

# Dell EMC Storage with the Avigilon Control Center System

## Safety & Security

November 2019

H15399.7

## Configuration 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 Avigilon Control Center.

Dell EMC Solutions

**Dell EMC**

Safety & Security Lab

**Validated**

**AVIGILON**

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

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 Technologies, Dell, EMC, 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](http://www.DellEMC.com)

# CONTENTS

<b>Chapter 1</b>	<b>Introduction</b>	<b>5</b>
	Purpose.....	6
	Scope.....	6
	Assumptions.....	6
 <b>Chapter 2</b>	 <b>Configuring the Dell EMC solution</b>	 <b>7</b>
	Design concepts.....	8
	Releases tested.....	8
	Isilon (NAS).....	9
	Data protection.....	9
	OneFS 8.1 job workers (required).....	10
	Impact policy and priority configuration.....	10
	Volume limits.....	10
	Large file system, small view (SmartQuotas).....	11
	Configuring SmartQuotas (recommended).....	11
	Unique share naming.....	12
	Configuring SmartConnect .....	12
	SMB specific configuration.....	13
	Link aggregation.....	15
	Configuring authentication and access control.....	15
	Specify an NTP time server.....	16
	Continuous Availability.....	17
	Job Engines and performance impact.....	17
	SSD strategies.....	18
	Client connections and Load Balancing.....	19
	Manually re-balancing recorders across nodes.....	19
	Network adapter configuration.....	19
 <b>Chapter 3</b>	 <b>Configuring the ACC Solution</b>	 <b>21</b>
	Configuring ACC.....	22
	Install the ACC Server.....	22
	Configure Storage.....	22
	(ACC 5 only) Map the network storage locations to a drive.....	23
	(ACC 5 only) Disable Automatic Service Starts.....	23
	(ACC 5 only) Configure Startup Tasks.....	23
	Configure Volumes.....	24
	Manually Configure Avigilon DB configuration files.....	25
	Configure the ACC Service.....	25
	Test the configuration.....	25
	Troubleshooting.....	26
	Problem: The network volume isn't visible in the admin panel.....	26
	ACC 5 Only Problem: The mounted drive isn't visible in the admin panel .....	26
	Problem: The ACC service doesn't start, could not locate the external drive.....	27
	Problem: The ACC 5 service doesn't start when the machine is rebooted.....	27
	Archiving.....	28
	Enabling Storage Management.....	28

	Enabling Continuous Archive.....	28
	Known Issues and Limitations.....	29
<b>Chapter 4</b>	<b>Conclusion</b>	<b>31</b>
	Summary.....	32
	Dell EMC Isilon scale-out storage.....	32
<b>Index</b>		<b>33</b>

# CHAPTER 1

## Introduction

This chapter presents the following topics:

- [Purpose](#)..... 6
- [Scope](#)..... 6
- [Assumptions](#)..... 6

## 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 Avigilon Control Center. This document is not a replacement for the Avigilon implementation guide nor is it a replacement for the *Dell EMC Storage with Avigilon Control Center: Sizing Guide*.


## Scope

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

The Dell EMC Isilon™ storage system has been tested.

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

Avigilon offers a server failover feature, which requires a hot-standby server with available storage, that was not included as part of the Avigilon Control Center validation testing. For more information about this feature, contact Avigilon.

 **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
- Avigilon-certified to install Avigilon Control Center services
- Proficient in installing and configuring Isilon storage solutions
- 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 Safety & Security 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:

• <a href="#">Design concepts</a> .....	8
• <a href="#">Releases tested</a> .....	8
• <a href="#">Isilon (NAS)</a> .....	9
• <a href="#">Continuous Availability</a> .....	17
• <a href="#">Job Engines and performance impact</a> .....	17
• <a href="#">SSD strategies</a> .....	18
• <a href="#">Client connections and Load Balancing</a> .....	19
• <a href="#">Network adapter configuration</a> .....	19

