Dell EMC Storage with Airship Digital Video Recording System

Surveillance

December 2018

H17541

Configuration Best Practices Guide

Abstract

This configuration guide aims to help Dell EMC field personnel understand how to configure Dell EMC storage system offerings to simplify the implementation of the Airship Digital Video Recording (DVR) System.

Dell EMC Solutions

DELLEMC

CONTENTS

CONTENTS

CHAPTER 1

Introduction

This chapter presents the following topics:

Purpose

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

Scope

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

The following Dell EMC storage systems have been tested:

- Dell EMC Isilon®

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

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

- Airship-certified to install Airship DVR 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 Dell EMC solution

This chapter presents the following topics:

Design concepts

There are many design options for an Airship DVR implementation. Airship offers many documents and materials related to the design and implementation of Airship DVR. These design details are beyond the scope of this paper.

The Airship Hybrid DVR Server uses dedicated Airship H.264 hardware and processors for video/audio compression. In real time, up to 64 channels of analog video can be simultaneously captured, compressed, and recorded. The corresponding audio channels are captured, compressed, and recorded as well.

The Airship Hybrid DVR Server can also record and store video from TCP/IP network-based cameras. IP cameras that are added to an Airship Hybrid DVR Server are treated just like another camera. The Airship Hybrid DVR Client connects to the Airship Hybrid DVR Server and is represented as just another camera, which happens to be an IP camera.

Tests were conducted using virtual servers for Airship DVR. In the Dell EMC Surveillance Lab environment, four node Isilon clusters were used for testing.

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

Figure 1 Airship DVR architecture
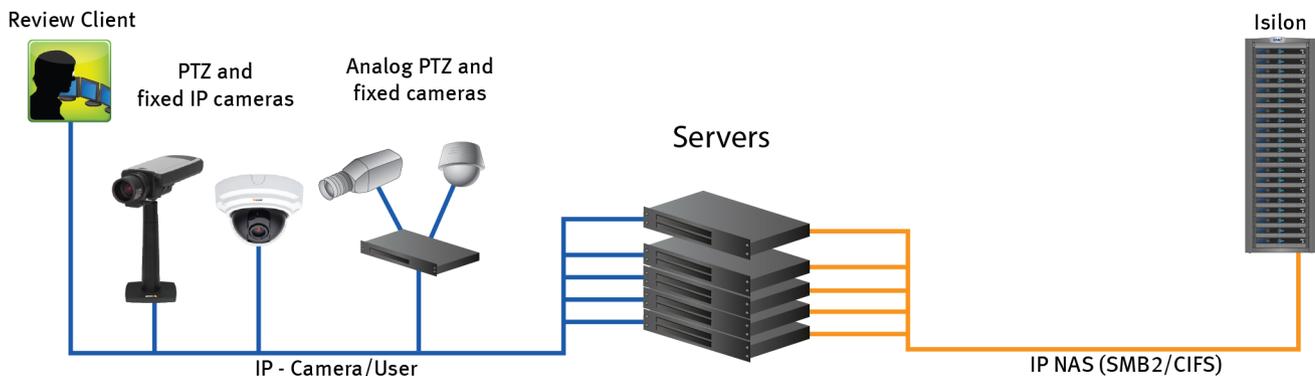
Dell EMC Surveillance Lab test environment

The Dell EMC Surveillance Lab is constantly being upgraded to the most recent software releases.

In order to test this solution, the Dell EMC Surveillance Lab was configured as follows:

Virtualized environment:

- 8 vCPUs

- 8 GB memory

- Network adapter type: VMXNET3 (10 GbE)

- Isolated VLAN for storage (if not FC)

Network environment:

- Network adapter type: 10 GbE

- Camera user VLAN

- Storage VLAN

For all the tests, the virtual CPU (vCPU), memory, and network were configured according to Airship best practices. The VMware vSphere configuration was in accordance with the VMware Compatibility Guide (www.vmware.com/resources/compatibility/search.php).

The Dell EMC Surveillance Lab's host hardware met and exceeded the minimum system requirements for an ESXi/ESX installation. The Airship Recorder VM was running on an ESXi 6.5 host using various Dell EMC servers, such as the Dell EMC FC630s, FC430s, R440, and R640. For more information about VM configuration, see the General recommendations for storage and sizing section of the *Using EMC VNX storage with VMware vSphere* guide.

Releases tested

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

Table 1 OneFS releases

Model	OneFS version
A2000	8.1.1.1

Table 2 Airship DVR releases

Release	Subrelease
Airship DVR	5.4.1.290

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.

