# Dell Storage with Milestone XProtect Corporate Configuration Guide

## Safety & Security

H14501.14

**Abstract**

This configuration guide provides the storage-specific configuration requirements and Milestone storage tiering options necessary for a successful Milestone XProtect Corporate installation.

**Dell Technologies Solutions**

Dell Technologies
Safety & Security Lab
Validated

milestone

February 2023

DELL Technologies

## Notes, cautions, and warnings

**NOTE:** A NOTE indicates important information that helps you make better use of your product.

**CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

**WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

# Contents

# 1

# Introduction

**Topics:**



## Solution overview

Milestone XProtect Corporate is a tiered solution that works well with Dell EMC Unity storage arrays as well as Dell EMC Isilon scale-out storage. The first tier of storage, Live DB, can accommodate stored video for the retention period prior to being moved to the second tier, of storage, Archive DB or deleted. The best practice retention time is between 2 and 24 hours. The second storage tier is Archive DB, which can accommodate long video retention cycles prior to being deleted from the second tier of storage.

Live DB requires block storage, such as Dell EMC Unity or **Dell** PowerEdge servers using iSCSI or Fibre Channel (FC), or storage local to the server. In a virtualized environment, the Unity arrays can serve a dual purpose by providing storage for the LiveDB and VMware datastores. The Archive DB used as the secondary storage for video data can be stored either on an Isilon scale-out storage cluster or on a unique Unity array.

While the Milestone XProtect Corporate tiered storage solution can be deployed within a site, depending on the requirements XProtect Corporate can also provide a solution for distributed to central site architectures.

## Purpose

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

Use this guide to determine the requirements for a successful Milestone XProtect Corporate 2020 installation, Milestone storage tiering options, and storage-specific configuration requirements.

## Scope

This guide is intended for internal Dell Technologies personnel and qualified Dell Technologies and Milestone partners. It provides configuration instructions for installing the Milestone XProtect Corporate video management software using Dell storage platforms.

The following Dell storage systems have been tested:

- Dell EMC Isilon
- Dell EMC Unity
- Dell EMC SC series
- Dell EMC ECS Object Storage

This guide supplements the standard Dell EMC Isilon Storage with Video Management Systems Best Practices: Configuration Guide and provides configuration information specific to Milestone XProtect Corporate.

**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 Technologies personnel and qualified Dell Technologies partners are using this guide with an established architecture.

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

- Associated with product implementation
- Milestone-certified to install Milestone XProtect Corporate services
- Proficient in installing and configuring Unity storage solutions
- Proficient in installing and configuring SC Series storage solutions
- Proficient in installing and configuring Isilon storage solutions
- Able to access the *Dell EMC Block Storage with Video Management Systems Best Practices: Configuration Guide*
- Able to access the *Dell EMC Isilon Storage with Video Management Systems Best Practices: Configuration Guide*

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

# 2

# Configuring the Dell solution

**Topics:**



## Dell storage considerations for Milestone XProtect Corporate

To successfully design and implement a Milestone XProtect Corporate system, you need to consider many aspects of the system, including networks, cameras, storage, and more. This section presents storage considerations and recommendations you should take into account when deploying a Milestone XProtect Corporate system on Dell storage platforms.

### Video Flow

There are many Dell storage platform options for each storage tier. The Live DB can be direct-attached storage (DAS), such as FC or iSCSI block storage. The Archive DB can be DAS if the storage requirement is minimal, and network-attached storage (NAS), FC, or iSCSI for virtualized server implementations and more substantial video storage requirements.

The following figure illustrates the video flow using NAS, DAS, and storage-area network (SAN).

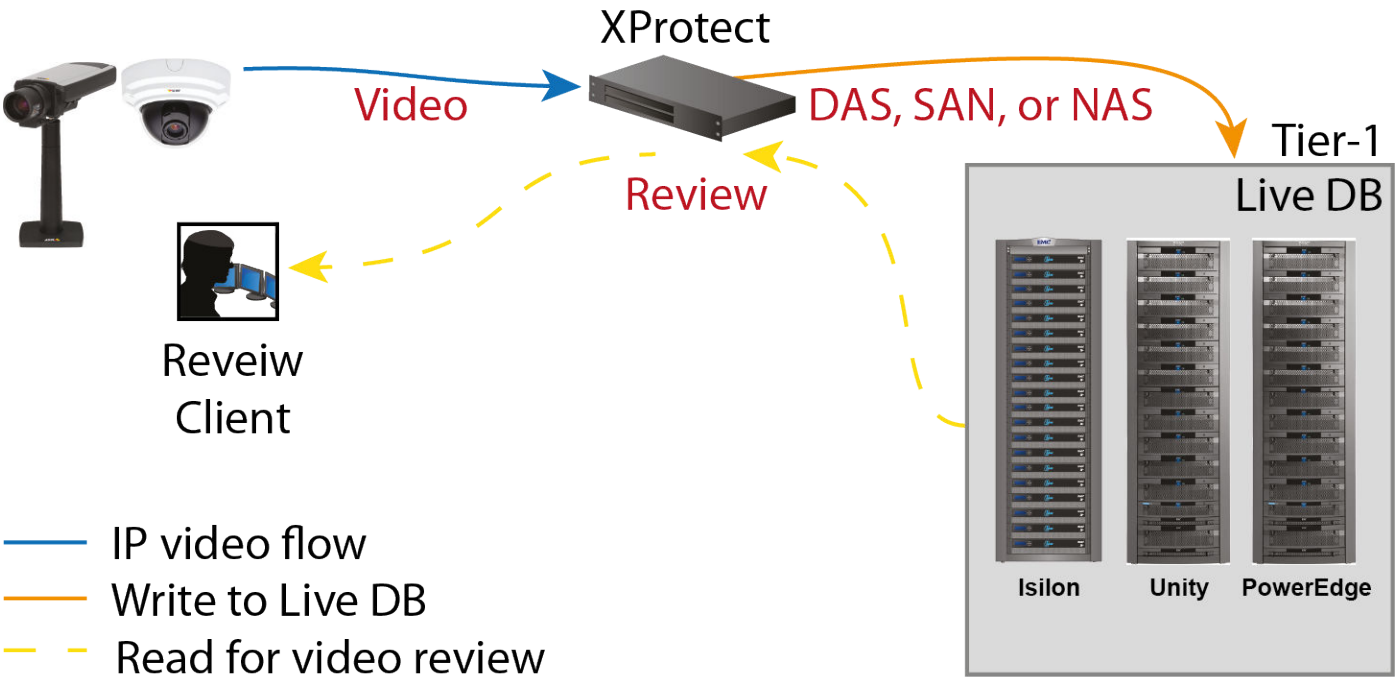


**Figure 1. Milestone XProtect Corporate architecture**

Video is initiated at the camera and XProtect initially places that video in the Live DB. Milestone recommends a retention period of from 2 to 24 hours for video in the Live DB, as outlined in Retention periods.

XProtect moves video files at rest from the Live DB storage tier to the Archive DB storage tier at regular intervals. The Archive DB stores each video file until that file's full retention time has expired.

## Live DB

XProtect's Live DB write algorithm is optimized for block storage. Therefore, the Live DB works best with the server's internal DAS, or with external FC or iSCSI storage such as Unity or SC series arrays. Milestone enables video to be kept in the Live DB storage indefinitely.

Internal DAS storage is ideal for small implementations with a few servers. As an installation grows, the need to optimize storage for reliability, scalability, manageability, and rack space increases. In larger environments, and in virtualized server environments, Unity or SC series arrays in a SAN (FC or iSCSI) configuration are more practical for the Live DB.

## Archive DB

The Archive DB is a long-term storage option for XProtect and typically constitutes the majority of the storage capacity requirement. Moving video from the Live DB to the Archive DB involves many activities, including optimizing index files for the larger video repository, and moving the files.

## Storage considerations for Live DB and Archive DB

The Live DB can be a storage array in a SAN configuration. The Archive DB can be a Unity or SC series storage array in a SAN configuration, or an Isilon scale-out cluster in a NAS configuration.