## Design concepts

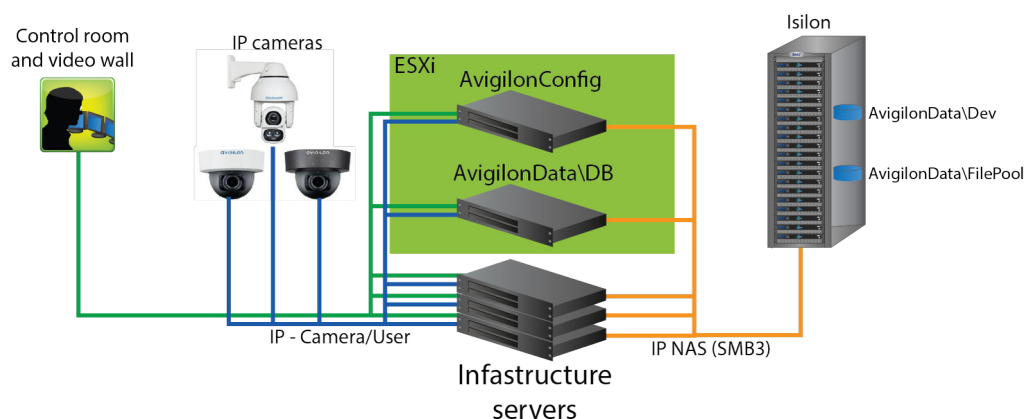
There are many design options for an Avigilon Control Center (ACC) implementation. Avigilon offers many training courses related to design and implementation. These design details are beyond the scope of this paper.

The *The Avigilon Control Center Server User Guide* provides the information that you need to plan an Avigilon Video Management Software (VMS) system and components.

This guide is intended for systems integrators and architects, network IT planners, and system administrators. This guide assumes that readers know what ACC VMS does and how it works, and know how to deploy and configure Windows IP networks. These documents are available from a Avigilon partner or through the Avigilon Partner Resource Center.

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

**Figure 1** Avigilon Control Center architecture



## Releases tested

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

### Note:

- Migrating from one EMC Isilon platform to another is not supported.
- Upgrading the ACC 5 system to the ACC 6 system requires the purchase of an ACC 6 license. Continue to use the ACC 5 configuration following the upgrade. Reconfiguration could result in data loss. Contact Avigilon Support to update the system to use UNC paths as recommended for ACC 6.

**Table 1** OneFS releases

Model	Firmware
NL410	8.0.0.2
HD400	8.0.0.2
X410	8.0.0.4, 8.0.1.2
H400	8.1.1.1



**Table 1** OneFS releases (continued)

Model	Firmware
A2000	8.1.2

**Table 2** Avigilon Control Center releases

Release	Subrelease
Avigilon Control Center 5	5.10.18.4
Avigilon Control Center 6	6.8.0
	6.10.0.24
	6.12
	6.14.8.26

## Isilon (NAS)

The Isilon scale-out network-attached storage (NAS) platform combines modular hardware with unified software to harness unstructured data. Powered by the distributed Isilon OneFS™ operating system, an Isilon cluster delivers a scalable pool of storage with a global namespace.

The platform's unified software provides centralized web-based and command-line administration to manage the following features:

- A symmetrical cluster that runs a distributed file system
- Scale-out nodes that add capacity and performance
- Storage options that manage files and tiering
- Flexible data protection and high availability
- Software modules that control costs and optimize resources

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

Before installing Dell EMC Isilon firmware updates for EMC, shut down your ACC service. The upgrade may take several hours. Prepare your maintenance schedule accordingly.

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

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

## Isilon protection with OneFS

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

## 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 Safety & Security Lab achieved optimum resilience when the number of job workers slowly increased their number per job phase.

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

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

## 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 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 Avigilon 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 Safety and Security Lab only uses the hard limit system during validation testing:

### Hard limit (recommended)

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

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

If necessary, both Isilon and the Avigilon 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 Avigilon Recorder. It presents a view of available storage that is based on the assigned quota to the Recorder. SmartQuotas enables each Recorder to calculate its available disk space and react appropriately.

### About this task

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 Management > SmartQuotas**.
2. For each listed share, select **View details**.
3. Under **Usage Limits**, select **Edit usage limits**.
4. Define the SmartQuotas limit and set the threshold:
  - a. Select **Specify Usage Limits**.
  - b. Select **Set a hard limit**.
  - c. Type the hard limit value.
  - d. Select the size qualifier, typically **TB**.
  - e. Select the size of the hard threshold.

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.