Volume limits

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

While there are three directory-level quota systems, the Dell EMC Surveillance 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.

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

If necessary, both Isilon and the Airship 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.

Configuring SmartQuotas (recommended)

The SmartQuotas feature enables you to limit the storage that is used for each Airship 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 Airship DVR 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.

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 Airship 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 Airship 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.

SMB specific configuration

To avoid timeout issues add two timeouts on the Isilon cluster, *keepidle* and *keepintvl*.

The Dell EMC Surveillance Lab recommends setting *keepidle* to 61 seconds, with 1 minute being the minimum that can be assigned to this parameter, and *keepintvl* to 5 seconds. Using this configuration, the Airship DVR Recorders start writing to the share with a data loss interval of 1-2 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.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

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.

For surveillance implementations of any cluster size, the Dell EMC Surveillance Lab recommends optimizing the parameters on the cluster to remove the frame loss duration.

Procedure

1. Set the parameters 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 that 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 Airship DVR 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

Node Active / Passive
NIC Failover Proction

Node Active / Active
NIC Failover Proction
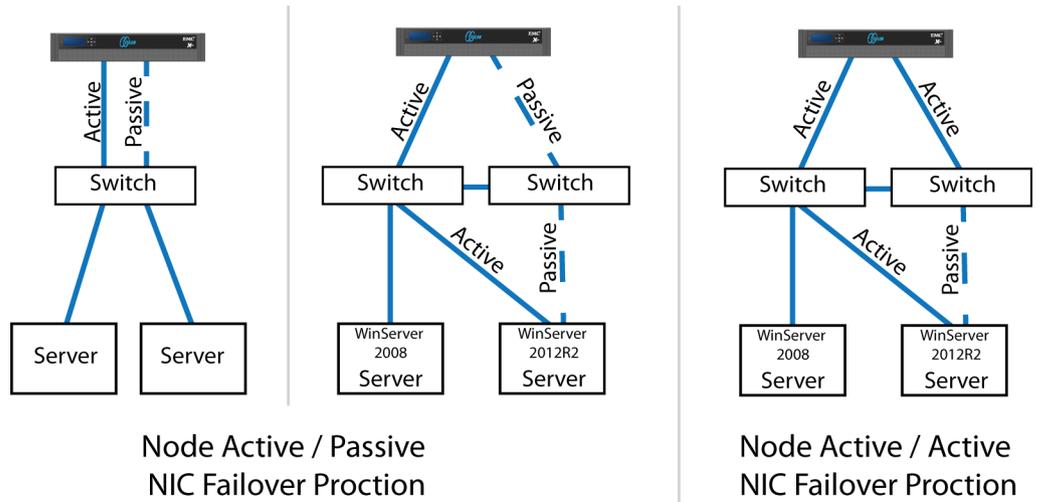
I/O optimization configuration

As of OneFS 7.0.x, no changes are necessary to the I/O profiles for the directories that are used for Airship.

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 Airship DVR server and the Isilon cluster are part of the same Windows domain.

Partial Active Directory

Where the Airship DVR servers are part of the Windows domain, but the Isilon cluster is administered locally.

Fully locally administered control

Where the Airship DVR 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 Airship 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 Airship DVR 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 Airship DVR 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.

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.

Job Engines and performance impact

During testing in the Dell EMC Surveillance Lab, we found certain job Engines that can impact the performance of the recorders.

FlexProtect and FlexProtectLin

The FlexProtect and FlexProtectLin job engines scan the file system after a device failure to ensure that all the files remain protected. FlexProtect is most efficient when used in clusters that contain only HDD drives. FlexProtectLin is most efficient when the file system metadata is stored on SSD drives.

InsightIQ®

InsightIQ takes large snapshots to provide better reporting on files that might need to be moved, which can cause performance issues in the cluster. For more information about disabling snapshots, refer to the Knowledge Base article How to enable or disable FSAnalyze from creating a snapshot.

FSanalyse

FSanalyse is a job Engine that collects File System Analytics for InsightIQ reporting. If you do not need this feature, use the following command to disable FSanalyse:

```
isi job types modify fsanalyze --enabled=no
```

Impact policies

There are three impact policies: low, medium, high. Avoid changing any of the impact policies if possible, but there are cases where changes are required. Use the following information for cases where a change must be made.

