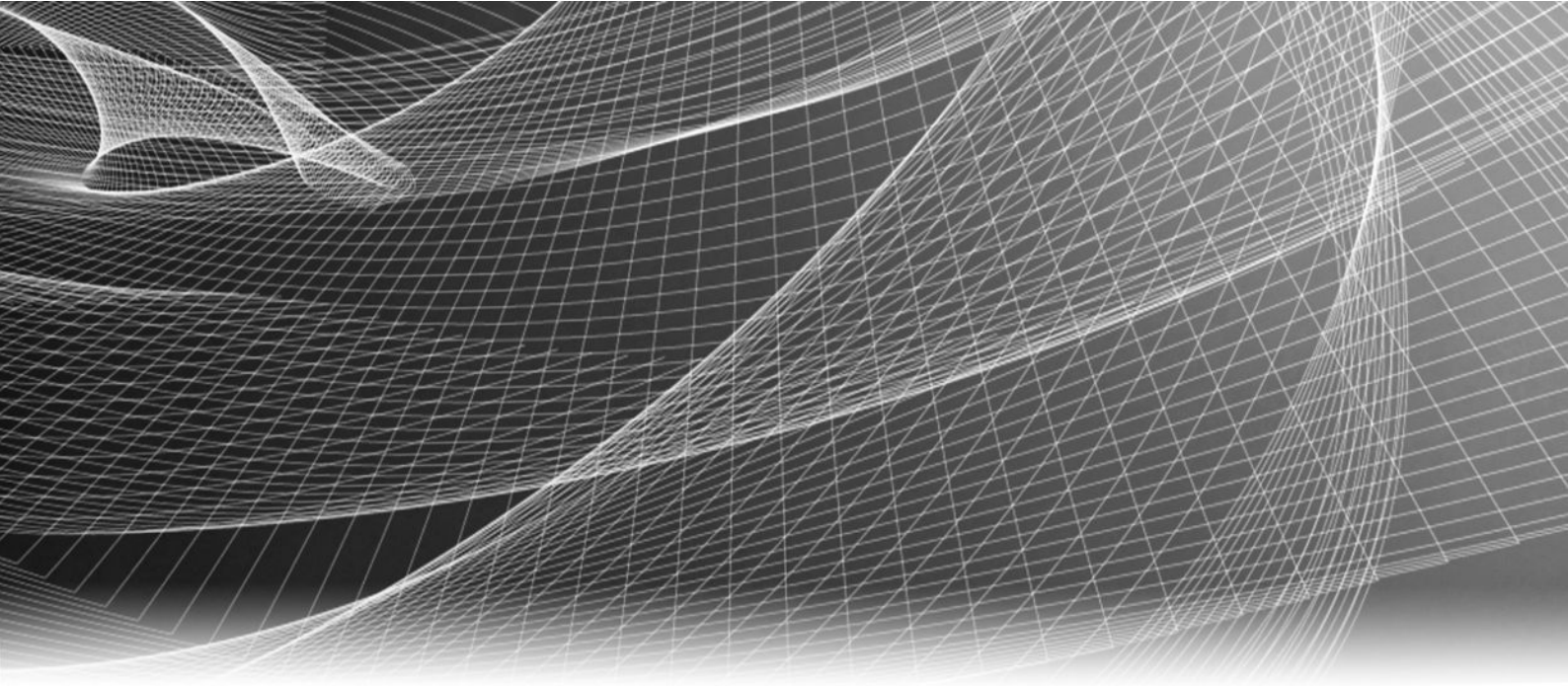


# Video Surveillance
# EMC Storage with Honeywell Digital Video Manager

## Configuration Guide

H14749

01

EMC² VS-LAB TESTED

Honeywell

EMC²

Published February, 2016



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

# CONTENTS

# CHAPTER 1

# Introduction

This chapter contains the following topics:

# Solution overview

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

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

# Scope

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

The following EMC Storage systems have been tested:

- EMC Isilon®
- EMC VNX®

This guide augments the standard *EMC VNX Storage with Video Management Systems: Configuration Guide* and *EMC Isilon Storage with Video Management Systems: Configuration Guide* and provides configuration information specific to Honeywell DVM.

