

Dell EMC Storage with Honeywell DVM

Surveillance

February 2019

H14749.2

Configuration Best Practices

Abstract

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

Dell EMC Solutions

Dell EMC

Surveillance Lab

Validated

Honeywell

Copyright © 2016-2019 Dell Inc. or its subsidiaries. All rights reserved.

Published February 2019

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, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

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

CONTENTS

Chapter 1	Introduction	5
	Solution overview.....	6
	Scope.....	6
	Assumptions.....	6
Chapter 2	Configuring the solution	9
	Design concepts.....	10
	Dell EMC Unity.....	10
	Disk drives.....	10
	Storage pool configuration (recommended).....	11
	LUN configuration.....	11
	iSCSI initiators.....	12
	Configure iSCSI front-end ports	12
	Connect the iSCSI target on Windows.....	13
	Format the iSCSI target on Windows.....	13
	Fibre Channel configuration.....	14
	Isilon (NAS).....	14
	Data protection.....	15
	OneFS 8.1 job workers (required).....	15
	Impact policy and priority configuration.....	15
	Volume limits.....	16
	Large file system, small view (SmartQuotas).....	16
	Configuring SmartQuotas (recommended).....	16
	Continuous Availability.....	17
	Unique share naming.....	17
	Configuring SmartConnect	17
	I/O optimization configuration.....	19
	Configuring authentication and access control.....	19
	SMB specific configuration.....	19
	Link aggregation.....	22
	Multipathing and NIC failures.....	22
	iSCSI Initiator Queue Depth On ESXi hosts.....	23
	Releases tested.....	23
Chapter 3	Conclusion	25
	Summary.....	26
	Dell EMC Unity arrays.....	26
	Dell EMC Isilon scale-out storage.....	26

CONTENTS

CHAPTER 1

Introduction

This chapter presents the following topics:

- [Solution overview](#).....6
- [Scope](#).....6
- [Assumptions](#).....6

Solution overview

Honeywell video management software (VMS) for video surveillance is scalable, provides sensor integration, and is standards-based for open integration. Honeywell VMS incorporates smart technology to automatically detect, analyze, and classify behaviors of people and vehicles. This solution is ideally coupled with Isilon Scale-out NAS storage or . These options provide the customer with exceptional performance and reliability creating a successful implementation.

The purpose of this Configuration Guide is to help Dell EMC field personnel understand how to configure Dell EMC storage system offerings to simplify Honeywell DVM implementation. This document is not a replacement for the Honeywell implementation guide nor is the document a replacement for the Dell EMC sizing guides.

Honeywell DVM provides a comprehensive system for video surveillance. This system enables customer's network and security teams to collaborate effectively in a highly scalable environment that combines video and network techniques to optimize the experience. The Dell EMC storage system provides no single point of failure while the Honeywell DVM design ensures resilience.

Scope

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

The following Dell EMC storage systems have been tested:

- Dell EMC Isilon®
- Dell EMC Unity®
- Dell EMC PowerEdge®

This guide supplements the standard [Dell EMC Isilon Storage with Video Management Systems Best Practices: Configuration Guide](#) and provides configuration information specific to Honeywell DVM .

Note

All performance data in this guide was obtained in a rigorously controlled environment. Performance varies depending on the specific hardware and software used.

Assumptions

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

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

- Associated with product implementation
- Honeywell-certified to install Honeywell DVM services
- Proficient in installing and configuring Unity storage solutions
- 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 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 EMC Surveillance Lab using worst-case scenarios to establish a performance baseline. Lab results might differ from individual production implementations.

CHAPTER 2

Configuring the solution

This chapter presents the following topics:

- [Design concepts](#)..... 10
- [Dell EMC Unity](#)..... 10
- [Isilon \(NAS\)](#)..... 14
- [Multipathing and NIC failures](#)..... 22
- [iSCSI Initiator Queue Depth On ESXi hosts](#)..... 23
- [Releases tested](#)..... 23