### About this task

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

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

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

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

SmartConnect balances connection loads to the Isilon cluster and handles connection failover. With SmartConnect, all Avigilon 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 Avigilon 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*.

**About this task**

The Dell EMC Safety and Security 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 ACC 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.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.keeppidle=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.bk01 /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.

### About this task

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 safety and security implementations of any cluster size, the Dell EMC Safety and Security Lab recommends optimizing the parameters on the cluster to remove the frame loss duration.

### 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 that the changes are logged in `sysctl.conf` file:

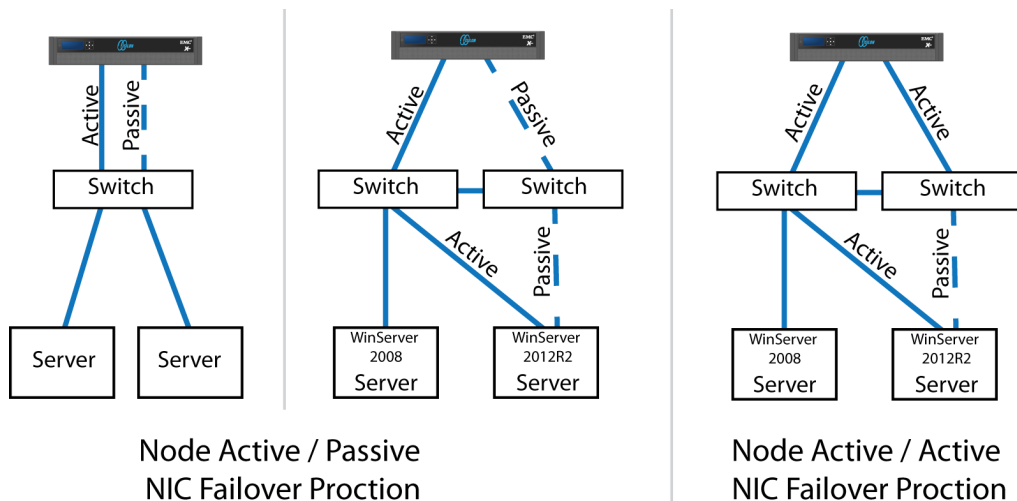
```
cat /etc/mcp/override/sysctl.conf
net.inet.tcp.keepidle=61000 #added by script
net.inet.tcp.keepintvl=5000 #added by script
kern.maxvnodes=10000 #added by script
kern.minvnodes=10000 #added by script
efs.lin.lock.initiator.lazy_queue_goal=10100 #added by script
efs.ref.initiator.lazy_queue_goal=10100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



## Configuring authentication and access control

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

### About this task

The following tests were conducted:

### Full Active Directory (recommended)

Where the Control Center server and the Isilon cluster are part of the same Windows domain.

### Partial Active Directory

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

### Fully locally administered control

Where the Control Center servers and the Isilon cluster are administered locally.

Alternatives to the previous methods might exist, but the Dell EMC Safety and Security 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 Avigilon and the Isilon cluster are not part of the same domain, use a local Isilon user to connect to the share. If the UNC share connection uses a local Isilon user, ensure that a local user with same username and password exists in the ACC Server on Windows. The ACC service must be configured to run under this account.
  - When the Isilon cluster and ACC server are part of the same domain, configure the Avigilon Control Center service to use the Domain account with read/write permissions to the Isilon cluster share. Specify the recording location for the ACC server using the full UNC path of the Isilon share .

## Specify an NTP time server

The Network Time Protocol (NTP) service is configurable manually, Dell EMC recommends that all nodes in a cluster and recorders are synchronized to the same time source. You can specify one or more servers to synchronize the system time on the Dell EMC Isilon cluster. The cluster periodically contacts the NTP servers and sets the date and time based on the information that it receives.

### About this task

For more information about configuring NTP with ESX, see Knowledge Base article [1003063](#), Guide to configure NTP on ESX servers.

### Procedure

1. Click **Cluster Management > General Settings > NTP**.
2. (Optional) In the **NTP Servers** area, enter the IPv4 or IPv6 address for one or more NTP servers. If you want to use a key file, enter the key numbers in the field next to the server's IP address.
3. (Optional) Click **Add Another NTP Server** if you are specifying multiple servers.
4. (Optional) If you are using a key file for the NTP server, enter the file path for that file in the **Path to Key File** field.
5. In the **Chimer Settings** area, specify the number of chimera nodes that contact NTP servers (the default is 3).
6. To exclude a node from chiming, enter its logical node number (LNN) in the **Nodes Excluded from Chiming** field.



7. Click **Save Changes**.

## 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.

CA describes when a node becomes inaccessible for any reason, such as administrative, failure, or infrastructure, then another node can be chosen to take its place and work can resume. CA is also known as "SMB Transparent Failover."

There are a couple of key features for this feature to work:

### Transparent Failover

The "Transparent Failover" capability of SMB3 allows the connection to the shares to be maintained despite the transition the node's role (planned, unplanned). This capability allows more seamless access to the video files during most failure scenarios. Because the failover activity is not instant, to cover the short period when the client is reconnecting and reopening its files on another node, sufficient or insufficient buffering determines the video frame loss.

### Witness service

Witness is service running on a second node that acts as the SMB connection witness monitoring the availability of the CA file shares. If there is a failover, the witness node has the responsibility to notify the SMB3 client that it should move its connection to a new node without waiting for TCP timeouts or DNS queries.

The Windows client starts the Witness connection. When the client makes the SMB connection to a node, the client also sends a Witness call (RPC) requesting a list of the cluster's IP addresses. The client picks the first address in the list marked as available for Witness registration. The client makes Witness calls to register for notification. There is no load-balancing algorithm because, at the moment, Witness is only providing status change notification.

When the CA-enabled share is available cluster-wide, the SMB connection moves from one node to another node seamlessly via a reconnection.

After a connection to a node fails with non-CA enabled shares, the operating system (OS) will quickly connect to a new node. Although the OS connection to the new node exists very quickly the SMB sessions are not available immediately. SMB maintains several timeout timers that must expire before the SMB session for the failed connection is made available.

To set up continuous availability, mark the CA box when creating the share. This selection causes a bit to be set in the supported configuration mask. If the client understands and supports the option, it just happens. It is important to remember you cannot add that setting after creating a share. There are tools to support re-creating the share with the CA setting enabled but they require disconnecting all the active clients during the process.

## Job Engines and performance impact

During testing in the Dell EMC Safety and Security 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](#).

**FSAnalyze**

FSAnalyze 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 FSAnalyze:

```
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 Safety and Security Lab recommends using two 1.6 TB SSDs if using metadata read/write mode.

## Client connections and Load Balancing

During a node or NIC failure, it is possible that of all the recorders in the failed node might reconnect to any other single available node. This connection issue is specific to CA enabled shares. If this connection issue occurs you can manually re-balance the cluster.

### Manually re-balancing recorders across nodes

After any activity that causes recorders to move between Isilon nodes, the recorder to node ratio can become unbalanced.

#### About this task

A recorder can be moved manually from the existing node to another node in the cluster to re-balance the node. You might have to perform the following procedure multiple times to get the recorder to the desired node.

When manually rebalancing a cluster, you can change the connection load balancing algorithm to Connection Count. When using Connection Count, use the `isi smb sessions` command to force the systems that you want to move. It is important to use a time interval greater than 1 minute between each forced server reconnection. Once the cluster is back in balance, change the connection load balancing algorithm back to Round Robin. Round Robin is the best algorithm for unattended reconnect scenarios.

#### Procedure

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

Enter the following commands:

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

## Network adapter configuration

When using the VMXNET3 driver on ESXi 4.x, 5.x or 6.x, there is significant packet loss during periods of very high traffic bursts.

#### About this task

To overcome this issue, the following network adapter configurations are recommended for virtual machine SVR servers.

#### Procedure

1. Click **Start > Control Panel > Device Manager**.
2. Right-click **vmxnet3** and click **Properties**.
3. Click the **Advanced** tab.
4. Click **Small Rx Buffers** and increase the value.

The default value is 512 and the maximum is 8192.

5. Click **Rx Ring #1 Size** and increase the value.

The default value is 1024 and the maximum is 4096.

6. Click **Tx Ring Size** and increase the value.

The default value is 1024 and the maximum is 4096.

# CHAPTER 3

## Configuring the ACC Solution

This chapter describes how to configure the ACC primary storage to record to a remote storage solution.

