Surveillance

Dell EMC Isilon Storage with Video Management Systems

Configuration Best Practices Guide

H14823

REV 2.0

Dell EMC
Surveillance Lab
Validated

DELL EMC

Published April 2018

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

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

CONTENTS

CHAPTER 1

Introduction

This chapter presents the following topics:

Solution overview

This guide is intended for internal Dell EMC personnel and qualified Dell EMC partners. It provides configuration instructions for preparing Dell EMC Isilon® storage systems for use with video management software (VMS).

The purpose of this guide is to help users understand how to configure Isilon storage for video surveillance specific implementations that include both hardware and software elements. This guide is not a replacement for Dell EMC partner implementation guides.

Assumptions

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

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

- Associated with product implementation
- VMS (partner)-certified to install VMS (long) services
- Proficient in installing and configuring Isilon storage solutions
- Familiar with installing and configuring VMware hypervisors and the appropriate operating system, such as Microsoft Windows or a Linux distribution
- Able to access the *Dell EMC Isilon Storage with Video Management Systems Best Practices: Configuration Guide*

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

CHAPTER 2

Configuring the solution

This chapter presents the following topics:

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 surveillance workloads, the Dell EMC Surveillance Lab recommends using two SSD system drives per node in clusters where it is supported, such as the NL-series.

Isilon clustered storage system

Isilon NAS was designed and developed specifically for storing, managing, and accessing digital content and other unstructured data.

An Isilon clustered storage system is composed of three or more nodes. Each node is a self-contained, rack-mountable device that contains industry-standard hardware such as disk drives, CPUs, memory, and network interfaces. These nodes are integrated with the proprietary Isilon OneFS™ operating system, which is a distributed networked file system that unifies a cluster of nodes into a single shared resource.

Cluster size

We recommend a minimum cluster size of five nodes for all single node chassis, and four nodes for all quad node chassis, even if you are not writing to all of them. For example, if you are implementing a four-node recorder solution, implement a five-node cluster. This also meets the recommended best practices for data protection.

To estimate the ideal number of nodes in a cluster, you need to consider cluster bandwidth and capacity.

Sizing by bandwidth

We recommend a cluster size with one or more additional nodes than calculated in bandwidth sizing. This ensures that failover of a node allows for redistribution of NAS connections and avoids any frame loss.

Sizing by aggregate capacity

We recommend a cluster size with enough usable capacity to handle 110 percent of the calculated space requirement, with a minimum added capacity of one full node plus 10 percent. The values are based on camera bit rate.

The Isilon sizing tool can use both the sizing by bandwidth and sizing by aggregate capacity methods when calculating ideal cluster size.

Data protection

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

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

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

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

Isilon protection with OneFS

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

OneFS 8.1 job workers (required)

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

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

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

Isilon SmartConnect

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

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

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

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

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

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

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

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

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

Round-robin (recommended)

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

Connection count

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

Network throughput

Based on NIC utilization. Use of throughput requires that each recording server 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 recording server IP address pool. Define additional pools for management (such as Isilon InsightIQ® or administrative access), evidence repository, post process, or other use.

Configuring SmartConnect (optional)

You can configure Isilon SmartConnect™ to provide load balancing of recording servers across nodes in an Isilon cluster. With the server message block (SMB) protocol, load balancing occurs at connection initiation with the Isilon cluster.

- Configure SmartConnect for round-robin.

- When designing per node capacity, allow for failover scenarios. If a node fails or is taken offline for maintenance or node removal, SmartConnect must be able to re-attach the recording servers on remaining active nodes, without overloading any node.
- The SMB protocol, along with their predictor Common Internet File System (CIFS), restricts the accuracy of load balancing. For best results, use the Isilon management console to monitor session connectivity and load balancing. The SMB protocol includes SMB, SMB2, and SMB3

Procedure

1. Select **Networking Configuration**.
2. Under **Subnet** > **Settings**, define the SmartConnect service IP (SSIP) address. The SSIP address is the IP address that the DNS uses for the Isilon Authoritative name service.
3. Under **Pool settings**:
   a. Define the SmartConnect zone name, which is the name to which clients connect.

   b. Define the SmartConnect service subnet (the subnet that has the SSIP configured on the DNS server).

   c. Define the connection balancing policy to **Round Robin**.

   d. Set the IP allocation strategy to **Static**.
4. Verify this configuration on the SmartConnect dashboard.

Configuring SmartConnect

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

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

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

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

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

SmartConnect balances connection loads to the Isilon cluster and handles connection failover. With SmartConnect, all 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 servers to specified nodes in the Isilon cluster. Use a unique IP address pool for video recording and read/write access.

Network throughput

Based on NIC utilization. Use of throughput requires that each 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 IP address pool. Define additional pools for management (such as Isilon InsightIQ™ or administrative access), evidence repository, post process, or other use.

