

Surveillance

Dell EMC Storage with Cisco Video Surveillance Manager

Configuration Guide

H14001

REV 1.1



Copyright © 2015-2017 Dell Inc. or its subsidiaries. All rights reserved.

Published May 2015

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

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

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

CONTENTS

| | | |
|------------------|---|-----------|
| Chapter 1 | Introduction | 5 |
| | Purpose..... | 6 |
| | Scope..... | 6 |
| | Assumptions..... | 6 |
| | | |
| Chapter 2 | Configuring the solution | 7 |
| | Design concepts and disclaimers..... | 8 |
| | EMC VNX..... | 8 |
| | Disk drives..... | 9 |
| | Storage pool configuration (recommended)..... | 9 |
| | LUN configuration..... | 10 |
| | Fibre Channel configuration..... | 10 |
| | VNXe RAID configuration..... | 11 |
| | VMware iSCSI initiator configuration..... | 11 |
| | Recommended cache configuration..... | 11 |
| | Releases tested..... | 11 |
| | Minimum requirements and recommendations..... | 12 |
| | VMware ESX/ESXi..... | 12 |
| | Recommended vCPU, memory, and network..... | 12 |
| | Storage adapter requirements..... | 12 |
| | | |
| Chapter 3 | Conclusion | 15 |
| | Summary..... | 16 |
| | EMC VNX arrays..... | 16 |

CONTENTS

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 Cisco VSM. This document is not a replacement for the Cisco implementation guide nor is it a replacement for the *Dell EMC Storage with Cisco VSM: Sizing Guide*.

Cisco Video Surveillance Manager (VSM) provides a comprehensive system for video surveillance. This system enables customer's network and security teams to collaborate effectively in a highly scalable environment combining both video and network techniques to optimize the experience. The Dell EMC storage system provides no single point of failure while the Surveillance VSM design ensures resilience.

Scope

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

The following Dell EMC storage systems have been tested:

- EMC VNX™
- EMC VNXe™

This guide supplements the standard *EMC VNX Storage Best Practices with Video Management Systems: Configuration Guide* and provides configuration information specific to Cisco VSM.

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
- Cisco-certified to install Cisco VSM services
- Proficient in installing and configuring VNX/VNXe 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 *EMC VNX Storage with Video Management Systems: Configuration Guide*

The configurations that are documented in this guide are based on tests that we conducted in the Dell EMC Surveillance Lab using worst-case scenarios to establish a performance baseline. Lab results might differ from individual production implementations.

CHAPTER 2

Configuring the solution

This chapter presents the following topics:

- [Design concepts and disclaimers](#).....8
- [EMC VNX](#).....8
- [Releases tested](#)..... 11
- [Minimum requirements and recommendations](#)..... 12

Design concepts and disclaimers

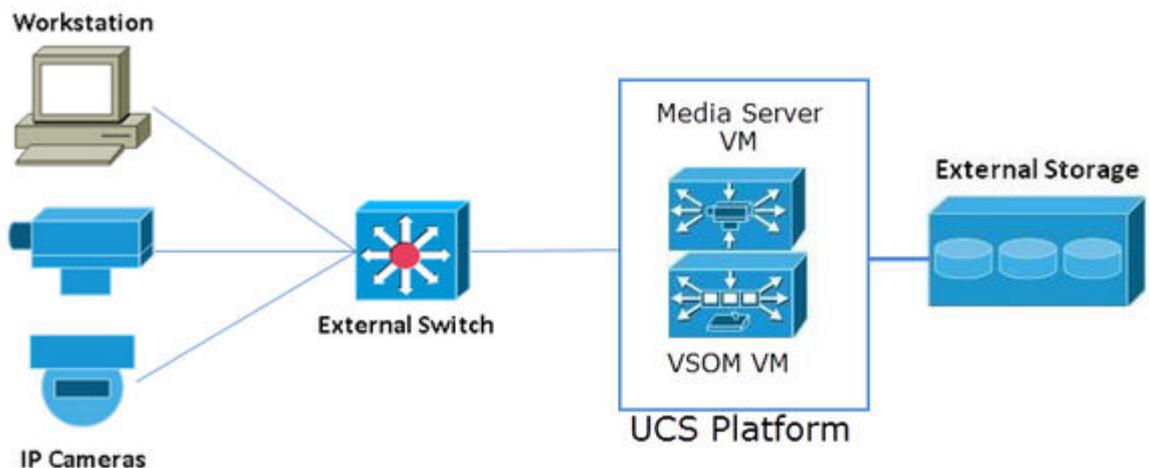
There are many design options for a Cisco VSM implementation. Cisco offers many documents and materials related to design and implementation of Cisco VSM. These design details are beyond the scope of this paper.

This paper describes how to deploy the Cisco VSM as a virtual machine (VM) on the Cisco Unified Computing System (UCS) platforms. The Dell EMC Surveillance Lab team worked with Cisco Engineering to set up and verify tests. We successfully tested the VSM write characteristics including bandwidth and camera count. Tests were based on 720p resolution camera streams. VSM media server and operations manager were hosted using SAN datastores.

Tests were conducted using VMware datastores for booting the Cisco virtual machines. In the Dell EMC Surveillance Lab environment, EMC VNX storage was used for testing.

The following figure illustrates the possible network configuration that can be deployed.