• <a href="#">Configuring ACC</a> .....	22
• <a href="#">Troubleshooting</a> .....	26
• <a href="#">Archiving</a> .....	28
• <a href="#">Known Issues and Limitations</a> .....	29

## Configuring ACC

The methods presented here allow ACC to write to any UNC network path supporting NTFS drive mounting. Contact the Dell EMC Safety and Security Lab team for support.

### About this task

Ensure you have the following:

- ACC Server Version 6.10.
- ACC Server Version 5.10.18.
- A remote storage solution that supports NTFS drive mapping and has the availability, durability, and performance guarantees of Direct Attached Storage (DAS).

**Note:** Upgrading the ACC 5 system to the ACC 6 system requires the purchase of an ACC 6 license. Continue to use the ACC 5 configuration following the upgrade. Reconfiguration could result in data loss. Contact Avigilon Support to update the system to use UNC paths as recommended for ACC 6.

## Install the ACC Server

### Procedure

1. Download and install the latest version of the ACC Server software.
2. Run through the installation wizard and click **Finish**.
3. When the ACC Admin Tool launches, click **Cancel** to exit the tool.

Do not configure storage or click **Next**.

## Configure Storage

### Procedure

1. Navigate to C:\Program Files\Avigilon\Avigilon Control Center Server\.
2. Open VmsDaemonConfig.cfg for editing and in the CmnSys/Storage namespace.
  - For ACC 5, Add **AllowRemoteVolumes** entry.

```
<CmnSys>
  <Network>
    <ConfigItem name="ServerBasePort" type="Boolean" value="true"/>
  </Network>
  <Storage>
    <ConfigItem name="AllowRemoteVolumes" type="Boolean"
value="true"/>
  </Storage>
</CmnSys>
```

- For ACC 6, Set **AllowNetworkVolumes** entry to true.

```
<CmnSys>
  <Network>
    <ConfigItem name="ServerBasePort" type="Integer" value="38880"/>
  </Network>
  <Storage>
    <ConfigItem name="AllowRemoteVolumes" type="Boolean"
value="true"/>
```

```
</Storage>
</CmnSys>
```

## (ACC 5 only) Map the network storage locations to a drive

Use the UNC path instead of an IP address for solutions that have multiple network ports and/or failover.

### Procedure

1. Open the windows command line **as an administrator** (right-click and choose 'run as administrator').
2. Use the net use command to temporally map the drive for ACC installation and setup.

For Example:

To map the network location `\\server\share` to the `Z:` drive under windows. Where `server` is the name or address of the storage server, `share` is the desired storage directory, `acc-storage-user` is a user with full access to that directory, and `TtC2WKkZGmEk9ug5Vs2z` is the user password determined by Isilon. The net use command to mount the drive under windows is:

```
>net use Z: \\server\share /user:acc-storage-user
TtC2WKkZGmEk9ug5Vs2z /persistent:yes
```

3. Launch the ACC Admin Tool.

The drive `Z:` should now show up as an available storage location.

## (ACC 5 only) Disable Automatic Service Starts

### Procedure


1. Navigate to `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup` and delete the Avigilon Control Center 5 Admin Tool shortcut.
2. Open the Windows Service Manager. Locate and right-click the Avigilon Control Center service to edit its properties.
3. In the **General** tab, set the Avigilon Control Center startup type to **Manual**.
4. Leave all other settings default.

## (ACC 5 only) Configure Startup Tasks

### Procedure

1. Open Windows Task Scheduler.
2. Under the **Actions** pane, click **Create Task....**
  - a. In the **Name** box, enter "ACC Startup Task" or an appropriate name.
  - b. To configure the task to run under the SYSTEM account, click **Change User or Group...** and enter SYSTEM as the object name.
3. In the **Triggers** tab:
  - a. Click **New....**
  - b. In the Begin the task drop-down list, select **At startup** and click **OK**.
4. In the **Actions** tab, click **New....**
  - a. In the **Action** drop-down list, select **Start a program**.