- With the Unity or SC series, both the Live DB and Archive DB can use either FC or iSCSI protocols. For iSCSI, you can use GigE or 10 GbE NICs.
- When using smaller Unity or SC series arrays with iSCSI, we recommend that the Live DB and Archive DB reside on different volumes.
- When using FC, Live DB and an FC Archive DB can co-exist on the sameUnity array.
- Arrays such as the Unity 600 can be used with iSCSI for both the Live DB and Archive DB.
- Unity or SC series storage can be used for:
  - LiveDB only
  - LiveDB as the first tier in a tiered implementation
  - Archive DB as the second tier in a tiered implementation
- For Isilon scale-out storage, NAS can be used with Isilon OneFS 7.0 or higher. Use the default Isilon protection scheme unless the customer needs additional protection.
- You can use GigE or 10 GbE network interface cards (NICs). Test results for this solution are based on both GigE and 10 GbE interfaces on the Isilon cluster. By default, XProtect moves video from the Live DB to the Archive DB using a single thread. With NAS, you can increase the Archive DB thread count to allow parallel video file moves within the archive process.
- When using Isilon storage, we recommend using it as the Archive DB storage tier.
- Although it is possible to use the NFS datastores for the Milestone boot drive in a VMware environment, this configuration with Milestone XProtect has not been tested in the Dell Technologies Safety & Security Lab.

### Retention periods

Milestone recommends a minimum retention period of two hours for the Live DB, although one hour is the minimum supported. There is no limitation on the maximum retention time for Live DB.

The Archive DB retention period depends on business requirements and can range from a few weeks to many months.

## Summary of Dell storage and network protocols

Live DB and Archive DB are two distinct repositories with different write characteristics.

They were evaluated on individual storage platforms and on a single platform in the following configurations:

- For the Live DB we tested various Unity and SC series arrays with both FC and iSCSI storage protocols.
- For the Archive DB we tested an Isilon scale-out cluster, Unity arrays, and SC series arrays with iSCSI.

The following table lists the Dell storage platforms and network protocols determined to be suitable for each XProtect video database storage tier.

### Table 1. Storage and protocols for XProtect database tiers

| Array/cluster | Database | Protocol | Verified |
|---|---|---|---|
| DAS | Live DB | DAS | Yes (by Milestone) |
| Unity series | Live DB | FC | Yes (functional test) |
| Unity series | Live DB | iSCSI | Yes |
| SC series | Live DB | iSCSI | Yes (functional) |
| DAS | Archive DB | DAS | Yes (by Milestone) |
| Isilon clusters [a] | Archive DB | SMB2, SMB3 | Yes |
| Unity series | Archive DB | iSCSI | Yes |
| SC series | Archive DB | iSCSI | Yes |
| ECS | Archive DB | S3 | Yes |

a. Isilon OneFS releases prior to OneFS 7.0 are not recommended.

# Releases tested

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

### Table 2. SAN firmware builds

| Model | Firmware | Tier | XProtect release |
|---|---|---|---|
| Unity 300 | 4.2.1.9535982, 4.3.1.1525703027 | 1, 2 | 2018 |
| Unity 500 | 4.2.1.9535982, 4.3.1.1525703027 | 1, 2 | 2018 |
| SC3000 | 7.2.30.21 | 2 | 2018 |
| ME4012 | GT275R005-04 | 2 | 2019 |
| PowerStore 5000T | 1.0.4.0.5.003 | 1, 2 | 2020 |
| PowerStore 5000X | 1.0.4.0.5.003 | 2 | 2020 |

### Table 3. OneFS releases

| Model | OneFS version | Tier | XProtect release |
|---|---|---|---|
| PowerScale A3000 | 9.2.1 | 2 | 2022 |
| Isilon A2000 | 9.1 | 2 | 2020 |

### Table 4. ECS Object Storage tested

| Cluster | ECS | GeoDrive | vSAN host | XProtect release |
|---|---|---|---|---|
| ECS U400 | 3.2 | 1.2.2.1 | E560 | 2018 |

### Table 5. PowerEdge servers tested

| Server | Storage Controller | XProtect release |
|---|---|---|
| XE7100 | H730P | 2020 |
| R740xd2 | H730P | 2018, 2019 |
| R740xd | H730P | 2018 |
| R540 | H740P | 2018 |

**Table 5. PowerEdge servers tested (continued)**

| Server | Storage Controller | XProtect release |
|---|---|---|
| R440/R640 | H740P | 2018 |

# 3

# Object Storage considerations

**Topics:**



## Dell EMC ECS

Dell EMC ECS is a complete software-defined cloud storage platform that supports the storage, manipulation, and analysis of video security and unstructured data on a massive scale on commodity hardware. ECS is specifically designed to support the mobile, cloud, and Big Data workloads that are similar to large-scale safety and security workloads.

## Retention periods and policies

ECS provides the ability to prevent data from being modified or deleted within a specified retention period. Bucket based retention is not supported and is not to be used with Milestone XProtect Corporate when using the GeoDrive service. XProtect managed time based retention is the only supported retention policy when using GeoDrive.

## Cluster Capacity

Dell Technologies only supports the use of time based retention settings with Milestone XProtect Corporate. To determine the capacity requirement for each recorder, calculate the number of cameras per recorder, the target bit rate per camera, and the retention time in days. Always consult with Milestone to determine an accurate capacity estimate.

All writes to the ECS cluster stop when the cluster capacity reaches 90% full. It is always recommended to plan for additional capacity as soon as you reach 75% of the cluster capacity.

## Quotas

When using GeoDrive, Dell EMC storage requires the use of ECS soft quotas. Quotas are the storage space limit that is specified for the ECS buckets. You can specify a storage limit for the bucket and define notification and access behavior when the quota is reached. The quota setting for a bucket cannot be less than 1 GB and can be specified in increments of 1 GB.

The Dell Technologies Safety & Security Lab recommends only using soft quotas for safety and security solutions. Dell Technologies recommends maintaining 15% overhead beyond the capacity requirement.

The quota behavior options are as follows:

**Table 6. Quota behavior options**

| Quota | Behavior |
|---|---|
| Notification Only at *<quota_limit_in_GB>* (recommended) | Soft quota setting at which you are notified. |

**Table 6. Quota behavior options (continued)**

| Quota | Behavior |
|---|---|
| Block Access Only at *<quota_limit_in_GB>* (not recommended) | Hard quota setting which, when reached, prevents write/update access to the bucket. |
| Block Access at *<quota_limit_in_GB>* and Send Notification at *<quota_limit_in_GB>* (not recommended) | Hard quota setting which, when reached, prevents write/update access to the bucket and the percentage of the quota setting at which you are notified. |

# Garbage collection and space reclamation

Garbage collection (GC) in ECS is designed such that it runs with lower priority than I/O activity. When an object is deleted, ECS waits for garbage collection to reclaim the space allocated to that object. However, the object is marked as deleted and the deletion is reflected in the user's view of system utilization through metering and chargeback reports.

Data and system metadata are written in chunks on ECS. An ECS chunk is a 128MB logical container of contiguous space. Each chunk can have data from different objects. ECS uses indexing to track all the parts of an object that may be spread across different chunks and nodes. Chunks are written in an append-only pattern. The append-only behavior means that an application's request to modify or update an existing object will not modify or delete the previously written data within a chunk. But rather, the new modifications or updates will be written in a new chunk.

Writing chunks in an append-only manner means that data is added or updated by first keeping the original written data in place and second by creating net new chunk segments, which may or may not be included in the chunk container of the original object. The benefit of append-only data modification is an active/active data access model, which is not hindered by file-locking issues of traditional file systems. This being the case, as objects are updated or deleted, the data in chunks that is no longer referenced or needed is referred to as Garbage.

For optimum performance, file size must not exceed 128 MB to provide more consistent data transfers and even out the workload to the ECS. Larger files add additional CPU load which reduces performance.

ECS uses two garbage collection methods to reclaim space from discarded full chunks, or chunks containing a mixture of deleted and nondeleted object fragments that are no longer referenced. These methods are:

| | |
|---|---|
| **Normal GC** | When an entire chunk is garbage, reclaim the space. |
| **Partial GC by Merge** | When a chunk is 0.66 garbage, reclaim the chunk by merging the valid parts with other partially filled chunks in a new chunk, then reclaim the space. |

**NOTE:** While designing a solution, take care such that the total ingest rate to the ECS cluster does not exceed the Garbage collection rate for the cluster.