Design concepts

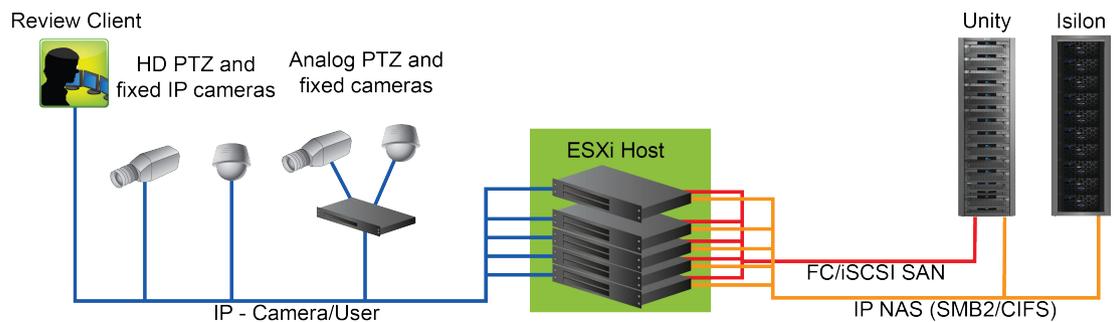
There are many design options for a Honeywell DVM implementation. These design details are beyond the scope of this paper.

The *Honeywell Building Solutions Digital Video Manager Release 500* provides the information that you need to plan a Honeywell DVM system. The document is available from a Honeywell partner or through dvm.honeywell.com. This configuration guide is not intended to replace or supersede any Honeywell document.

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

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

Figure 1 Honeywell DVM architecture



Dell EMC Unity

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

The Unity series arrays are designed for midtier 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 storage arrays, see [Dell EMC Block Storage with Video Management Systems Best Practices: Configuration Guide](#)

Disk drives

Although any supported drive will work, video surveillance systems typically rely on the density of the array. Dell EMC recommends NL-SAS drives of the highest available density in this solution. In general, we used one-terabyte (TB) or multi-TB NL-SAS drives when performing our tests.

Note

Because of the high percentage of sequential, large block writes, Dell EMC does not recommend using flash drives for video storage within a surveillance application.

Storage pool configuration (recommended)

The tests we conducted show how storage pools that are defined with the maximum allowable number of disks per pool perform as well as, or better than, traditional RAID groups. Therefore, Dell EMC recommends that you use storage pools rather than RAID groups. Storage pools also reduce the required array management tasks.

The Unity and SC series array architecture is optimized for storage pools. A storage pool is a construct that is built over one, or more commonly multiple, RAID groups. LUNs are built on top of the storage pool. The read/write activity is a random distribution across all disks defined to the storage pool. This distribution results in increased and balanced per disk utilization and improved performance when compared to traditional RAID implementations.

The RAID groups underlying storage pools can be either RAID 5 or RAID 6. RAID 5 is used for optimizing the array to achieve the maximum amount of storage and RAID 6 is used for enhancing data protection. Our tests using an isolated surveillance infrastructure did not reveal any notable performance variances when using RAID 5 as compared to RAID 6.

Building a storage pool is a straightforward process. You can configure either RAID 5 or RAID 6 pools depending on the storage system restrictions and the level of risk that the customer is willing to accept. When configuring storage pools, use large storage pools with large logical unit number (LUN) sizes, and configure the LUNs as thick. Do not use thin LUN provisioning.

Dell EMC recommends the following RAID configurations for SAN arrays:

- RAID 5 or RAID 10 with SAS drives
- RAID 6 with NL-SAS drives

Procedure

1. In Unisphere, select **Storage > Storage Pools** for block.
2. Click **Create** under **Pools** in the **Pools** section.
3. Set the following options for the storage pool:
 - Storage pool name
 - RAID type
 - Number of SAS drives
 - Number of NL SAS drives
4. Choose a method for selecting disks to include in the storage pool:
 - **Automatic:** Provides a list of available disks.
 - **Manual:** Enables you to select specific disks to include in the storage pool from a list of available disks. Be sure to clear the automatic disk recommendation list before you select new disks from the list.
5. Select **Perform a Background verify on the new storage** and set the priority to medium.
6. Click **Apply**, and then click **YES** to create the storage pool.

LUN configuration

A Unity or SC series pool LUN is similar to a classic LUN. Pool LUNs comprise a collection of slices. A slice is a unit of capacity that is allocated from the private RAID

groups to the pool LUN when it needs additional storage. Pool LUNs can be thin or thick.

