Dell EMC Storage with Qognify Cayuga

Surveillance

June 2019

H17653

Configuration Best Practices Guide

Abstract

This configuration guide aims to help Dell EMC field personnel understand the best practices for Dell EMC storage system offerings to simplify the implementation of Qognify Cayuga.

Dell EMC Solutions

Qognify

DELL EMC

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

CONTENTS

CHAPTER 1

Introduction

This chapter presents the following topics:

Solution overview

Qognify video management software (VMS) for video surveillance is scalable, provides sensor integration, and is standards-based for open integration. Qognify 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. 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 Qognify Cayuga implementation. This document is not a replacement for the Qognify implementation guide nor is the document a replacement for the Dell EMC sizing guides.

Qognify Cayuga 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 Qognify Cayuga design ensures resilience.

Scope

This guide is intended for internal Dell EMC personnel and qualified Dell EMC and Qognify partners. It provides configuration instructions for installing the Qognify Cayuga 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 Qognify Cayuga.

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
- Qognify-certified to install Qognify Cayuga 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:

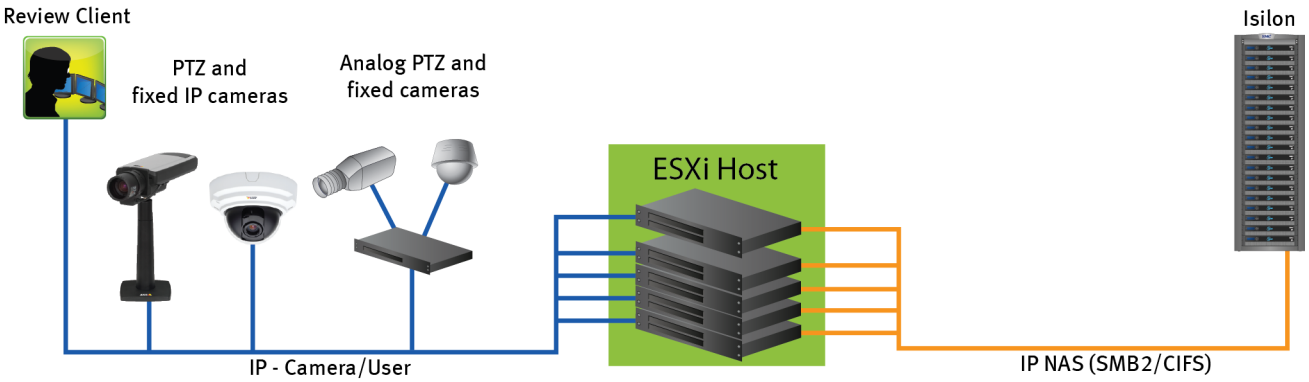
Design concepts

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

This guide is intended for systems integrators and architects, network IT planners, and system administrators. The guides assume that readers know what Qognify Cayuga does and how it works, and know how to deploy and configure Windows IP networks. This configuration guide is not intended to replace or supersede any Qognify document.

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

Figure 1 Qognify Cayuga architecture



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 Qognify Cayuga releases

Product	Release
Qognify Cayuga	R13

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.

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 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 Qognify 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 Qognify 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 Qognify Recorder. It presents a view of available storage that is based on the assigned quota to the Recorder. SmartQuotas enables each Recorder to calculate its available disk space and react appropriately.

About this task

To better cache the meta data associated with SmartQuotas, the Dell 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 Cayuga 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.

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.

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 Qognify 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 Qognify 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 Qognify.

Note: This setting does not require a SmartPool license.

Configuring authentication and access control

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

About this task

The following three tests were conducted:

Full Active Directory (recommended)

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

Partial Active Directory

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

Fully locally administered control

Where the Cayuga 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 Qognify 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 Cayuga 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 Cayuga 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.

About this task

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

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

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

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

About this task

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

Procedure

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

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

```
$COUNT
isi_sysctl_cluster efs.ref.initiator.lazy_queue_goal=$COUNT
isi_sysctl_cluster
efs.mds.block_lock.initiator.lazy_queue_goal=$MDS
isi_sysctl_cluster efs.bam.datalock.initiator.lazy_queue_goal=
$MDS
```

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

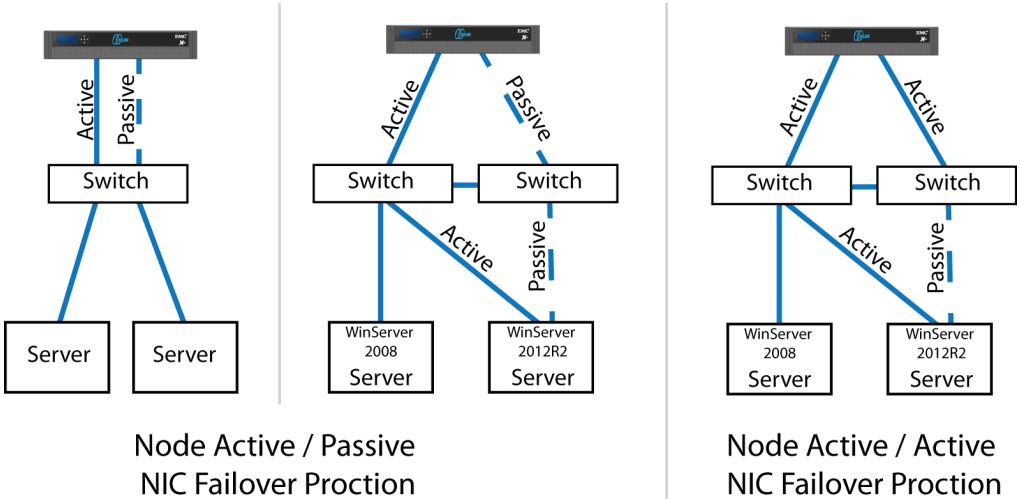
```
cat /etc/mcp/override/sysctl.conf
net.inet.tcp.keepidle=61000 #added by script
net.inet.tcp.keepintvl=5000 #added by script
kern.maxvnodes=10000 #added by script
kern.minvnodes=10000 #added by script
efs.lin.lock.initiator.lazy_queue_goal=10100 #added by script
efs.ref.initiator.lazy_queue_goal=10100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

Link aggregation

The active/passive configuration involves aggregating the NIC ports on the Isilon nodes for high availability. If one of the ports on the node or switch port fails, the Cayuga 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



CHAPTER 3

Conclusion

This chapter presents the following topics:

Summary

Dell EMC performed comprehensive testing with Qognify Cayuga against Dell EMC Isilon clusters. Depending on the implementation needs, you can use Dell EMC storage for Qognify Cayuga. The Qognify Cayuga 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 Qognify Cayuga as a best practice.