By default, the garbage collection process is purposely configured to run slowly in a conservative effort to protect against data loss. Our testing shows that this process can be safely tuned to reclaim space more quickly, while remaining a safe operation. Our suggested garbage collection parameters are:

- Decrease the time interval for the frequency of verification scanner
- Increase the scanner throttle for number of objects
- Increase the scan tasks expiration times
- Increase the maximum number of pending partial GC tasks

Contact Dell EMC ECS technical support for more information about tuning these parameters.

**NOTE:** Bucket level retention on ECS should not be used. Milestone handles the retention policy so bucket level retention is not recommended.

# Dell EMC GeoDrive

The Dell EMC GeoDrive tool provides a local file system interface through which you can store and retrieve files on Dell EMC ECS Object Storage. Use GeoDrive to store and retrieve files, such as pictures, movies and documents, in the cloud using the same applications and tools that you use today.

Refer to the Dell EMC ECS: GeoDrive Best Practices for additional information about installation and configuration of GeoDrive on the recorder.

## Configure GeoDrive parameters for the ECS bucket

Set the USN journal files to active.

**Steps**

1. Open GeoDrive.
2. Click **Modify GeoDrive**.
3. Click on the **Settings** tab.
4. Select **Write all files and folders to the cloud in lower case**.

## Configuring Milestone for use with RSA

You must configure Milestone for use with SecurID.

**Steps**

1. Open GeoDrive.
2. Click **Modify GeoDrive**.
3. Click **Advanced**.
4. Select **Minimum time to wait for a file to close before uploading to the Cloud.**.

# ECS tuning for safety and security implementations

Various parameters on the ECS EX3000 were tuned to optimize the bandwidth performance with safety and security video traffic. ECS performance tuning in the Dell Technologies Safety & Security Lab is based on the Milestone Recorders using a video file (object) size of 500 MB.

The following table shows the updated parameters and settings:

**Table 7. ECS tuning parameters**

| Parameter | Default value | Tuned value |
|---|---|---|
| com.emc.ecs.chunk.gc.repo.partial.task.generator.max_pending_task_num | 50 | 200 |
| com.emc.ecs.chunk.gc.repo.verification.new_run_interval | 6 hours | 30 minutes |
| com.emc.ecs.chunk.gc.repo.verification.sleep_obj_interval | 200 | 400 |
| com.emc.ecs.chunk.gc.scanner.task.cache_expire | 2 hours | 1 hour |
| com.emc.ecs.chunk.gc.scanner.task.cache_expire | 2 hours | 1 hour |
| com.emc.ecs.chunk.gc.repo.verification.sleep_obj_interval | 200 | 400 |
| com.emc.ecs.chunk.gc.btree.scanner.throttling | 50 | 80 |
| com.emc.ecs.chunk.gc.btree.reclaimer.throttling | 50 | 80 |
| com.emc.ecs.chunk.gc.btree.reclaimer.new_round_interval | 90 minutes | 2 hours |
| com.emc.ecs.chunk.gc.deletejobscanner.timeout | 30 minutes | 60 minutes |
| com.emc.ecs.chunk.gc.deletejobscanner.job_pause_interval | 20 milliseconds | 10 milliseconds |
| com.emc.ecs.chunk.gc.repo.partial.task.generator.throttling.chunk_task_ratio | 10 | 3 |
| com.emc.ecs.chunk.gc.repo.partial.task.generator.throttling.pending_task_num_lower_limit | 50 | 1000 |

# 4

# SAN considerations

**Topics:**



## Dell EMC Unity and Dell EMC SC series

Dell EMC Unity and Dell EMC SC series storage arrays are ideal for recording and managing terabytes of video from distributed locations. This section describes best practices for configuring a Unity or SC series storage system for this solution.

The Unity and SC series series arrays are designed for mid-tier to enterprise storage environments, are ideal for distributed environments, and can scale to handle large petabyte (PB) environments with block-only requirements at central locations.

For more information about configuring Unity and SC series storage arrays, see Dell EMC SAN Storage with Video Management Systems Configuration Best Practices.

## Dell PowerVault ME4

The Dell PowerVault ME4 Series SAN/DAS Storage Series is optimized to run a variety of mixed workload applications -physical and virtual - for small businesses.

Based on the family of Intel processors, Dell PowerVault ME4 Series storage implements a block architecture with VMware virtualization integration and concurrent support for native iSCSI, Fibre Channel, and SAS protocols. Each system leverages dual storage processors (single storage processor systems are available) and a full 12Gb SAS back-end. Additional storage capacity is added via Disk Array Enclosures (DAEs) while Distributed RAID (ADAPT) delivers faster drive re-build times. And all ME4 Series arrays are managed by an integrated HTML5 web-based GUI.

Frame loss was observed during testing on the ME4 platform as tier 1 storage.

Dell Technologies recommends using ME4 platforms for:

- Small implementations
- Archive storage as a second tier
- Installations that include noncritical cameras where some video frame loss is acceptable during storage recovery activities, such as disk rebuilds and controller outages that are required for maintenance upgrades or failures

Behavior can vary per video management software product and implementation decisions, such as selected infrastructure hardware, camera setup, and so forth.

**NOTE:** For mission critical safety and security video applications, Dell Technologies recommends Unity, Isilon, or ECS with GeoDrive.

## Multipathing and NIC failures

Configure the Unity and SC block storage arrays with multiple paths to recorders using Microsoft MPIO. For redundancy, configure multiple NICs with the recorders and controllers. Recorders that are configured with multipathing reconnect to the volume across another available path after a NIC failure.

The TCP Max transmissions value determines how many times the Transmission Control Protocol (TCP) retransmits an unacknowledged data segment on an existing connection. The TCP retransmits data segments until they are acknowledged or until this value expires.

TCP/IP adjusts the frequency of retransmissions over time. The TCP establishes an initial retransmission interval by measuring the round trip time on the connection. This interval doubles with each successive retransmission on a connection, and it is reset to the initial value when responses resume.

To reduce the reconnection time and eliminate video loss, adjust the following TCP retransmission timers:

**NOTE:** It is recommended that you perform a backup before editing registry settings.

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
Value Name:  TcpMaxDataRetransmissions
Data Type:   REG_DWORD - Number
Valid Range: 0 - 0xFFFFFFFF
Value:     3
```

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
Value Name:  TCPInitialRtt
Data Type:   REG_DWORD - Number
Valid Range: 0 - 0xFFFFFFFF
Value:     2
```

To reduce path failover times for volumes that are mapped through ESXi hosts using raw device mapping (RDM) LUN's or Datastores, use the following timeouts. Modify these settings on the iSCSI software adapter for each SAN attached host. These settings are located on the **Advanced** tab in the properties section of the individual ESXi servers Software iSCSI adapter.

```
iSCSI Login Timeout 5
NoopInterval 2
NoopTimeout 10
Recovery Timeout 4
Delayed ACK Disabled
```

# iSCSI Initiator Queue Depth On ESXi hosts

Define the iSCSI initiator queue depth for each SAN attached ESXi host.

Run the following command:

```
esxcli system module parameters set -m iscsi_vmk -p iscsivmk_LunQDepth=255
```

5

# Isilon considerations with SMB

**Topics:**



## Design concepts and disclaimers

There are many design options for a Milestone XProtect Corporate implementation including Federations, Auxiliary Servers, and multicast considerations.

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

The following diagram illustrates the Dell Technologies and VMware components that were tested.