Procedure

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.

Isilon SmartQuotas

When using Isilon clusters, we recommend using Isilon SmartQuotas™ to protect the storage from a run-away application or misconfigured recording server. When configuring SmartQuotas, you must use a Hard Quota.

SmartQuotas allows administrators to limit the storage used for each recording server and presents to the server a view of available storage based on the assigned quota. SmartQuotas allows each recording server to calculate its available disk space and react correctly. Without SmartQuotas, the VMS administrator must anticipate the total write rate to the cluster and adjust the Min Free Space field on each recording server accordingly. A miscalculation could result in lost video. SmartQuotas resolves the issues caused by manual calculations.

Configure SmartQuotas when more than one recording server is writing to the Isilon cluster and/or the cluster is shared with other users. Enable SmartQuotas and define a quota for each share or directory.

Large file system, small view (SmartQuotas)

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

There are three directory-level quota systems:

Advisory limit

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

Soft limit

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

Hard limit (recommended)

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

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

If necessary, both Isilon and the VMS (partner) Recorder can add or subtract storage, even if a hard quota is set.

Configuring SmartQuotas (recommended)

The SmartQuotas feature enables you to limit the storage that is used for each VMS (partner) 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.

To better cache the meta data associated with SmartQuotas, the Dell EMC Surveillance 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 VMS (base) 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.

Procedure

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.

Configuring authentication and access control

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

The following three tests were conducted:

Full Active Directory (recommended)

Where the VMS (base) server and the Isilon cluster are part of the same Windows domain.

Partial Active Directory

Where the VMS (base) servers are part of the Windows domain, but the Isilon cluster is administered locally.

Fully locally administered control

Where the VMS (base) servers and the Isilon cluster are administered locally.

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

Procedure

1. 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 VMS (partner) 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 VMS (short) 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 VMS (short) 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.

Impact policy and priority configuration

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

Releases with OneFS 7.0 or greater

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

Releases prior to OneFS 7.0

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

Priority configuration

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

Unique share naming

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

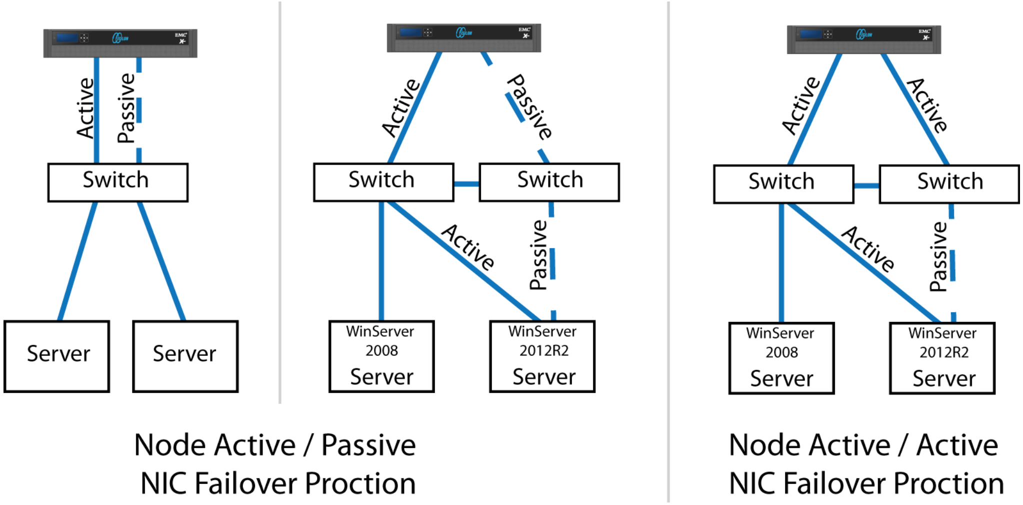
To avoid corruption caused by overwriting or grooming (deleting) files prematurely, create a unique share for each recording server.

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 VMS (short) 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 EMC 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 1 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 .

Note

This setting does not require a SmartPool license.

Impact policy and priority configuration

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

Releases with OneFS 7.0 or greater

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

Releases prior to OneFS 7.0

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

Priority configuration

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

CHAPTER 3

Conclusion

This chapter presents the following topics:

Summary

The Dell EMC Surveillance Lab performed comprehensive testing with multiple VMS vendors against many Dell EMC Isilon clusters.

Dell EMC Isilon scale-out storage

Isilon scale-out storage is ideal for midtier and enterprise customers. An Isilon cluster is based on independent nodes working seamlessly together to present a single file system to all users.

Licensed SmartQuotas options can be configured so that each recording server view of the storage is based on the assigned quota and not the entire file system. Dell EMC recommends using SmartQuotas with Dell EMC Isilon as a best practice.