Thin LUNs typically have lower performance than thick LUNs because of the indirect addressing. The mapping overhead for a thick LUN is less than for a thin LUN.

Thick LUNs have more predictable performance than thin LUNs because they assign slice allocation at creation. Because thick LUNs do not provide the flexibility of oversubscribing like a thin LUN, use thick LUNs for applications where performance is more important than saving space.

Thick and thin LUNs can share the same pool, enabling them to have the same ease-of-use and benefits of pool-based provisioning.

Procedure

1. In Unisphere, right-click a storage pool and then click **Create LUN**.
2. Type the user capacity for the LUN.
3. Type the starting **LUN ID**, and then select the number of LUNs to create.
For example, if the selected LUN ID is 50, and the selected number of LUNs to create is 3, the names for the LUNs are 50, 51, and 52.
4. Select **Automatically assign LUN IDs as LUN names**.
5. Click **Apply**.

iSCSI initiators

Software or hardware initiators may be used with VMware ESXi server or a non-virtualized server.

Microsoft Internet SCSI (iSCSI) initiators

For both physical servers and VMware ESXi server, the Dell EMC Surveillance Lab uses Microsoft iSCSI initiators with excellent results.

Hardware iSCSI initiators

Hardware iSCSI initiators can be used. There are many iSCSI initiators available on the market, and results might vary.

Configure iSCSI front-end ports

Configure the storage system iSCSI front-end ports when the cabling is completed.

For cable specifications, refer to the technical specifications for your storage system. You can generate an up-to-date version of these specifications using the **Learn about storage system** link on the storage system support website.

For high availability:

- Connect one or more iSCSI front-end data ports on SP A to ports on the switch or router. If two switches or routers are available, connect the same number of iSCSI front-end data ports on SP B to ports on the same switch or router, or on another switch or router.
- For a multiple NIC or iSCSI host bus adapter (HBA) server, connect one or more NIC or iSCSI ports to ports on the switch or router. If two switches or routers are available, connect the same number of NIC or iSCSI HBA ports to ports on the same switch or router, or on another switch or router.

Procedure

1. To start Unisphere, in an Internet browser, type the IP address of the storage system SP that you want to manage.
2. Type your user name and password.
3. Click **Login**.
4. From Unisphere, select **System > Hardware > Storage Hardware**.
5. Identify the storage system iSCSI front-end ports by selecting **SPs > SP A/B > IO Modules > Slot [#] > Port [#]** in the **Hardware** window.
For example: **SPs > SP A > IO Modules > Slot A4 > Port 0**
6. Click **OK**.
7. Highlight the iSCSI front-end port that you want to configure and click **Properties**.
8. To assign an IP address to the port, click **Add** in **Virtual Port Properties**.
9. Click **OK** and close all open dialog boxes
10. Click **OK**.
11. Click **OK**.

The iSCSI Port Properties window displays the added virtual ports in the Virtual Port Properties area.

Connect the iSCSI target on Windows

When the iSCSI target is connected to the Windows iSCSI initiator, the volume is shown on the computer as a local physical hard drive, which can be used for video storage.

Procedure

1. Connect the iSCSI target with the Windows iSCSI initiator.
 - a. Launch the iSCSI initiator at **Control Panel > Tools**.
 - b. On the iSCSI Initiator **Properties** page, click **Discovery**.
 - c. Enter the IP address of the NAS and then click **OK**.
 - d. Click **Targets** and then select the available iSCSI targets that you want to connect.
 - e. Click **Connect**.
 - f. Click **OK**.

On successful connection, the status changes to Connected.

Format the iSCSI target on Windows

After the iSCSI target has been successfully connected on Windows, Windows displays the iSCSI target as an Unallocated Disk. Set the disk to online and format the disk before you can start using it as a local disk to store video. Formatting the disk using the 64k allocation unit provides better performance.

Procedure

1. Right-click **Computer** and then click **Manage**.
2. Click **Disk Management** to display current disk information.

3. Right-click **iSCSI Disk** and then click **Online** to activate the disk.
4. Right-click **iSCSI Disk** again to open the **New Simple Volume Wizard** window.
5. Follow the wizard to complete formatting the disk.

