recording storage is now set. Storage is selected to accommodate the expected retention period as cameras are added.

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.

Name:

Description:

Active: ☒

Step 5: Stop actions

Select stop action to perform

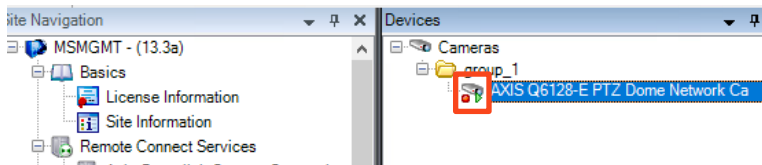
- ☒ Stop recording
- ☐ Stop feed
- ☐ Set <Smart Wall> to <preset>
- ☐ Set <Smart Wall> <monitor> to show <cameras>
- ☐ Set <Smart Wall> <monitor> to show text '<message>'
- ☐ Remove <cameras> from <Smart Wall> monitor <monitor>
- ☐ Restore default live frame rate
- ☐ Restore default recording frame rate
- ☐ Restore default recording frame rate of keyframes for MPEG-4/H.264/H.265
- ☐ Resume patrolling

Edit the rule description (click an underlined item)

Perform an action in a time interval
 always
 start recording immediately on All cameras

Perform an action when time interval ends
 stop recording immediately

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.

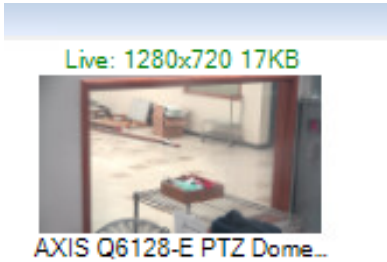
Some workflows allow multiple cameras. Use the one that fits your needs. The camera addition process allows cameras to be grouped as desired. This grouping can be used to describe which storage destination the camera is assigned to. Each camera can change its target if necessary. About 30 cameras should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

Default camera group:

Default microphone group:

Devices	Add to Group
Cameras	
AXIS Q6128-E PTZ Dome Network Camer...	Default Group

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



Configuring Genetec video management

For more information about the workflows used in the deployment, see the Genetec Main Server Installation documentation.

1. Attach and use the domain account for all Genetec installations.
2. Use the Genetec installation manual to install the Genetec Directory Server Role. The Windows Media Foundation feature and .NET Framework 4.5 are prerequisites for Genetec Security Center 5.9 Software.
3. When the directory server completes installation, open a browser on the network, go to `http://<directory_server>/genetec`, and use the Administration view to insert a valid license. Also open the Config Tool application on the directory server, which will be used to administer the VMS.

Scaling the archiving server

The archivers are the most likely servers to require scaling (that is, deployments of multiple archiving server virtual machines). First, clone the archiver (template or export) by using the Virtual Machine Manager

For VMware, see [Clone a Virtual Machine to a Template in the vSphere Web Client](#).

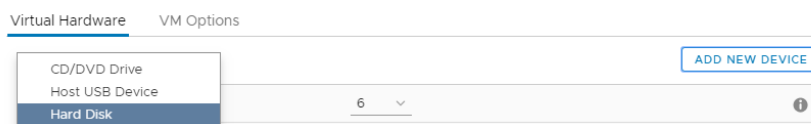
For Windows Hyper-V, see [Export and Import Virtual Machines](#). Use import type Copy the Virtual Machine.

Attaching storage to the archivers

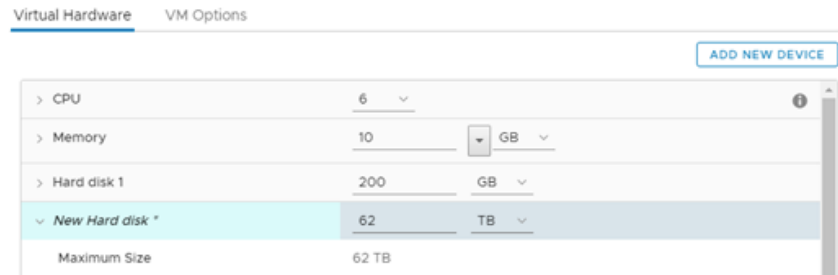
Before you begin, make sure that the VM is powered down. To attach all the hypervisor volumes to the archivers, follow these procedures.

VMware archiver storage

1. In vSphere, right-click the recording server VM and select Edit Settings. At the top right, select Add New Device > Hard Disk.