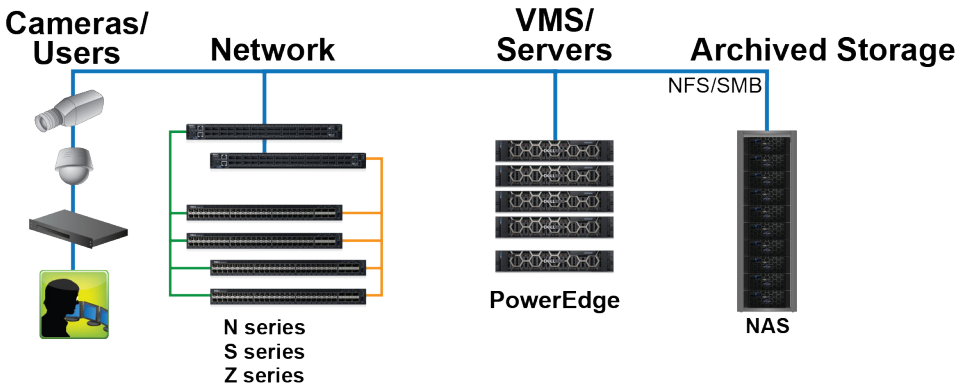


**Figure 2.**

The Dell Technologies Safety & Security Lab vSAN test environment uses various servers and storage options throughout the lab, as shown in the following figure. When conducting a test, the nodes are contained in a single cabinet. Traffic can originate from application servers within the cabinet or servers external to the cabinet or both.

# 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

To maximize caching performance for safety and security workloads, the Dell Technologies Safety & Security Lab recommends using two SSD system drives per node in clusters where it is supported, such as the NL-series.

# OneFS 8.1 job workers (required)

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

To modify the job workers to 0 per core, run the following command from the command line interface:

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

**NOTE:** With OneFS 8.2.2, this setting will be the default and this modification will not be necessary.

# Endurant cache

Endurant Cache (EC) is a caching mechanism that is enabled by default in OneFS. EC consolidates multiple small, random, synchronous writes to create fewer, more efficient writes to disk. For many workloads, the use of EC can help smooth out latency and increase performance.

EC is not needed with traditional safety and security video workloads and performance can actually improve when EC is disabled. Video workloads for safety and security use one, two or three video recorders to write to a node, including Tier 1 video ingest or Tier 2 video archiving. While these workloads are synchronous, they are also large and sequential, which can cause a bottleneck when using EC.

To disable EC, run the following command from the command line interface:

```
isi_sysctl_cluster "efs.bam.ec.mode=0"
```

# Impact policy and priority configuration

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

| | |
|---|---|
| **Releases with OneFS 7.0 or greater** | Dell Technologies recommends using OneFS 7.0 or later to maximize bandwidth and minimize video review response times. You can use the default impact policy with Isilon X400, Isilon X410, Isilon NL410, and greater. For less powerful nodes, such as the Isilon X200 and earlier running OneFS 7.0 or greater, modify all jobs to use an impact policy of **Low**. |
| **Releases prior to OneFS 7.0** | For releases prior to OneFS 7.0, the best I/O performance is obtained by configuring all background jobs with the impact policy set to **Low**. To set the impact policy select **Operations** > **Jobs and Impact Policies**. |

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

# Volume limits

Implementations greater than 8 TB are common when video is stored on high-end storage, such as Isilon scale-out NAS storage and Unity block 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 XProtect Recorder, the Dell Technologies best practice is to use SmartQuotas to segment the single Isilon file system so that each Recorder has a logical subset view of storage.

While there are three directory-level quota systems, the Dell Technologies Safety & Security Lab only uses the hard limit system during validation testing:

| | |
|---|---|
| **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.<br>Use the **Hard limit** quota system to set the video storage as a defined value.<br>If necessary, both Isilon and the XProtect Recorder can add or subtract storage, even if a hard limit quota is set. |
| **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. |

# Unique share naming

When working with a single file system, each Recorder 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 Recorder.

# Configuring SmartConnect

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

### About this task

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 XProtect Recorders 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. Static pools must be used for SMB connections. We recommend using Dynamic IP addresses for NFS. There is a connection policy per pool used by both Static IP (SMB) and Dynamic IP (NFS), while the rebalance policy is only used with Dynamic IP.

| | |
|---|---|
| **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 XProtect Recorder servers to specified nodes in the Isilon cluster. Use a unique IP address pool for video recording and Recorder read/write access. |
| **Network throughput** | Based on NIC utilization. Use of throughput requires that each Recorder 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 Recorder IP address pool. Define additional pools for management (such as Isilon InsightIQ or administrative access), evidence repository, post process, or other use.

### Steps

1. Click **Cluster Management** > **Network 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.

# Configuring SmartQuotas (recommended)

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

### About this task

To better cache the meta data associated with SmartQuotas, the Dell Technologies Safety & Security Lab recommends using two SSD drives per node where possible. The second SSD drive provides no performance gain with A-series clusters.

Without SmartQuotas, the XProtect Corporate administrator must anticipate the total write rate to the cluster and adjust the **Min Free Space** on each Recorder 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 Recorder 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 Recorder 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.

### Steps

1. From the OneFS GUI, select **File System** > **SmartQuotas** > **Quotas & Usage**.
2. On the **Storage Quotas & Usage** page, click **Create a storage quota**.
3. In the **Directory path** field, click **Browse**, and then select the share directory.

4. Define the SmartQuotas limit and set the threshold:
   a. Select **Specify storage limits**.
   b. Select **Set a hard storage limit**.
   c. Type the hard limit value.
   d. Select the size qualifier, typically **TB**.
   e. Select **Size of hard threshold** for **Show Available Space as:**.
5. Click **Save**.
6. Repeat the process for the remaining shares.

# SMB specific configuration

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

### About this task

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

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

### Steps

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

```
touch /etc/mcp/override/sysctl.conf && cp /etc/mcp/override/sysctl.conf /etc/mcp/
override/sysctl.conf.bku1
```

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

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

   The following output is displayed:

```
Value set successfully
```

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

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

   Output similar to the following is displayed:

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

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

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

```
cp /etc/mcp/override/sysctl.conf.bku1 /etc/mcp/override/sysctl.conf
```

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

# Frame loss reduction

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

### About this task

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

### Steps

1. Set the paramters in the `syctl` configuration file using the following commands:

```
declare -i COUNT MDS
BASE=10000
COUNT=$((1.01 * $BASE))
MDS=$(($BASE * 0.75))
isi_sysctl_cluster kern.maxvnodes=$BASE
isi_sysctl_cluster kern.minvnodes=$BASE
isi_sysctl_cluster efs.lin.lock.initiator.lazy_queue_goal=$COUNT
isi_sysctl_cluster efs.ref.initiator.lazy_queue_goal=$COUNT
isi_sysctl_cluster efs.mds.block_lock.initiator.lazy_queue_goal=$MDS
isi_sysctl_cluster efs.bam.datalock.initiator.lazy_queue_goal=$MDS
```

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

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

# Link aggregation

The active/passive configuration involves aggregating the NIC ports on the Isilon nodes for high availability. If one of the ports on the node or switch port fails, the XProtect Recorder can continue writing to the Isilon share using the other port connection without affecting the recording. The SMB share continues to be accessible to the server using the passive connection port.

NIC aggregation can be used to reduce the possibility of video loss from a cable pull, NIC failure, or switch port issue. Dell Technologies recommends NIC aggregation, also known as link aggregation, in an active/passive failover configuration. This method transmits all data through the master port, which is the first port in the aggregated link. If the master port is unavailable, the next active port in an aggregated link takes over.