- b. In the **Program/script** box, enter `net`.
  - c. In the **Add arguments (optional)** box, enter: `use <mappedDriveLetter> <remoteStorageLocation> /user:<remoteStorageUsername> <remoteStoragePassword>`

 **Note:** The `remoteStoragePassword` is determined by Isilon.

For example: `use Z: \\server\share /user:acc-storage-user TtC2WKkZGmEk9ug5Vs2z`
  - d. Click **OK**.
5. Add a second action by clicking **New....**
  - a. In the **Action** drop-down list, select **Start a program**.
  - b. In the **Program/script** box, enter `net`.
  - c. In the **Add arguments (optional)** box, enter the following command to start the Avigilon Control Center service:
 

```
start "Avigilon Control Center"
```
  - d. Click **OK**.
6. In the **Conditions** tab:
  - a. In the **Power** section, clear the **Start the task only if the computer is on AC power** check box.
  - b. In the **Network** section, select the **Start only if the following network connection is available** check box and in the drop-down list, select the network connection that the share is mounted over.
7. In the **Settings** tab:
  - a. Select the **Run task as soon as possible after a scheduled start is missed** check box.
  - b. Select the **If the task fails, restart every:** check box and in the drop-down list, select **10 minutes** or your preferred time.
  - c. In the **Attempt to restart up to:** box, enter 3 times or your preferred setting.
  - d. Keep the default for all other settings.
8. Click **OK** to create the task.

## Configure Volumes

ACC network storage will only support volumes with paths at the share roots. Attempting to configure storage into subpaths of network shares is unsupported. For this reason, the admin panel will automatically truncate selected paths to the UNC root.

### About this task

For example, if the path `\\server\sharename\subfolder` is selected, it will be replaced with `\\server\sharename\`.

If you require multiple volumes on the same host, expose each volume under a different share name. For example, `\\server\volume1\` , `\\server\volume2`.

### Procedure

1. In the ACC Admin Tool, in the **Settings** tab, click **Storage**.
2. Click **Add Primary Volume** to create primary volume in drive `C:`.



3. Click **Change Volume Size**.

Specify 15 GB for the primary volume and your desired storage size for the secondary volume.

4. Add additional Volumes:

- **ACC 5:** Click **Add Secondary Volume** and your desired storage size for the secondary volume in drive Z:.
- **ACC 6:** Click **Add Network Volume** to create secondary volumes.

5. Click **OK**, then **Next** to initialize storage volumes.

**Note:** If the UNC share connection uses a local Isilon user, ensure that a local user with same username and password exists in the ACC Server on Windows. The ACC service must be configured to run under this user. It is important the same user is logged on to Windows when launching the Admin Tool to perform storage configuration changes.

## Manually Configure Avigilon DB configuration files

### Procedure

1. In the C:\ and Z:\ drives, open the `DataStore.avconfig` files and set the `TargetSize` of the primary storage `<VolumeConfig>` to 0.

```
<VolumeConfig>
<Desc>
    <Uuid>8a1d9ea6-91e4-4642-a9fb-8fb5c621a9d0</Uuid>
    <Path>C:/AvigilonData</Path>
    <MinimumFreeSpace>5368709</MinimumFreeSpace>
    <TargetSize>0</TargetSize>
```

2. Delete file pool directory in Db storage volume C:\AvigilonData\FilePool.
3. Restart the ACC Admin Tool.

## Configure the ACC Service

If you don't want the machine to enter a reboot loop when the network becomes unavailable:

### About this task

- In the Windows Service Manager, configure the ACC software to restart or stop on third-attempt rather than reboot the machine.

## Test the configuration

### Verify the configuration works

#### Procedure

1. Manually start the ACC Server from the Admin Panel and verify it runs.
2. Reboot the machine hosting the ACC Server service.
3. When the host machine starts up, do not log in.
4. From a separate physical PC, use the ACC Client to check if the ACC Server service is visible on the network and usable.

## Verify the configuration works when the network connection is temporally unavailable at startup

### Procedure

1. Unplug the network connection to the remote filesystem on the machine hosting the ACC server service.
2. Reboot the machine hosting the ACC Server service.
3. Wait 10 minutes.
4. Using a separate physical PC, use the ACC Client to check that the ACC Server service is not available on the network.
5. Reconnect the network cable to the physical machine hosting the ACC Server service.
6. Using a separate physical PC, use the ACC Client to check that the ACC Server service shows up on the network within 5 minutes of reconnecting the cable.