2. Browse for a new location and then select the VSS volume. Increase the size of the hard disk to its maximum capacity. Add as many disks as required by the archiver.

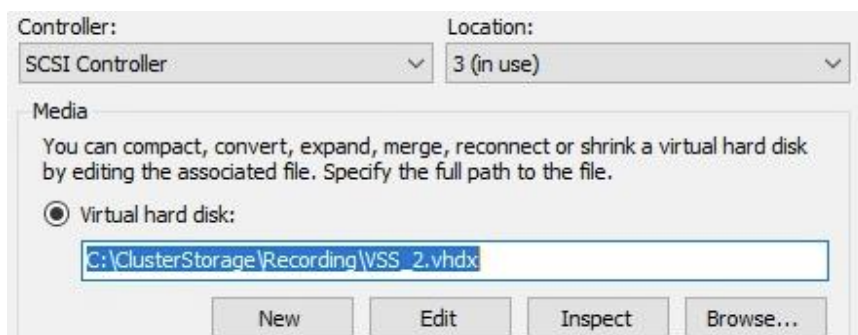


Windows archiver storage

1. In Failover Cluster Manager, right-click the archiver server VM and select Settings. Under Hardware, select SCSI Controller. Select Hard Drive and then click Add.

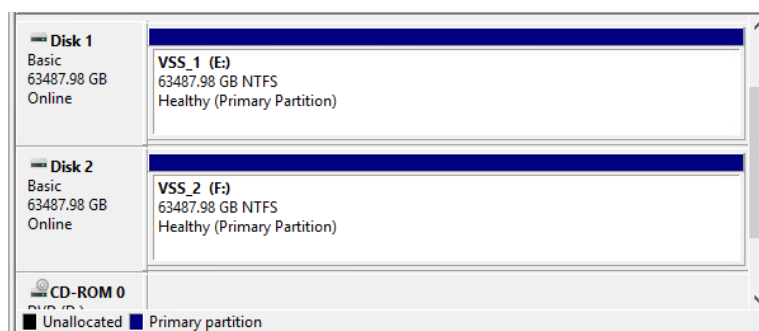


2. Browse for the VHDX drives in the cluster shared volume. Add as many disks as required by the archiver server.



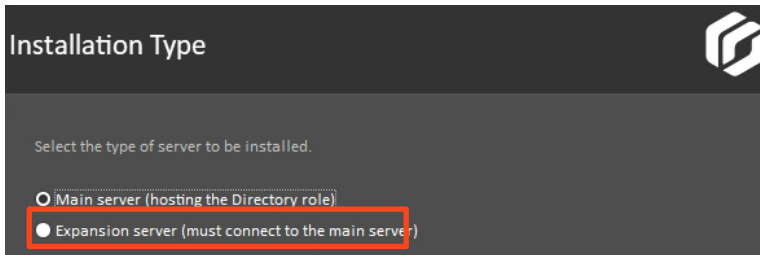
Formatting archiver server drives to here