# Assumptions

This solution assumes that internal EMC personnel and qualified EMC partners are using this guide with an established architecture based on the EMC Sizing Guide.

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

- Associated with product implementation
- Honeywell-certified to install Honeywell DVM services
- Proficient in installing and configuring EMC storage solutions
- Familiar with installing and configuring VMware hypervisors and Microsoft Windows operating systems

The configurations that are documented in this white paper are based on tests that were conducted in the EMC Physical Security lab, production implementations, or a combination of the two.

# CHAPTER 2

# Configuring the solution

This chapter contains the following topics:

# Design concepts

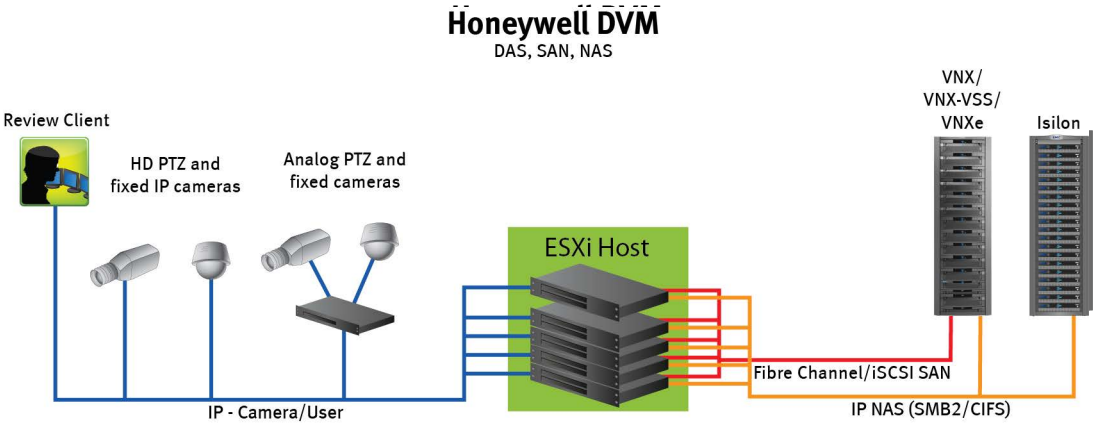
There are many design options for a Honeywell DVM implementation. These design details are beyond the scope of this paper.

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

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

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

**Figure 1** Honeywell DVM architecture




# EMC VNX

EMC VNX storage is ideal when you need to record and manage terabytes of video from distributed locations. This section describes best practices for configuring a VNX storage system for this solution.

The VNX family includes the VNX and VNX-VSS series arrays. The VNX series is designed for midtier to enterprise storage environments. The EMC VNX-VSS series is ideal for entry level and more highly distributed video surveillance environments in markets such as City Surveillance, Government, and Transportation.

## Disk drives

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

**Note**

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

## Storage pool configuration (recommended)

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

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

EMC recommends the following RAID configurations for VNX arrays:

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

### Procedure

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

## LUN configuration

A VNX pool LUN is similar to a classic LUN in many ways. Pool LUNs comprise a collection of slices and have the option to be thin or thick. A slice is a unit of capacity that is allocated from the private RAID groups to the pool LUN when it needs additional storage.

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

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

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

### Procedure

1. Right-click a storage pool and click **Create LUN**.
2. Type the user capacity for the LUN.
3. Type the starting **LUN ID**, and then select the number of LUNs to create.

   If the selected LUN ID is 50, and 3 is the selected number of LUNs to create, the LUNs' names would be 50, 51, and 52.
4. Select **Automatically assign LUN IDs as LUN names**.
5. Click **Apply**.

