Dell EMC Storage with FLIR Latitude

Surveillance

June 2019

H15106.3

Configuration Best Practices Guide

Abstract

This configuration guide aims to help Dell EMC field personnel understand how to configure Dell EMC storage system offerings to simplify the implementation of FLIR Latitude.

Dell EMC Solutions

Dell EMC
Surveillance Lab
Validated

◆FLIR®

DELLEMC

CONTENTS

Contents

CHAPTER 1

Introduction

This chapter presents the following topics:

Purpose

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

Scope

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

The following Dell EMC storage systems have been tested:

- Dell EMC Unity

This guide supplements the standard and provides configuration information specific to FLIR Latitude.

(i) **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
- FLIR-certified to install FLIR Latitude services
- Proficient in installing and configuring Unity 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 Block 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 solution

This chapter presents the following topics:

Design concepts

There are many design options for a FLIR Latitude implementation. FLIR offers many training courses related to design and implementation. These design details are beyond the scope of this paper.

The FLIR *8.0 Installation instructions and clarifications* document provides information that you need to plan a Latitude Video Management Software (VMS) system.

These guides are intended for systems integrators and architects, network IT planners, and system administrators. These guides assume that readers know what Latitude VMS does, how it works, and how to deploy and configure Windows IP networks. These documents are available from a FLIR partner or through the FLIR Partner network.

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

Figure 1 FLIR Latitude architecture
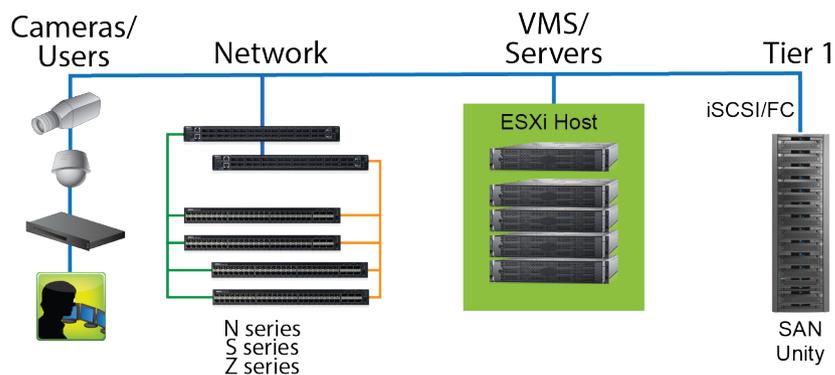
Releases tested

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

Table 1 SAN firmware builds

Model	Firmware
Unity 500	4.5.0.0.5.096

Table 2 FLIR Latitude releases

VMS	Release
FLIR Latitude	8.0.X.61XX

Dell EMC Unity

Dell EMC Unity storage arrays are ideal for recording and managing terabytes of video from distributed locations. This section describes best practices for configuring a Unity storage system for this solution.

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

For more information about configuring Unity storage arrays, see Dell EMC Block Storage with Video Management Systems Best Practices: Configuration Guide

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.

(i) 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)

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, Dell EMC recommends that you use storage pools rather than RAID groups. Storage pools also reduce the required array management tasks.

About this task

The Unity and SC series array architecture is optimized for storage pools. A storage pool is a construct that is built over one, or more commonly multiple, RAID groups. LUNs are built on top of the storage pool. The read/write activity is a random distribution across all disks defined to the storage pool. This distribution results in increased and balanced per disk utilization and improved performance when compared to traditional RAID implementations.

The RAID groups underlying storage pools can be either RAID 5 or RAID 6. RAID 5 is used for optimizing the array to achieve the maximum amount of storage and RAID 6 is used for enhancing data protection. Our tests using an isolated surveillance infrastructure did not reveal any notable performance variances when using RAID 5 as compared to RAID 6.

Building a storage pool is a straightforward process. You can configure either RAID 5 or RAID 6 pools depending on the 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.

Dell EMC recommends the following RAID configurations for SAN 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** 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 Unity or SC series 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.

About this task

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**.

iSCSI initiators

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

Microsoft Internet SCSI (iSCSI) initiators

For both physical servers and VMware ESXi server, the Dell EMC Surveillance Lab uses Microsoft iSCSI initiators with excellent results.