When the wizard completes, the disk appears as a local hard disk drive, which can then be used as extra storage space.

Fibre Channel configuration

To transfer traffic from the host servers to shared storage, the serial-attached network (SAN) uses the Fibre Channel (FC) protocol that packages SCSI commands into FC frames.

Note

iSCSI is prevalent for video security implementations because it often provides a lower-cost option when compared to FC.

To restrict server access to storage arrays that are not allocated to the server, the SAN uses zoning. Typically, zones are created for each group of servers that access a shared group of storage devices and LUNs. A zone defines which HBAs can connect to specific service providers (SPs). Devices outside a zone are not visible to the devices inside the zone.

Zoning is similar to LUN masking, which is commonly used for permission management. LUN masking is a process that makes a LUN available to some hosts and unavailable to other hosts.

Zoning provides access control in the SAN topology. Zoning defines which HBAs can connect to specific targets. When you use zoning to configure a SAN, the devices outside a zone are not visible to the devices inside the zone.

Zoning has the following effects:

- Reduces the number of targets and LUNs presented to a host
- Controls and isolates paths in a fabric
- Prevents non-ESXi systems from accessing a particular storage system and from possible virtual machine file system (VMFS) data loss
- Optionally, separates different environments, such as test and production environments

With VMware ESXi hosts, use single-initiator zoning or single-initiator-single-target zoning. The latter is the preferred zoning practice because it is more restrictive and prevents problems and misconfigurations that can occur on the SAN.

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

Data protection

In the Isilon N+M data protection model, N represents the number of nodes, and M represents the number of simultaneous node, drive, or a combination of node and drive failures that the cluster can withstand without incurring data loss. N must be larger than M.

Isilon OneFS supports N+1, N+2, N+3, and N+4 data protection schemes, and up to 8x mirroring. OneFS also supports several hybrid protection schemes. These include N+2:1 and N+3:1, which protect against two drive failures or one node failure, and three drive failures or one node failure, respectively.

The following best practices are based on a five-node minimum cluster size. You can use cluster sizes as small as a three-node cluster, but Dell EMC does not recommend this.

- Our five-node cluster lab tests were based on the Isilon recommended +2:1 protection level for this node count range. Larger node-count clusters have more disks, which cause an increase in the possibility of multiple disk failures. For larger clusters, consult the Isilon team or your Isilon representative for appropriate protection schemes: N+2:1, N+2, N+3, or N+4.
- Include a minimum free space calculation for proper cluster sizing. Dell EMC recommends a cluster size that enables a node to be removed, while retaining a minimum of 10 percent free space in the remaining capacity. This free space ensures that node removal and node failures have minimal or no impact on video ingestion.

An Isilon sizing tool provides a more accurate calculation. You can find this tool at <https://isilon-lawndart.herokuapp.com/pools/search>. Other sizing tools are available for sizing bandwidth and storage capacity needed.

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.

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
```

Impact policy and priority configuration

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

Releases with OneFS 7.0 or greater

Dell EMC recommends using OneFS 7.0 or later to maximize bandwidth and minimize video review response times. You can use the default impact policy with Isilon X400, Isilon X410, Isilon NL410, and greater. For less powerful nodes, such

as the Isilon X200 and earlier running OneFS 7.0 or greater, modify all jobs to use an impact policy of **Low**.

Releases prior to OneFS 7.0

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

Priority configuration

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

Volume limits

Implementations greater than 8 TB are common when video is stored on high-end storage, such as .

Large file system, small view (SmartQuotas)

Although it is possible to assign the full Isilon cluster file system to a single Honeywell 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 Honeywell 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 Honeywell 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 Digital Video Manager 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.

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.

Continuous Availability

Continuous Availability (CA) is a feature in OneFS 8.0 that contributes to a transparent failover during a node or NIC failure. Dell EMC recommends using CA enabled shares to minimize video loss during node or NIC failure operations.

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.

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 Honeywell 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 Honeywell 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.

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.

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 Honeywell.

Note

This setting does not require a SmartPool license.

Configuring authentication and access control

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

The following three tests were conducted:

Full Active Directory (recommended)

Where the Digital Video Manager server and the Isilon cluster are part of the same Windows domain.

Partial Active Directory

Where the Digital Video Manager servers are part of the Windows domain, but the Isilon cluster is administered locally.

Fully locally administered control

Where the Digital Video Manager servers and the Isilon cluster are administered locally.

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

Procedure

1. Select **Cluster Management > Access Management**.
2. Select **Access zone** and ensure that the **System access zone** has the provider status **Active Directory**, **Local**, and **File** marked with a green dot.
3. Under **Active Directory**, select **Join a domain** and add the Windows domain and appropriate users using one of the following options:
 - When the Isilon cluster and Honeywell 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 DVM 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 DVM 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.

SMB specific configuration

The Dell EMC Surveillance 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.

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.

Procedure

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.bkul
```