Figure 1 Cisco network configuration



The following video surveillance components comprise the network configuration:

- A UCS platform that runs the Cisco VSM virtual machine(s) that host the Media Server, the Operations Manager, or both.
- The Cisco VSM image (.ova file format) for the UCS platform.
- Various IP cameras, encoders, and analog cameras.
- The operator workstations that run the Operations Manager client.
- An external network switch and external storage.

EMC VNX

VNX storage is ideal for recording and managing terabytes of video from distributed locations. This section describes best practices for configuring a VNX or VNXe storage system for this solution.

The VNX family includes the VNX, VNXe, and VNX-VSS series arrays. The VNXe series is designed for small to midsize environments. The VNX series is designed for

mid-tier to enterprise storage environments, is ideal for distributed environments, and can scale to handle large petabyte (PB) environments with block-only requirements at central locations.

Disk drives

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

Note

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

Storage pool configuration (recommended)

Cisco recommends that each VSM media server have exclusive access to its own RAID array. For example, if you have a RAID 5 set of 10 drives with 3TB, then the entire ~25TB is provided as a single volume; the single volume appears to the Cisco VSM server as a single hard drive. Therefore, we recommend using a storage pool with a single RAID group for each VSM media server virtual machine, and create a single LUN for the pool with maximum available space.

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

Procedure

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

LUN configuration

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

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

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

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

Procedure

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

For example, if the selected LUN ID is 50, and the selected number of LUNs to create is 3, the names for the LUNs are 50, 51, and 52.

4. Select **Automatically assign LUN IDs as LUN names**.
5. Click **Apply**.

Fibre Channel configuration

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

Note

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

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

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

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

Zoning has the following effects:

- Reduces the number of targets and LUNs presented to a host
- Controls and isolates paths in a fabric
- Prevents non-ESXi systems from accessing a particular storage system and from possible virtual machine file system (VMFS) data loss

- Optionally, separates different environments, such as test and production environments

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

VNXe RAID configuration

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

Dell EMC recommends the following RAID configurations:

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

VMware iSCSI initiator configuration

We used VMware iSCSI software initiators in this solution as the Cisco VSM is designed for a virtualized environment.

The LUNs are mapped as a raw device to the Cisco VSM media server to configure as video storage.

Recommended cache configuration

EMC VNX generation 2 systems, such as VNX5200 or VNX5400, manage the cache. If the array is shared with other applications, you can use a lower write cache value, but avoid excessive forced flushes.

Dell 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).

Releases tested

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

Table 1 Firmware builds

| Model | Firmware |
|------------|-----------------------|
| VNXe3100 | VNXe OE 2.1.0.14097 |
| VNXe3150 | VNXe OE 2.4.0.20932 |
| VNXe3300 | VNXe OE 2.1.0.14097 |
| VNX5100 | VNX OE 5.31.000.5.006 |
| VNX5300 | VNX OE 5.31.000.5.006 |
| VNX-VSS100 | VNX OE 5.32.000.5.215 |
| VNX5400 | VNX OE 5.33.000.5.015 |
| VNX5500 | VNX OE 5.31.000.5.720 |

Minimum requirements and recommendations

Different Cisco VSM roles have different hardware specifications that include the processor speed and type, memory specification based on the processor, storage concerns, and Ethernet NICs.

Refer to the Cisco installation guide for the VMS version you are implementing for software and operating system requirements.

VMware ESX/ESXi

VMware vSphere minimum system requirements are as follows:

- VMware ESX/ESXi 5.0 or later
- Four-core 1.99 GHz processors or greater
- 12 GB of memory for each vSphere guest running a Cisco VSM server
- Dell EMC PowerPath™ for block storage (FC and iSCSI)

For a list of compatible hardware, refer to the [VMware Compatibility Guide](#).

Recommended vCPU, memory, and network

Our test environment had the following configuration:

- VMware ESXi 5.1 Update 1 or ESXi 5.5
- 20-core ESXi host at 2.2 GHz or greater
- 128 GB or greater memory per ESXi 5.1 host

Each virtualized Cisco VSM host featured:

- 8 virtual CPUs (vCPU)
- 12 GB memory
- Network adapter type: VMXNET3
- Private VLAN for storage if not FC
- Dedicated vNIC for storage

This recommended ESXi virtual machine configuration provides a full-time review of 10 to 20 percent of the archived video files.

Storage adapter requirements

All storage adapters must be VMware certified. If used, FC/iSCSI adapters must be VMware and Dell EMC certified.

The following table shows the requirements for each of the storage types.

Table 2 Storage requirements

| Storage type | Requirements |
|---------------|---|
| Datstore | DAS or SAN devices. A minimum of 80 GB for each virtual machine |
| Video storage | SAN devices with unpartitioned space (VMware RAW): |

Table 2 Storage requirements (continued)

| Storage type | Requirements |
|---------------------|---|
| | <ul style="list-style-type: none"><li data-bbox="805 331 986 359">• FC-attached<li data-bbox="805 375 1015 403">• iSCSI-attached |

CHAPTER 3

Conclusion

This chapter presents the following topics:

- [Summary](#) 16

Summary

We performed comprehensive testing with Cisco VSM on an EMC VNX array.

Depending on a customer's requirements, you can use EMC VNX storage systems with Cisco VSM for this solution. The Cisco VSM architecture and product suite enables scaling from a few cameras up to tens of thousands of cameras with this solution.

EMC VNX arrays

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.