## iSCSI initiators

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

### Microsoft iSCSI initiators

For both physical servers and VMware ESXi server, the EMC surveillance lab uses Microsoft iSCSI initiators with excellent results.

### Hardware iSCSI initiators

Hardware iSCSI initiators might be used. There are many available on the market, results may vary. Hardware initiators may be used with varying results.

## Configure iSCSI front-end ports

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

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

For high availability:

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

### Procedure

1. Start Unisphere by typing the IP address of one of the storage system SP in an Internet browser that you are trying to manage.
2. Type your user name and password.
3. Click **Login**.
4. From Unisphere, select **System** › **Hardware** › **Storage Hardware**.
5. Identify the storage system iSCSI front-end ports by clicking **SPs** › **SP** *A/B* › **IO Modules** › **Slot** *[#]* › **Port** *[#]* in the **Hardware** window.

   The example used here is **SPs** › **SP A** › **IO Modules** › **Slot A4** › **Port 0**.
   The **Properties** message box appears.

6. Click **OK**.
7. Highlight the iSCSI front-end port that you want to configure and click **Properties**.
8. Click **Add** in **Virtual Port Properties** to assign IP address to the port. The **iSCSI Virtual Port Properties** window appears.
9. Click **OK** and the close all open dialog boxes

   A Warning message appears asking if you want to continue.
10. Click **OK**.

    A message showing successful completion appears.
11. Click **OK**.

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

## Connect the iSCSI target on Windows

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

### Procedure

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

      A **Connect to Target** window appears.
   f. Click **OK**.

      On successful connection, the status changes to Connected.

## Format the iSCSI target on Windows

After the iSCSI target has been successfully connected on Windows, the iSCSI target is displayed as an Unallocated Disk on Windows. You must set the disk to online and format it before you can start using it as a local disk to store video.

### Procedure

1. Right-click **Computer** and click **Manage**.

   The **Computer Management** page opens.
2. Click **Disk Management** to display current disk information.

   The iSCSI target is displayed on this page.
3. Right-click **iSCSI Disk** and click **Online** to activate the disk.
4. Right-click **iSCSI Disk** again and the **New Simple Volume Wizard** window appears.
5. Follow the wizard to complete formatting the disk.

   When complete, the disk appears as a local hard disk drive, which can then be utilized as extra storage space.

## Fibre Channel configuration

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

**Note**

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

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

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

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

Zoning has the following effects:

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

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

## VNXe RAID configuration

VNXe offers RAID 5, RAID 6, and RAID 10 configurations. Different configurations offer different types of protection against disk failures.

EMC recommends the following RAID configurations:

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

## Recommended cache configuration

With the VNX Gen2 systems, such as EMC VNX5200 or EMC VNX5400, the system manages the cache. If the array is shared with other applications, you can then use a lower write cache value, but avoid excessive forced flushes.

EMC recommends that you configure the cache as 90 percent write and 10 percent read if the storage array does not automatically adapt to the write characteristics of video surveillance (for example, EMC VNX5500 or EMC VNX-VSS100).

# EMC Isilon (NAS)

The EMC Isilon scale-out NAS storage platform combines modular hardware with unified software to harness unstructured data. Powered by the distributed 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, block data, and tiering
- Flexible data protection and high availability
- Software modules that control costs and optimize resources

## Data protection

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

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

The following best practices are based on a five-node minimum cluster size. You can use cluster sizes as small as a three-node cluster, but 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. 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.

## 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 is unless Isilon directs a change to one or more policies.

### Releases with OneFS 7.0 or greater

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 X200, Isilon X400, Isilon NL400, 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**. You can set the impact policy by selecting **Operations** › **Jobs and Impact Policies**.

**Priority configuration**

Even if the impact policy is modified, for example by modifying 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 and VNX block storage. Isilon can handle these large volumes because of the clustered file system that is used by OneFS.

## Large file system, small view (SmartQuotas)

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

There are three directory-level quota systems:

**Advisory limit**

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

**Soft limit**

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

**Hard limit (recommended)**

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

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

## Configuring SmartQuotas (recommended)

The SmartQuotas feature enables you to limit the storage that is used for each Honeywell Recorder and 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.