To list all Impact Policy parameters

```
isi_gconfig -t job-config impact profiles
```

To list only Medium Impact Policy parameters

```
isi_gconfig -t job-config impact.profiles.medium
```

To reduce the number of workers to 50 percent

Tuning should revolve around workers per core. If the workers per core is set to 1, then the maximum number of workers in a cluster equals the maximum number of cores. For example, if the medium impact policy default is 1 worker

per core, use the following command to reduce the maximum workers allowed by 50 percent:

```
isi_gconfig -t job-config impact profiles medium
workers_per_core=0.5
```

Sample Output:

```
CLuster# isi_gconfig -t job-config impact profiles medium
impact.profiles.medium.id (enum job_impact_id) = Medium
impact.profiles.medium.ionice (int) = 1
impact.profiles.medium.workers_per_core (float) = 0.5
impact.profiles.medium.min_workers_per_cluster (float) =
0.25
impact.profiles.medium.max_workers_per_storage_unit (float)
= 2
impact.profiles.medium.fixed_worker_count (float) = 0
impact.profiles.medium.max_node_load_factor (float) = 3
impact.profiles.medium.min_node_load_factor (float) = 2
impact.profiles.medium.disk_types.sata.type (enum
disk_type) = sata
impact.profiles.medium.disk_types.sata.enabled (bool) = true
impact.profiles.medium.disk_types.sata.max_client_load_kbps
(int) = 1024
```

SSD strategies

`Metadata read/write acceleration` writes file data to HDDs and all metadata mirrors to SSDs. This strategy accelerates metadata writes, in addition to reads, but requires about four to five times more SSD storage than metadata read acceleration. For the Isilon X410 and NL410, the Dell EMC Surveillance Lab recommends using two 1.6 TB SSDs if using metadata read/write mode.

Manually re-balancing recorders across nodes

After and activity that causes recorders for move between Isilon nodes, it is possible for the recorder to node ratio be become unbalanced. Using this procedure, a recorder may be moved from the existing node to another node in the cluster. To get the recorder to the desired node, it may take multiple iterations of the procedure.

Procedure

1. Delete the SMB sessions that allow it to reconnect to other nodes.

   Type the following commands:

   ```
   isi smb sessions list
   isi smb sessions delete -f <computer name>
   ```

Airship VMS recorder configuration

When using Airship VMS software with Dell EMC Isilon the following changes were made to achieve the optimum performance and utilization of the Isilon storage cluster and Virtual hardware.

Performance settings and buffers

Define the Performance settings and buffers for the Airship server to ensure that Airship VMS can handle the load of the performance tests under failure scenarios.

In the `C:\Program Files (x86)\Airship\Server` folder, change the following Airship VMS server configuration files:

setup.ini

- `MaxMemoryCache` - change the default value `200000000` (200MB) to `2000000000` (2GB)
- `DropFramesMemoryThreshold` - change the default value `125000000` to `1000000000` (1GB)
- `WriteBufferSize` - change the default value `262144` to `4194304`
- Add a line immediately under the `WriteBufferSize` line: `Threads=4`

watchdog.ini

In the `[Data Writer]` section, change the `Timeout` value from `30000` to `90000`

Logmanager.ini

In the `[DATAREAD]` section, change the `logLevel` value from `-1` to `1`

Watermarking

Airship VMS supports watermarking the recorded video surveillance data. Initial testing showed very high IOPs and CPU utilization on the Isilon cluster, which was caused by the watermarking process. Isilon performance improved in tests with watermarking disabled.

To disable watermarking, rename the `wmark.dll` file to `wmark.bck` in the path `C:\Program Files (x86)\Airship\Server`.

Video Indexing

Define the video indexing settings for the Airship recorders.

In the recorder configuration file `C:\Program Files (x86)\Airship\Server\setup.ini`, change the `OSDriveIndexing` value from `0` to `1`.

A value of `1` causes the Airship recorders to write the temporary index files on the OS drive instead of the recording storage, which enhances performance.

CHAPTER 3

Conclusion

This chapter presents the following topics:

Summary

Dell EMC performed comprehensive testing with Airship DVR against Dell EMC Isilon clusters. The Airship architecture and product suite allows extreme scaling, from a few cameras to up to tens of thousands of cameras, by using Dell EMC storage.

Airship DVR 5.4.1.290 deliver a complete, end-to-end IP video surveillance VMS, that captures, records, analyzes, investigates and visualizes thousands of IP cameras. With an open platform that supports ONVIF standards, Airship DVR integrates with new and existing edge devices, as well as security management and access control systems.

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 Airship DVR as a best practice.