## Troubleshooting

### About this task

Ensure the following requirements are met or the volume may not appear in the Admin Panel, or the ACC service may fail to start:

- Total volume space is greater than 15 GB.
- Filesystem is NTFS.
- The user account assigned to the ACC Server has full access to root of the network path (eg. \\servername\sharename\).
- The user account from which the ACC administrative panel is launched has full access to the root of the network path (eg. \\servername\sharename\).
- The network path is accessible.

## Problem: The network volume isn't visible in the admin panel

### Procedure

1. Verify that the drive is not read-only.
2. Check that files and folders can be created and deleted to verify permissions.
3. Verify that the drive is larger than 1 GB in total size.

## ACC 5 Only Problem: The mounted drive isn't visible in the admin panel

Double check that you enabled remote storage in the VmsDaemonConfig.cfg in the directory that you are running the admin panel from.

### Procedure

1. Verify that the drive is mounted under the local administrator account:
  - Open the Cmd window using **Run as administrator** and type net use. If the drive does not appear, it is not visible to the local administrator account.
2. Verify that the drive is not read-only.
3. Check that files and folders can be created and deleted to verify permissions.

4. Verify that the drive is larger than 1 GB in total size.

## Problem: The ACC service doesn't start, could not locate the external drive

### About this task

```
2017-03-09 18:58:49 WARN : DataStoreManager::Impl_t::OpenHealDataStoreConfig_ : Attempting to heal primary volume config of data store.
2017-03-09 18:58:49 ERROR : DataStoreManager::Impl_t::OpenHealDataStoreConfig_ : Primary volume cannot be found because 'Z:/' does not exist
2017-03-09 18:58:49 ERROR : DataStoreManager::Impl_t::OpenHealDataStoreConfig_ : Failed to locate any Image Volumes on disk
2017-03-09 18:58:49 WARN : Stor::DataStoreManager::InitializeMaster : Could not initialize data store from path Z:/AvigilonData.
2017-03-09 18:58:49 ERROR : Stor::DataStoreManager::InitializeMaster : Failed to initialize data store from .avlocate Z:/AvigilonData
```

### If ACC 6 is running under a user account

Verify that the user-account under which the ACC server is running can create directories and files under the UNC directory.

#### Procedure

1. Launch the command prompt by right-clicking on the program and selecting **Run as a different user**.
2. Enter the username and password used by the ACC service account.
3. Test the ability to access the share using the command `mkdir \\serverName\shareName\testDirectory`.

### If ACC 6 is running under a built-in service account

#### Procedure

1. Download `psexec` from SysInternals and use it to launch a console running as the SYSTEM user using the command: `psexec -i -s cmd`.
2. Follow the `mkdir` verification steps for user accounts described previously.

### If ACC 5 is running

#### Procedure

1. Download `psexec` from SysInternals and use it to launch a console running as the SYSTEM user using the command: `psexec -i -s cmd`.
2. Test the use command from the Setup section, Map the network storage location to a drive.
3. Verify that the system user can create directories and files under the mapped directory.

## Problem: The ACC 5 service doesn't start when the machine is rebooted

#### Procedure

1. Check that the ACC 5 Setup task was completed without error using the history in the Task Scheduler
  - In the Task Category **Action Completed** the return code should be **0**. If the return code is not 0, the task has not executed correctly.
  - Return code **2** shown in the example below generally indicates that the network path to the share is incorrect, or the credentials are not correct.
2. If the task completed successfully, check the Windows Event Logs for errors. If the ACC service itself failed to start, check the ACC logs.

- Usually, the ACC service failing to start indicates that the configured storage location was not available. Check the storage configuration and drive mappings and ensure they match.

## Archiving

You can enable the Storage Management Continuous Archive feature to automatically archive video in hourly blocks during the configured time frame.

### Enabling Storage Management

To enable users to archive video from the ACC network video management server, you must enable the Storage Management feature in the Admin Tool and assign a location for the archived files.

#### About this task

Once Storage Management is enabled, you can archive video on demand. If you have an Enterprise Edition system, you can also set up the Storage Management Continuous Archive feature.

#### Procedure

1. In the Admin Tool, select **Settings > Storage Management**.
2. In the **Storage Management** dialog box, select the **Enable Storage Management** check box to enable the server to archive video files.
3. Enter a location for the Archive Folder: Click ... to browse to the preferred folder location.