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

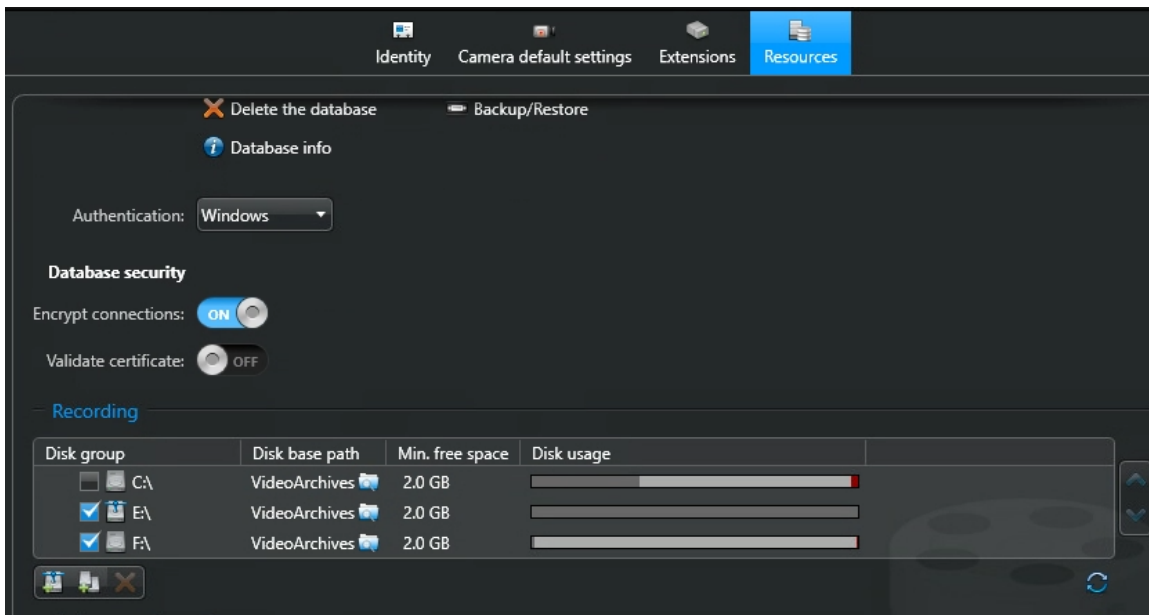


Installing an archiver server

1. Use the same installer package used to install the Directory server to install each archiver. Be sure to specify the server as an expansion server. Supply the connection information back to the primary directory server during installation.



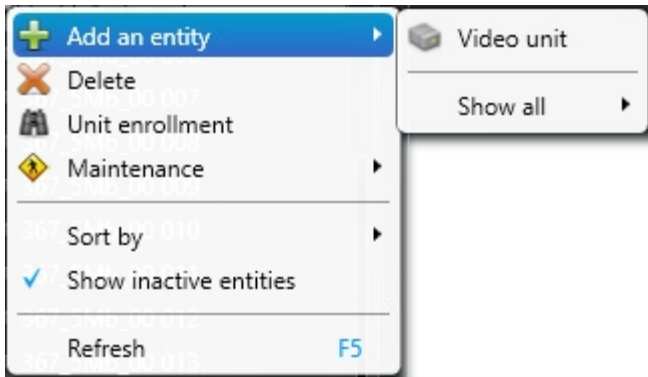
2. The archivers automatically show up in the System view of the Genetec Config Tool. Select each archiver and then select the Resources tab.



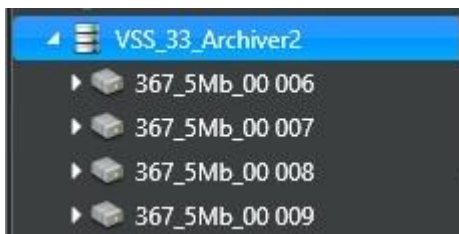
3. This tab allows you to change from the local drive to the drive letter created from the VSS storage pool. Select those drive letters as recording storage.

Connecting cameras

To connect cameras, go to the Genetec Config Tool Video view and right-click the archiver. Add a video unit to the archiver.



New cameras are attached as children to the archiver they were created on.



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.

Note: Milestone does not support ReFS.

Can I use VMware RDM instead of a datastore?

Answer: Yes. Although this document is geared toward the layout of traditional virtual deployments, there are two minor advantages to using an RDM:

- The RDM is slightly faster to bypass the datastore overhead (2% to 5% faster).
- The RDM provides the full capacity of the drive (64TB instead of 62TB) to the VM.

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.

Can I have a single network for VMware that covers both public management and vMotion?

Answer: Yes, but be sure to review your network requirements for vMotion to allow enough bandwidth across the network to service both connections.

Can I deploy a vSphere server as a VM?

Answer: Yes. However, if vSphere is running on the same ESXi nodes it is managing, consider the following:

- Licenses might be more difficult to apply. The vSphere VM itself could go down as part of the license expiration.
- The vSphere deployment is susceptible to any infrastructure outage, potentially making debugging more difficult.

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 disconnect 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>
```

VMware using the hypervisor prompt:

```
ping -I <src> <dst>
ping -I <src> -s 9000 <dst>
```

Conclusion

A virtualized video surveillance solution using NetApp E-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:

- E-Series and SANtricity Documentation Resources
<https://www.netapp.com/us/documentation/eseries-santricity.aspx>
- E-Series and SANtricity Documentation Center
<https://docs.netapp.com/ess-11/index.jsp>
- Genetec
<https://www.resources.genetec.com>
- Milestone
<https://www.milestonesys.com/support/>
- VMware
<https://docs.vmware.com/>
- NetApp Product Documentation
<https://docs.netapp.com>

Version history

Version	Date	Document version history
Version 1.0	February 2020	Initial release
Version 1.0.1	May 2020	Added Windows Hyper-V Examples
Version 1.0.2	November 2021	Minor updates

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright information

Copyright © 2021 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

TR-4818-1121