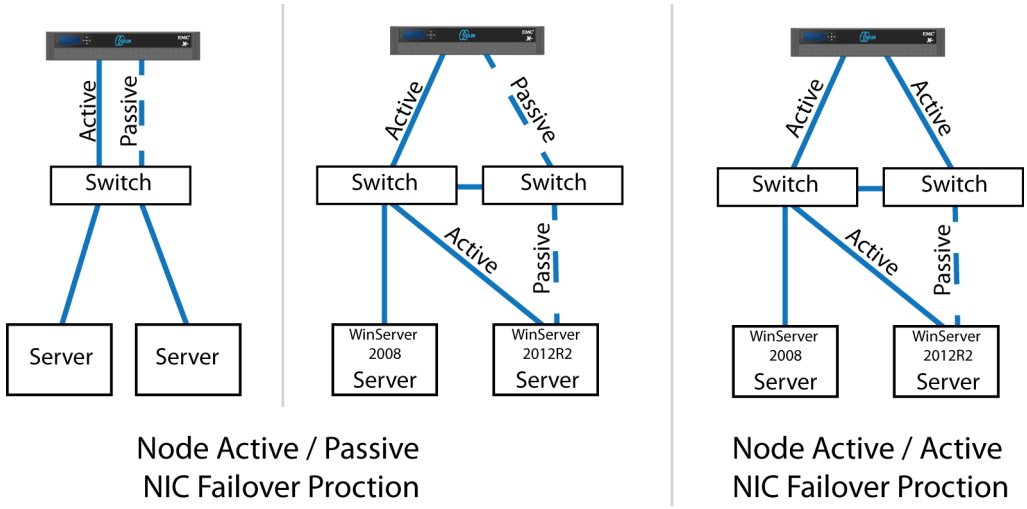


**Figure 3. Isilon Active/Passive and Active/Active configuration**

# 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 XProtect.

**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.

### About this task

The following three tests were conducted:

| | |
|---|---|
| **Full Active Directory (recommended)** | Where the XProtect Corporate server and the Isilon cluster are part of the same Windows domain. |
| **Partial Active Directory** | Where the XProtect Corporate servers are part of the Windows domain, but the Isilon cluster is administered locally. |
| **Fully locally administered control** | Where the XProtect Corporate servers and the Isilon cluster are administered locally. |

Alternatives to the previous methods might exist, but the Dell Technologies Safety & Security Lab team does not plan to derive or support other methods.

### Steps

1. Click **Access** > **Authentication Providers**.
2. 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 XProtect 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 XProtect 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 XProtect 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.

# Data protection

OneFS does not rely on hardware-based RAID for data protection. The Isilon system uses the Reed-Solomon algorithm for N+M protection with Forward Error Correction (FEC).

Protection is applied at the file level, enabling the cluster to recover data quickly and efficiently. Nodes, directories, and other metadata are protected at the same or a higher level as the data blocks they reference. Since all data, metadata, and FEC blocks are spread across multiple nodes, dedicated parity drives are not required. For more information about Isilon data protection, see *Dell PowerScale OneFS: A Technical Overview*.

Although cluster sizes as small as three nodes are possible, for safety and security applications we recommend a minimum of nodes. Sizing calculations need to include a minimum free space calculation for proper cluster sizing. We recommend a cluster size that enables a node to be removed while retaining a minimum of 10 percent free space in the remaining capacity. This cluster size ensures that node removal and node failures have minimal or no impact on video ingestion.

The Isilon sizing tool provides an accurate calculation. You can find this tool at https://isilon-sizing-tool.herokuapp.com. Other sizing tools from video management software (VMS) and camera vendors may also be used for sizing the necessary bandwidth and storage capacity.

## Isilon protection with OneFS

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

6

# Converged considerations with VxRail

**Topics:**



## Design concepts and disclaimers

There are many design options for a Milestone XProtect Corporate implementation including Federations, Auxiliary Servers, and multicast considerations.

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

The following diagram illustrates the Dell Technologies and VMware components that were tested.

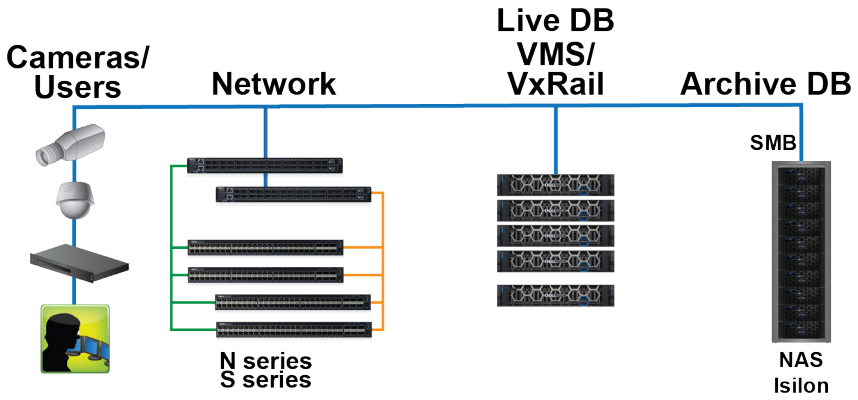


**Figure 4. Dell Technologies Solution | Safety & Security with Milestone XProtect Corporate architecture**

The Dell Safety & Security Lab VxRail test environment uses P570 VxRail nodes with Dell S4148F-ON switches and Isilon storage arrays throughout the lab, as shown in the following figure. When conducting a test, the VxRail nodes are contained in a single cabinet. Traffic can originate from application servers within the cabinet or servers external to the cabinet or both. Any additional storage is external to the VxRail cabinet, including the Isilon storage nodes.

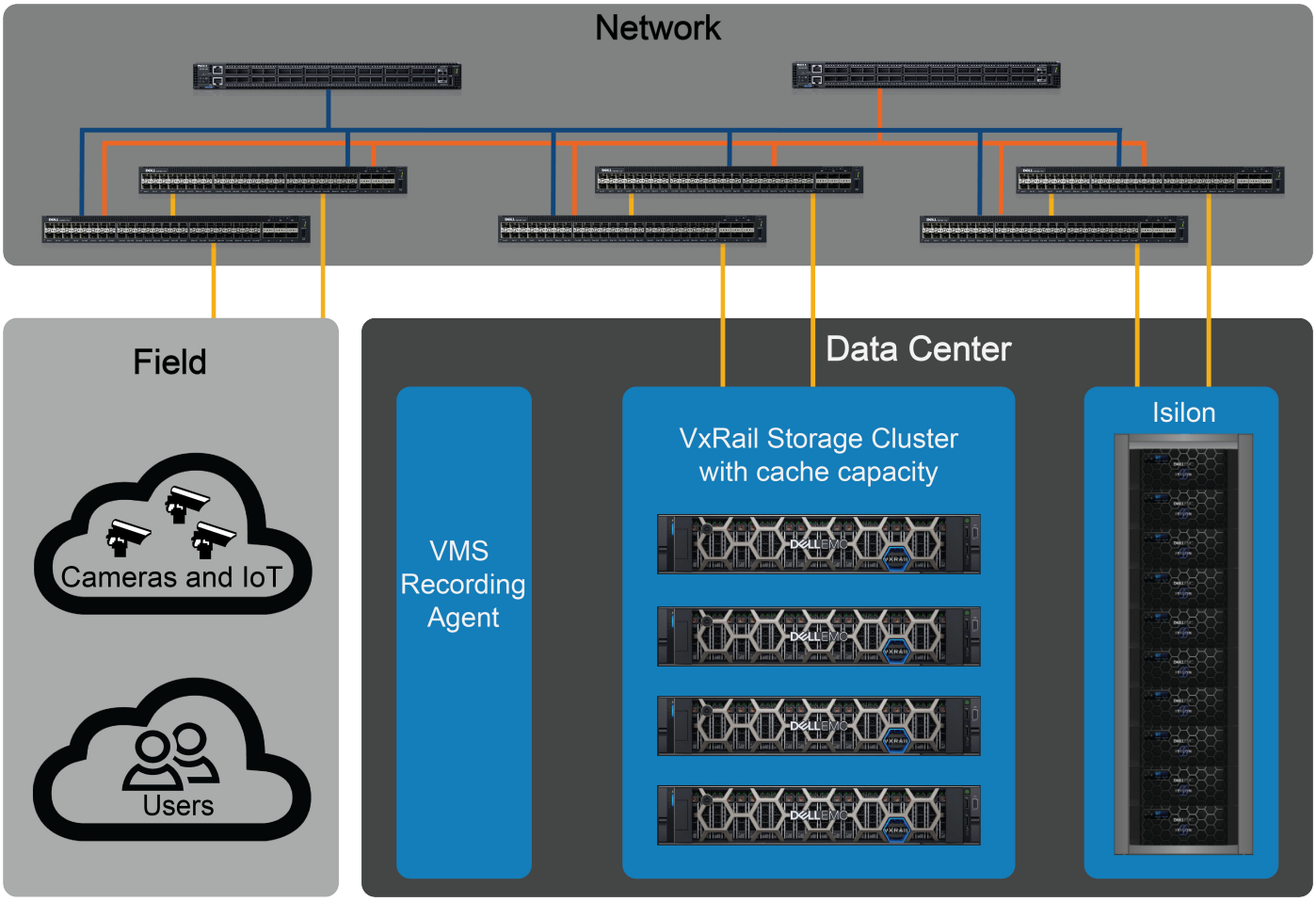


**Figure 5. Dell Safety & Security Lab VxRail test environment**

The VMware software solution in this Safety & Security environment uses VMware's vSAN, vSphere, and vCenter for Safety & Security management. The vCenter Server provides a platform for managing vSphere while vSAN provides a scalable storage solution with high availability.