Without SmartQuotas, the DVM 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 are 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.

The SmartQuotas setup requires the following configuration 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 that is caused by overwriting or grooming (deleting) files prematurely, you must create a unique share for each Recorder.

## Configuring SmartConnect (optional)

SmartConnect uses the existing DNS Server and provides a layer of intelligence within the OneFS software application.

The resident Domain Name Service (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 either voluntarily or involuntarily surrendered its authority status. 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 DVM 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, Dynamic IP address (for NFS), and the following load balancing options (connection and rebalance policy):

**Round-robin (recommended)**

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

**Connection count**

Provides uniform distribution of the DVM 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. Select **Networking Configuration**.
2. Under **Subnet** › **Settings**, define the SmartConnect service IP (SSIP) address. The SSIP address is the IP address that the DNS uses for the Isilon Authoritative name service.
3. Under **Pool settings**:
   a. Define the SmartConnect zone name, which is the name to which clients connect.
   b. Define the SmartConnect service subnet (the subnet that has the SSIP configured on the DNS Server).
   c. Define the connection balancing policy to Connection Count or Network Throughput.
   d. Set the IP allocation strategy to **Static**.
4. Verify this configuration on the SmartConnect dashboard.

## I/O optimization configuration

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

**Note**

This setting does not require a SmartPool license.

## Configuring authentication and access control

Authentication and access control tests were conducted to determine the best method for share access.

The following three tests were conducted:

**Full Active Directory (recommended)**

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

**Partial Active Directory**

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

**Fully locally administered control**

Where the DVM servers and the Isilon cluster are administered locally.

Alternatives to the previous methods might exist, but the EMC Physical 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 the Isilon cluster and Honeywell are not part of the same domain, set the shares to **Run as Root**. This setting is not ideal from a security perspective.
   - When the Isilon cluster and DVM server are part of the same domain, configure the `DVM Camera` service to use the Domain account with read/write permissions to the Isilon Cluster share. During the initial installation of the Camera server, use the DVM administrator account specification wizard to configure the camera service. Specify the recording location for the camera server using the full UNC path of the Isilon share.

# Releases tested

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

**Table 1** Firmware builds

| Model | Firmware |
|---|---|
| VNXe1600 | VNXe 0E 3.1.3.5754151 |
| VNXe3200 | VNXe 0E 3.1.3.5754151 |
| VNXe3300 | VNXe 0E 2.1.0.14097 |
| VNX-VSS100 | VNX OE 5.32.000.5.215 |
| VNX5200 | VNX OE 5.33.008.5.119 |
| VNX5400 | VNX OE 5.33.000.5.015 |
| VNX5600 | VNX OE 5.33.000.5.052 |

**Table 1** Firmware builds (continued)

**Table 2** OneFS releases

| Model | Firmware |
|---|---|
| X410 | 7.2.1 |
| NL410 | 7.2.1 |
| HD400 | 7.2.1 |

**Table 3** Honeywell DVM releases

| Release | Subrelease |
|---|---|
| Honeywell DVM | 600.1 Build 1833 |

# CHAPTER 3

# Conclusion

This chapter contains the following topics:

# Summary

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

**VNX**

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

**EMC VNX-VSS100 arrays**

The VNX Video Surveillance Storage (VSS) is a storage solution that is purpose-built to meet the unique demands of the video surveillance environment. We found that this high availability, low-cost array performs comparably to other arrays in the VNX family.

**EMC VNXe arrays**

An iSCSI-connected VNXe array, implemented with storage pools, provides a cost-effective implementation while maintaining the expected performance. Many mid-sized deployments can use VNXe.

Low-bandwidth implementations can use a NAS-connected VNXe, but ideally NAS implementations should be based on EMC Isilon scale-out storage.

**EMC Isilon scale-out storage**

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

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