**Note:** The archive folder can be on any Windows file system that is accessible by the server. Multiple servers can reference a common file system creating a centralized video archive.

4. Click **OK**.

### Enabling Continuous Archive

We recommend that you set up the Storage Management Continuous Archive feature to work with video data aging. By configuring the two features together, you can create a tiered storage configuration to help manage the amount of video retained on the local ACC Server. Review your video data aging settings in the Recording and Bandwidth dialog box, and set up the Storage Management Continuous Archive feature to begin archiving before data aging starts. This helps ensure that you always have high bandwidth quality video of important events, while the ACC Server continues to have space for new recordings.

#### About this task

**Note:** Ensure that the `Archive video older than:` parameter is set so that archiving to the archive directory starts and completes before data is deleted on the local ACC Server. Best practice is to set the `Archive video older than:` parameter to at least one day less than the value set for video data aging to account for retries if the network connection is restricted or degraded.

#### Procedure

- 1.

In the server Setup tab, click . The Storage Management dialog box is displayed.

**Note:**

- If you see an error message, the Storage Management feature must be enabled in the Avigilon Control Center Admin Tool or Edge Solution device web interface first. That is also where you select the preferred archive directory.
- If you are running the ACC Server software on a network video recorder, see *The Avigilon Control Center Server User Guide* for more information. If you are running an Edge Solution device, refer to the device user guide for more information.

2. Select the **Enable Continuous Archive** check box.
3. In the **Camera(s) to Archive:** list, select the device video to include in the archive.
4. In the **Options** area, define the following:

#### Archiving permitted

Specify the time frame when Continuous Archive is permitted.

If you want archiving operations to occur 24 hours each day, including retries, specify the time frame to be 00:00 to 23:59.


The time specified is in the server's local time. If you are physically located in a different time zone from the server, remember to consider the time difference.

#### Archive video older than

The minimum age of recorded video in days before it is archived.


Ensure the minimum age specified here is less than the age specified in the Recording and Bandwidth dialog box for deleting High Bandwidth video on the local ACC Server. A one day difference is sufficient to account for retries if the network connection is restricted or degraded.

For example, if the **Recording and Bandwidth** dialog box marks that the system will maintain 10 days of High Bandwidth video on the local ACC Server, enter 9 or less.

 **Note:** Recorded video remains in the site until it is removed by data aging.

#### Delete oldest archives when disk full

Check this box to automatically delete the oldest archive files when the archive storage location is full.

 **Note:** Disable this setting if your storage is managed by a disk system.

5. Click **OK**.

The Status area displays when the next archive will occur.

## Known Issues and Limitations

Issue	Workaround
The ACC service may not have time to completely stop before the network drive is unmounted during a windows shutdown resulting in write errors.	Manually shutdown the service using the Windows Service Manager or the ACC Admin Panel prior to any scheduled system restart.
ACC 6.6 fails to write certain file types in archive or to detect that disks are full if the host-name contains 'dot' elements. For example, a network share with a UNC path of the form: \\server.company.com\share-name\myarchive	Upgrade to ACC 6.10. Configure hosts file or archive target to use a host name without 'dot' elements.

Issue	Workaround
High processing load on Isilon when AVD files are overwritten.	<p data-bbox="727 254 1337 317">Disable ACC recycling of AVD files by adding the following entry to the <code>VmsDaemonConfig.cfg</code> file:</p> <pre data-bbox="743 359 1337 506">&lt;CmnSys&gt; &lt;Storage&gt; &lt;ConfigItem name="DisableFileRecycling"   type="Boolean" value="True"/&gt; &lt;/Storage&gt; &lt;/CmnSys&gt;</pre>

# CHAPTER 4

## Conclusion

This chapter presents the following topics:

- [Summary](#) ..... 32

## Summary

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

ACC is an easy to use video management software that delivers complete, end-to-end safety and security IP video that captures, records, analyzes, investigates, and visualizes. As a distributed network platform with enterprise-class reliability, the ACC system can efficiently capture, manage, and store high definition safety and security video while intelligently managing bandwidth and storage.

The Isilon clusters tested performed well with ACC. Contact the Dell EMC Safety and Security Lab team with any questions regarding recommended node types.

## 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 Avigilon Control Center as a best practice.