# Dell Technologies Safety & Security VxRail environment

The Dell Safety & Security Lab recommends the following base configuration for a successful implementation:

| | |
|---|---|
| **Dell Storage platforms** | • Dell EMC Isilon<br>  ○ SMB protocol |
| **Virtualized environment** | • 6 vCPUs<br>• 12 GB memory<br>• Network adapter type: VMXNET3 (GbE and 10 GbE) |
| **VxRail P570 nodes (vSAN certified storage)** | • Dual Intel Xeon gold 6126 2.6G, 12C/24T<br>• 192 GB memory<br>• 10 x 3.84 TB SSD SAS Read Intense<br>• 2 x 800 GB SSD SAS Write Intense<br>• Intel 10GbE 4P X710 rNDC |
| **vSAN cluster** | • 5 VxRail P570 nodes (One node contains all Management servers)<br>• 50 total capacity drives |

| | |
|---|---|
| | • 10 Disk Groups (1 vSAN cache to 5 capacity SSD<br>• 10 GbE NIC connections for:<br>  ○ vSAN<br>  ○ Administration<br>  ○ vMotion<br>  ○ vSAN Managment |
| **Switching** | • Dual Dell S4148F-ON (top of rack) SmartFabric<br>• Dual Dell Z9100s network core (leaf) |
| **External storage** | • Isilon A2000<br>• 4 node with 20 drives per node |
| **Supporting Servers** | • Review stations: Dell PowerEdge servers - various models<br>• Work stations: Dell Precision - various models |

Refer to the following network and design guides for more information on configuring vSAN for your environment, or contact ProDeploy Plus for vSAN configuration assistance:

- VMware Storage and Availability Technical Documents
- VMware vSAN Design and Sizing Guide
- VMware vSAN Network Design

Microsoft MPIO is recommended for use with Unity and SC series arrays.

The Dell Safety & Security Lab's host hardware met and exceeded the minimum system requirements for a VxRail installation. The Milestone Recorder VM was running on vSphere 6.7 using Dell VxRail nodes.

# Releases validated

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

### Table 8. VMware releases

| Product | Release |
|---|---|
| vSAN Advanced | 6.7 Update 3 |
| VxRail P570 | 4.7.300 |
| vCenter Standard | 6.7 Update 3 |
| vSphere Enterprise plus | 6.7 Update 3 |

### Table 9. Isilon releases

| Product | Version |
|---|---|
| OneFS | 8.1.2 |

### Table 10. Milestone XProtect Corporate releases

| Release | Subrelease |
|---|---|
| Milestone XProtect Corporate | 2019 R3 |

# Connecting the VxRail and Isilon nodes

The VxRail nodes and Isilon nodes are not connected internally and must be integrated through external switches. Each node should be connected to 2 physical switches to ensure redundancy and avoid a single point of failure.

The following figure shows the standard configuration for the Isilon and VxRail racks.

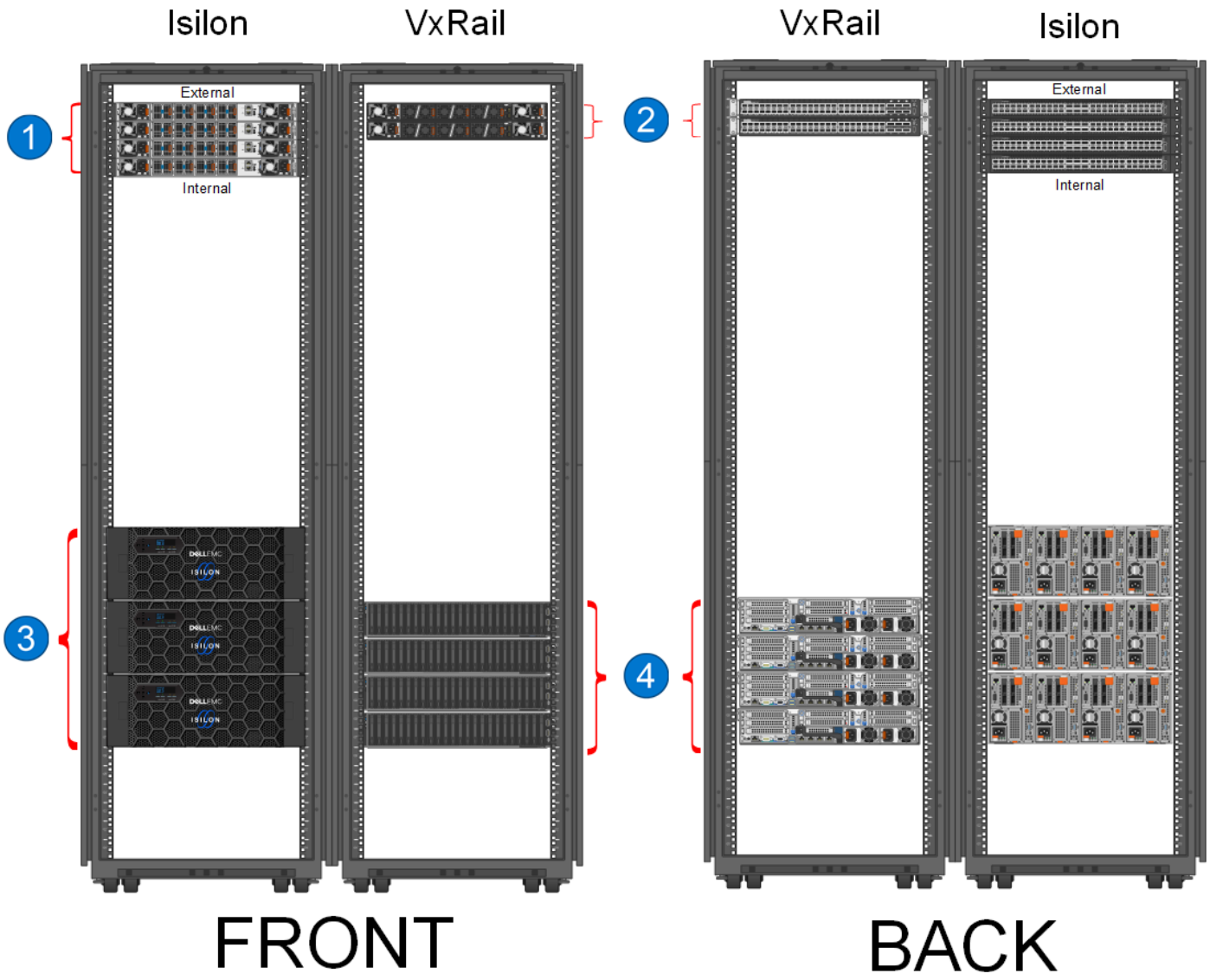


**Figure 6. Dell EMC Isilon and Dell VxRail rack configuration**

1. Dell S4148F-ON 10 GbE switches
2. Dell S4048-ON 10 GbE switches
3. Dell EMC Isilon A2000
4. Dell VxRail P570F nodes

# Connecting the VxRail P570 nodes

Connect the VxRail P570 nodes to the network starting with ports 1 and 2 on the switch. Add additional management nodes using open ports in ascending order (left to right) on the switch, as shown in the following figure.