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.bkul /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.

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

Procedure

1. Set the parameters in the `sysctl` 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.data_lock.initiator.lazy_queue_goal=
$MDS
```

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

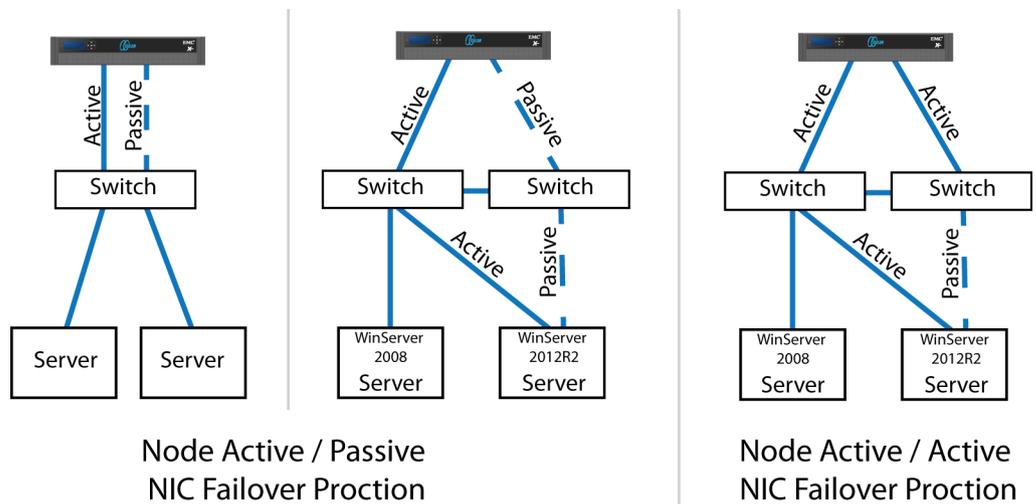
```
cat /etc/mcp/override/sysctl.conf
net.inet.tcp.keepidle=61000 #added by script
net.inet.tcp.keepintvl=5000 #added by script
kern.maxvnodes=10000 #added by script
kern.minvnodes=10000 #added by script
efs.lin.lock.initiator.lazy_queue_goal=10100 #added by script
efs.ref.initiator.lazy_queue_goal=10100 #added by script
efs.mds.block_lock.initiator.lazy_queue_goal=7500 #added by
script
efs.bam.data_lock.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 DVM 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 2 Isilon Active/Passive and Active/Active configuration



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
```

Releases tested

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

Table 1 SAN firmware builds

Model	Firmware
Unity	4.4.1.1539309879

Table 2 OneFS releases

Model	OneFS version
H400	8.1.1.1

Table 2 OneFS releases (continued)

Model	OneFS version
HD400	7.2.1
NL410	7.2.1
X410	7.2.1

Table 3 Honeywell DVM releases

Release	Subrelease
Honeywell DVM	700.1
	600.1 Build 1833

CHAPTER 3

Conclusion

This chapter presents the following topics:

- [Summary](#).....26

Summary

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

Dell EMC Isilon scale-out storage

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

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

Dell EMC Unity arrays

The use of storage pools to create LUNs within the Dell EMC Unity arrays greatly simplifies the configuration and increases the performance when compared to traditional block-level storage. Either iSCSI or FC can be implemented. FC performs better than iSCSI.

Dell EMC Isilon scale-out storage

Dell EMC 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 Recorder view of the storage is based on the assigned quota and not the entire file system. We recommend using SmartQuotas with Honeywell DVM as a best practice.