Hardware iSCSI initiators

Hardware iSCSI initiators can be used. There are many iSCSI initiators available on the market, and results might vary.

Configure iSCSI front-end ports

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

About this task

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 host bus adapter (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.

Add or edit iSCSI interfaces

When you log in to Unisphere for the first time, the **Initial Configuration Wizard** includes a step that enables you to add iSCSI interfaces.

To add or manage iSCSI interfaces later, under **Storage**, select **Block** > **iSCSI Interfaces**.

(i) Note: iSCSI interfaces can only be created on an Ethernet port that is not participating in a link aggregation.

Before you begin creating or updating an iSCSI interface, ensure that you have the following information:

- The Ethernet port that you will use for the iSCSI interface.
- For each Storage Processor (SP), the following address information:

  - IP address associated with the iSCSI interface. Although you can specify an IPv4 or IPv6-based address, ensure that you specify the same type of address for both SPs.

  - IP address mask or prefix length that identifies the subnet where the iSCSI interface resides.

- Gateway IP address associated with the iSCSI interface.
- Alias name associated with the IQN. The IQN and the IQN alias are associated with the port, and not the iSCSI interface. When you change the IQN alias for an iSCSI interface, the alias changes for all interfaces on that port.
- If applicable, the VLAN ID (1–4904) you want to associate the iSCSI interface with.

Connect the iSCSI target on Windows

When 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.

About this task

Connect the iSCSI target with the Windows iSCSI initiator.

Procedure

1. Launch the iSCSI initiator at **Control Panel** > **Tools** > **iSCSI initiator properties**.
2. Under the **Discovery** tab, click **Discover Portal**.
3. Enter the IP address or DNS name of the Storage iSCSI interface.
4. Click **OK** to save the configuration.
5. Under the **Targets** tab, select **Discovered targets**.
6. Click **Connect**.
7. In the **Connect to Target** window, select **Enable multi-path**.
8. Click **Advanced**.
9. Choose **Microsoft iSCSI initiator for Local adapter** from the dropdown list.
10. Choose the **Local Interface IP for Initiator IP** from the dropdown list.
11. Choose the **iSCSI interface IP of SAN** from the dropdown list.
12. Click **OK** to save the configuration.

    On successful connection, the status changes to Connected.
13. Repeat steps 2-7 for all discovered targets.

Format the iSCSI target on Windows

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

Procedure

1. Right-click **Computer** and then click **Manage**.
2. Click **Disk Management** to display current disk information.
3. Right-click **iSCSI Disk** and then click **Online** to activate the disk.
4. Right-click **iSCSI Disk** again to open the **New Simple Volume Wizard** window.
5. Follow the wizard to complete formatting the disk.

    When the wizard completes, the disk appears as a local hard disk drive, which can then be used 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.

(i) 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.

Dell EMC PowerPath

Dell EMC PowerPath is recommended for block storage (FC and iSCSI) implementations. PowerPath Multipathing automates data path management, failover and recovery, and optimizes load balancing to ensure application availability and performance.

FC LUN configuration for a virtualized environment

Fibre Channel LUNs can be configured using two methods for virtualized environments.

Raw device mappings (RDM)

RDM can be used for virtual machine archivers to store Video data. The RDM allows a virtual machine to access and use the storage device directly. The RDM contains metadata for managing and redirecting disk access to the physical device. The file gives you some of the advantages of direct access to a physical device while keeping some advantages of a virtual disk in VMFS. As a result, it merges VMFS manageability with raw device access.

FC datastores

ESXi uses datastores, which are logical containers that hide specifics of physical storage from virtual machines and provide a uniform model for storing virtual machine files. Datastores that you deploy on block storage devices use the vSphere VMFS format, a special high-performance file system format that is optimized for storing virtual machines.

Recommended cache configuration

Dell EMC Unity and SC series systems 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.

CHAPTER 3

Conclusion

This chapter presents the following topics:

Summary

Dell EMC performed comprehensive testing with FLIR Latitude using Dell EMC Unity arrays.

Depending on the implementation needs, you can use Dell EMC storage for FLIR Latitude. The FLIR Latitude architecture and product suite enables extreme scaling from a few cameras to tens of thousands of cameras using Dell EMC storage.

Dell EMC Unity arrays

The use of storage pools to create LUNs within the Dell EMC Unity 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.