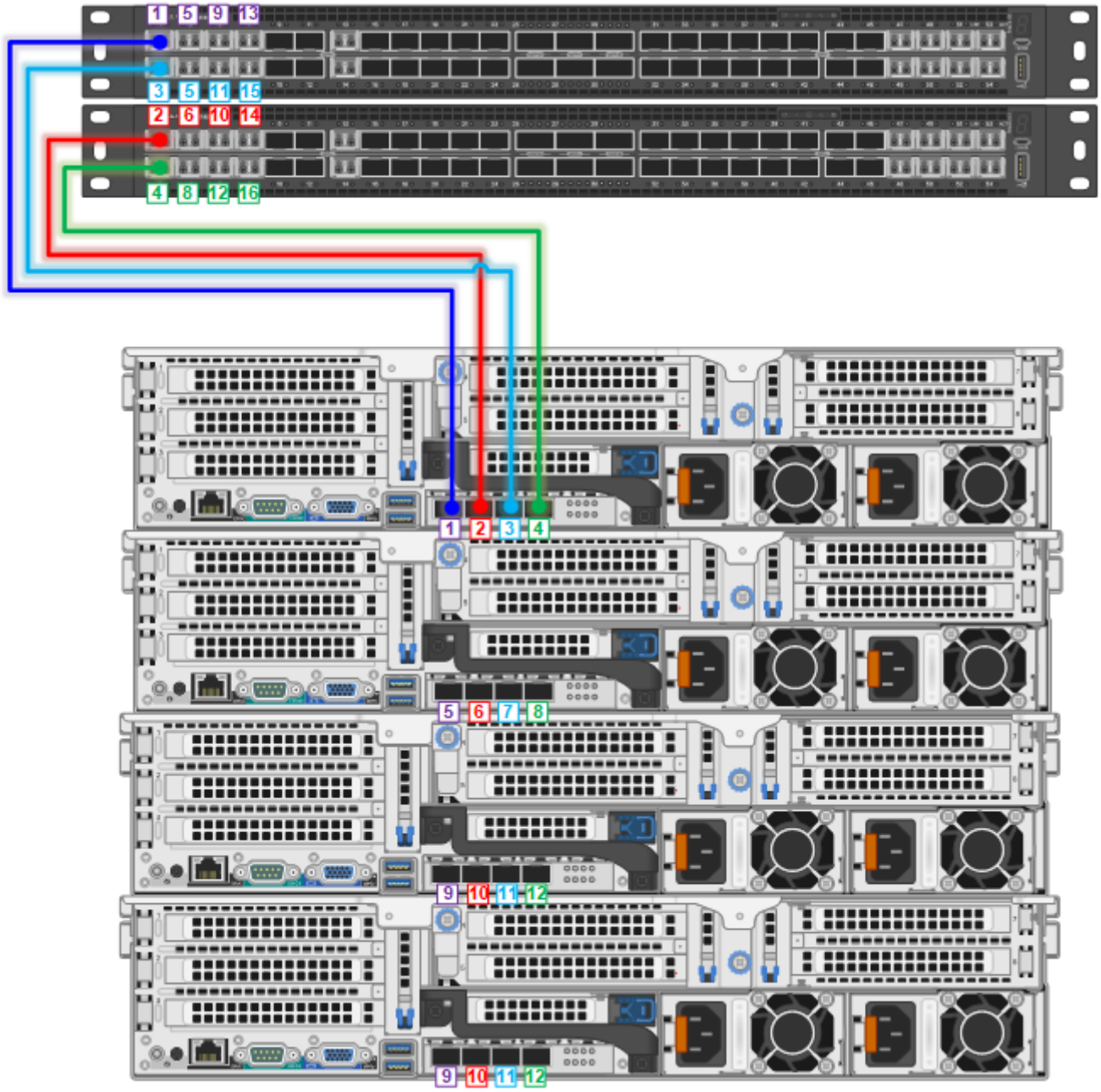


**Figure 7. VxRail P570 node cabling diagram**

# Connecting the Isilon nodes

Connect the Isilon nodes to the network, starting with node 1 and ports 1 and 2 on the external and internal switches .

Connect Node 1 on the Isilon to the network in the following manner:

- Port 1 on the Isilon to port 1 on the primary external switch (ext1)
- Port 2 on the Isilon to port 1 on the secondary external switch (ext2)
- Port 3 on the Isilon to Port 1 on the primary internal switch (int1)
- Port 4 on the Isilon to port 1 on the secondary internal switch (int2)

Add additional Isilon nodes using open ports in ascending order (left to right) on the switch, as illustrated in the following figure.

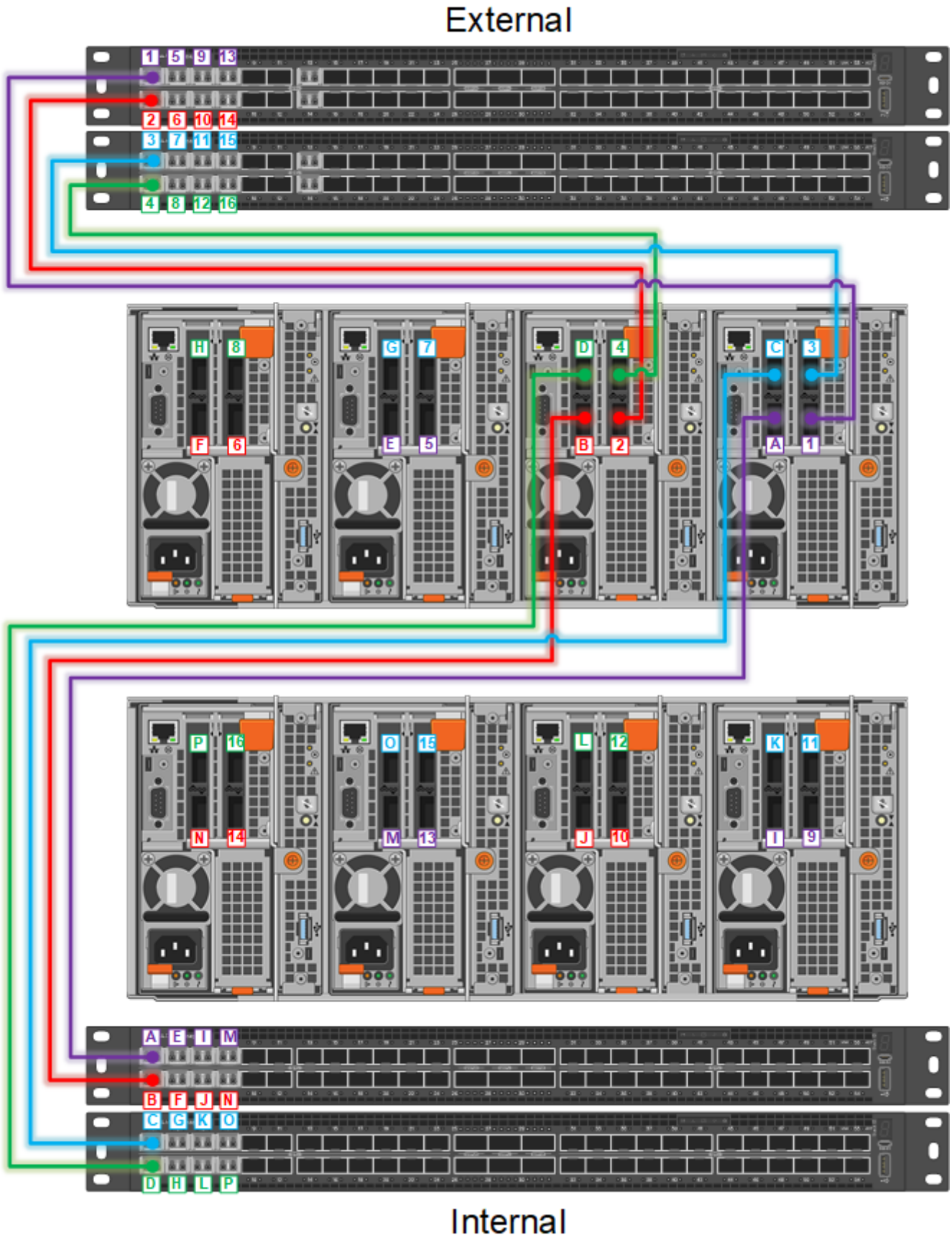


**Figure 8. Isilon node cabling diagram**

# 7

# XProtect-specific configuration

**Topics:**



## Configuring Active Directory and domain controller

Although local user account authentication is available, we configured Active Directory (AD) user account authentication in the lab to simplify user management.

### About this task

AD is a distributed directory service included with several Windows Server operating systems. It identifies resources on a network in order for users or applications to access them. If you wish to add users through the AD service, you must have a server with AD installed that acts as the domain controller on your network. Consult your network administrator regarding the use of AD with your XProtect deployment.

### Steps

1. Ensure that there is a server with AD installed and acting as the domain controller on the network.
2. Add all recording servers and management hosts to the available domain controller.
3. Add the Isilon cluster to the available domain controller.
4. Log in as the Domain user on the host.
5. In Windows Services, select **Milestone XProtect Corporate Recording Server**. Click the **Log On** tab and update the credentials for the Active Directory user.
6. Restart the service.

## Hard disk formatting

One factor that can impact a disk's performance in a safety and security video system is the cluster size of the formatted hard disk.

**NOTE:** Update the `allocation unit size` when formatting the hard drive to significantly improve the performance of the archive process.

Dell recommends the following `allocation unit size` settings:

| | |
|---|---|
| **Multi-tier implementation-Live DB** | Change the `allocation unit size` setting to 8 KB when formatting the hard disk for the Live DB in a two-tier structure. This block size is better suited for the balanced reads and writes rate caused by the archive process. |
| **Multi-tier implementation-Archive DB** | Change the `allocation unit size` setting to 64 KB when formatting the hard disk for the Archive DB. A 64 KB block size significantly improves the performance of the archive process. |

| | |
|---|---|
| **Single-tier implementation** | Change the`allocation unit size` setting to 64 KB when formatting the hard disk for the Live DB only. |

See the Microsoft Support article Default cluster size for NTFS, FAT, and exFAT for more information about single and multi-tier allocation unit sizes.

# Enabling motion detection

If motion detection is not working, you must enable a new rule for motion detection.

### Steps

1. Disable the **Default Record on Motion Rule** on the management server.
2. Add a new rule named **Record Always** using the following definition:

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

Perform an action when time interval ends
stop recording immediately
```

# Modifying the number of archive process threads

When using archive storage, such as NAS attached Isilon scale-out cluster, each recording server must be modified to use either three or four archive processes. By default, XProtect uses a single thread.

### About this task

To minimize the risk of errors, the `RecorderConfig.xml` file can be edited with the Recorder Configuration Manager tool available from Milestone.

### Steps

1. Stop the Milestone XProtect Corporate Recording Server Service.
2. Go to: `C:\ProgramData\Milestone\XProtect Recording Server`.
3. Open the `RecorderConfig` file.
4. Edit the file as follows to change the low priority archive thread pool size to 4 and the high priority archive thread pool size to 4:

```
<thread_pools>
<delete_thread_pool_size>2</delete_thread_pool_size
<low_priority_archive_thread_pool_size>4</low_priority_archive_thread_pool_size>
<high_priority_archive_thread_pool_size>4</high_priority_archive_thread_pool_size>
</thread_pools>
```

5. Save the file.
6. Start the Milestone XProtect Corporate Recording Server Service.

**NOTE:** These steps apply to XProtect starting with version 2014.

# Modifying the Archive DB write block size

When using archive storage, such as NAS attached Isilon scale-out cluster, the Archive DB write block must be modified.

**Steps**

1. Stop your Recording Server Services.
2. Rename the file `%ProgramFiles%\Milestone\XProtect Corporate Recording Server\VideoOS.Platform.Database.dll` to, for example, `VideoOS.Platform.Database.dll,orig`.
3. Open the file `%ProgramData%\Milestone\XProtect Recording Server\RecorderConfig.xml` in an editor.
4. Update the disk utilization section. Use one of the following methods:
   - For Milestone version 2013 5.0, add the following xml code highlighted in bold:

```
<disk_utilization>
  <max_bytes_in_block_files>16777216</max_bytes_in_block_files>
  <max_records_in_block_files>2000</max_records_in_block_files>
  <truncate_block_files>true</truncate_block_files>
  <precreate_block_files>true</precreate_block_files>
  <precreate_sizes>
    <regular>16777216</regular>
    <sequence>65536</sequence>
    <signature>4194304</signature>
  </precreate_sizes>
  <media_block_files use_os_cache="true">
  <read_buffer_size>4096</read_buffer_size>
  <write_buffer_size>4096</write_buffer_size>
 </media_block_files>
 <sequence_block_files use_os_cache="true">
  <read_buffer_size>4096</read_buffer_size>
  <write_buffer_size>4096</write_buffer_size>
 </sequence_block_files>
 <signature_block_files use_os_cache="true">
  <read_buffer_size>4096</read_buffer_size>
  <write_buffer_size>4096</write_buffer_size>
 </signature_block_files>
 <index_files use_os_cache="true">
  <read_buffer_size>4096</read_buffer_size>
  <write_buffer_size>4096</write_buffer_size>
 </index_files>
 <chunk_files use_os_cache="true">
  <read_buffer_size>65536</read_buffer_size>
  <write_buffer_size>65536</write_buffer_size> <!-- default 4096 -->
 </chunk_files>
</disk_utilization>
```

   - For Milestone version 2013 R2 through 2017, the 2018 version has these values included. Update the `chunk_files use_os_cache` section. Modify the `read_buffer_size` and `write_buffer_size` values to `65536`.

```
<chunk_files use_os_cache="true">
  <read_buffer_size>65536</read_buffer_size>
  <write_buffer_size>65536</write_buffer_size> <!-- default 4096 -->
</chunk_files>

<precreate_block_files>false</precreate_block_files>

<maxframesinqueue>500</maxframesinqueue>
```

5. Save the `RecorderConfig.xml` file.
6. Restart your recording server.

# Isilon OneFS for the Archive DB

Configure XProtect to use an Isilon cluster for the Archive DB.

Refer to the *Dell EMC Isilon Storage with Video Management Systems: Configuration Guide* to configure the following with Isilon OneFS:

- Configure SmartConnect and Domain Name System (DNS)
- Configure SmartQuotas

## OneFS 8.1 job workers (required)

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

To modify the job workers to 0 per core, run the following command from the command line interface:

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

**NOTE:** With OneFS 8.2.2, this setting will be the default and this modification will not be necessary.

# Multipathing and NIC failures

Configure the Unity and SC block storage arrays with multiple paths to recorders using Microsoft MPIO. For redundancy, configure multiple NICs with the recorders and controllers. Recorders that are configured with multipathing reconnect to the volume across another available path after a NIC failure.

The TCP Max transmissions value determines how many times the Transmission Control Protocol (TCP) retransmits an unacknowledged data segment on an existing connection. The TCP retransmits data segments until they are acknowledged or until this value expires.

TCP/IP adjusts the frequency of retransmissions over time. The TCP establishes an initial retransmission interval by measuring the round trip time on the connection. This interval doubles with each successive retransmission on a connection, and it is reset to the initial value when responses resume.

To reduce the reconnection time and eliminate video loss, adjust the following TCP retransmission timers:

**NOTE:** It is recommended that you perform a backup before editing registry settings.

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
Value Name:  TcpMaxDataRetransmissions
Data Type:   REG_DWORD - Number
Valid Range: 0 - 0xFFFFFFFF
Value:     3
```

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
Value Name:  TCPInitialRtt
Data Type:   REG_DWORD - Number
Valid Range: 0 - 0xFFFFFFFF
Value:     2
```

To reduce path failover times for volumes that are mapped through ESXi hosts using raw device mapping (RDM) LUN's or Datastores, use the following timeouts. Modify these settings on the iSCSI software adapter for each SAN attached host. These settings are located on the **Advanced** tab in the properties section of the individual ESXi servers Software iSCSI adapter.

```
iSCSI Login Timeout 5
NoopInterval 2
NoopTimeout 10
Recovery Timeout 4
Delayed ACK Disabled
```

# iSCSI initiator queue depth on ESXi hosts

Define the iSCSI initiator queue depth for each SAN attached ESXi host.

Run the following command to iSCSI initiator queue depth:

```
esxcli system module parameters set -m iscsi_vmk -p iscsivmk_LunQDepth=255
```

# Index

## O