VMware ESX Server Using EMC CLARiiON Storage Systems Solutions Guide
Version 1.0

- Connectivity of VMware ESX Server to CLARiiON Storage
- CLARiiON Virtual LUN Technology on VMware ESX Server
- Generating Restartable Copies with VMware ESX Server on CLARiiON Storage

EMC Engineering Solutions Guide

Sheetal Kochavara

www.emc.com
## Contents

Preface ........................................................................................................................................... xi  

### Chapter 1 Introduction to VMware

1.1 VMware infrastructure components ........................................................................1-3  
  1.1.1 VMware platforms ..................................................................................1-3  
  1.1.2 VMware Management .........................................................................1-4  
  1.1.3 VMware Tools ......................................................................................1-5  

1.2 VMware ESX Server .............................................................................................1-6  
  1.2.1 VMware ESX architecture .....................................................................1-6  
  1.2.2 VMware ESX Server virtualization layer ...........................................1-7  
  1.2.3 VMware ESX Server disk provisioning methods ................................1-7  

### Chapter 2 EMC Foundation Suites

2.1 EMC CLARiiON .................................................................................................2-3  

2.2 EMC CLARiiON management ............................................................................2-4  
  2.2.1 Navisphere Manager ...........................................................................2-4  
  2.2.2 Navisphere CLI ....................................................................................2-5  
  2.2.3 Navisphere host utilities .......................................................................2-6  
  2.2.4 Navisphere Analyzer ...........................................................................2-6  

2.3 CLARiiON virtual LUN technology ......................................................................2-6  
  2.3.1 CLARiiON metaLUNs ..........................................................................2-6  
  2.3.2 CLARiiON LUN migration ...................................................................2-8  

2.4 EMC SnapView ...................................................................................................2-9  
  2.4.1 SnapView clones ..................................................................................2-9  
  2.4.2 SnapView snapshots ...........................................................................2-11  

2.5 EMC SAN Copy ..................................................................................................2-13  
  2.5.1 Copying data between LUNs within a CLARiiON CX storage system...2-13  
  2.5.2 Copying data between CLARiiON, Symmetrix, and supported third-party storage systems ........................................................................2-14  
  2.5.3 Integration of EMC SnapView with SAN Copy ................................2-14  

2.6 EMC MirrorView ...............................................................................................2-15  
  2.6.1 MirrorView products ............................................................................2-15
Chapter 2 MirrorView and MirrorView/S Operations ........................................ 2-1
2.6.2 MirrorView terminology ......................................................................... 2-15
2.6.3 MirrorView/S operations ........................................................................... 2-17
2.6.4 MirrorView/A operations ........................................................................... 2-17
2.6.5 MirrorView consistency groups............................................................... 2-18
2.6.6 Integration of EMC SnapView and EMC SAN Copy with MirrorView. 2-18

Chapter 3 Connectivity of VMware ESX Server to a CLARiiON Storage System ............... 3-1
3.1 Booting ESX Server from CLARiiON............................................................. 3-2
3.2 Booting guest operating systems on CLARiiON ........................................... 3-2
3.2.1 Presenting LUNs to virtual machines ....................................................... 3-2
3.2.2 Integration of Navisphere host utilities with VMware ESX Server............ 3-2
3.3 High availability when using VMware ESX Server with CLARiiON.............. 3-3
3.3.1 Multipathing and failover functionality in VMware ESX Server.............. 3-3
3.3.2 Configuring CLARiiON storage with VMware failover software ............ 3-4
3.4 Optimizing CLARiiON LUN layout with VMware ESX Server.................... 3-6

Chapter 4 CLARiiON Virtual LUN Technology on VMware ESX Server ................................ 4-1
4.1 Introduction .................................................................................................. 4-2
4.2 Expanding LUNs used as raw device mapping (RDM)................................. 4-2
4.2.1 Guest OS considerations ......................................................................... 4-2
4.3 Expanding VMFS volumes ........................................................................... 4-3
4.4 Migrating VMFS and raw device mapping volumes ..................................... 4-4

Chapter 5 VMware ESX Server and EMC SnapView ................................................. 5-1
5.1 Introduction .................................................................................................. 5-2
5.2 Configuring SnapView with VMware ESX Server ........................................ 5-2
5.2.1 Replicating VMFS volumes using SnapView (clones and snapshots) ........ 5-2
5.2.2 Replicating RDM volumes using SnapView (clones and snapshots) ........ 5-3
5.2.3 Installing and configuring admsnap on virtual machines ....................... 5-3
5.3 Using SnapView with VMware ESX Server ................................................... 5-4
5.3.1 Implementing SnapView within a single VMware ESX Server............... 5-4
5.3.2 Implementing SnapView with two or more VMware ESX Servers ......... 5-5
5.3.3 Implementing SnapView to test application data replicas of native (physical) servers on virtual machines ....................................................... 5-6
5.3.4 Implementing SnapView to back up virtual machine data to a native (physical) server ................................................................. 5-7

Chapter 6 VMware ESX Server with EMC SAN Copy .............................................. 6-1
6.1 Introduction .................................................................................................. 6-2
6.2 Configuring SAN Copy with VMware ESX Server ....................................... 6-2
6.2.1 Replicating VMFS volumes using SAN Copy ........................................ 6-2
6.2.2 Replicating RDM volumes using SAN Copy ........................................ 6-2
6.2.3 Installing and configuring admhost on Windows virtual machines ........ 6-3
6.3 Using SAN Copy with VMware ESX Server ................................................... 6-3
6.3.1 Implementing SAN Copy to transfer data from one CLARiiON array to another using a single VMware ESX Server. ........................................ 6-3
6.3.2 Implementing SAN Copy to transfer data from one CLARiiON array to another using two VMware ESX Servers ................................................................. 6-4
6.3.3 Migrating physical servers to virtual servers from a third-party storage system to a CLARiiON array using SAN Copy .............................................. 6-5

Chapter 7 VMware ESX Server and EMC MirrorView ......................................................... 7-1
7.1 Introduction ............................................................................................................. 7-2
7.2 Configuring MirrorView with VMware ESX Server ............................................. 7-2
  7.2.1 Replicating VMFS volumes using MirrorView (Synchronous and Asynchronous).............................................................................................. 7-2
  7.2.2 Replicating RDM volumes using MirrorView (Synchronous and Asynchronous).............................................................................................. 7-3
7.3 Using MirrorView with VMware ESX Server ..................................................... 7-3
  7.3.1 MirrorView from a physical-to-virtual infrastructure .................................... 7-3
  7.3.2 MirrorView virtual-to-virtual infrastructure.................................................... 7-4

Appendix A References ............................................................................................... A-1
A.1 EMC references ................................................................................................... A-2
A.1 VMware references .............................................................................................. A-2
Figure 1-1  Representation of virtual infrastructure ...............................................................1-3
Figure 1-2  VMware ESX Server architecture ........................................................................1-6
Figure 2-1  MetaLUN expansion using striping method .......................................................2-7
Figure 2-2  MetaLUN expansion using concatenation method .............................................2-8
Table 2-1  Defining SnapView snapshot .............................................................................2-11
Figure 3-1  Dynamically scanning LUNs using the Rescan SAN option ..........................3-3
Figure 3-2  VMware ESX Server path information using CLI ...........................................3-4
Figure 3-3  VMware ESX Server path information using MUI ........................................3-5
Figure 5-1  Using SnapView on the same ESX Server ......................................................5-5
Figure 5-2  Using SnapView with two ESX Servers ............................................................5-6
Figure 5-3  Using SnapView on physical (native) server volumes to test replicas on a VMware ESX Server .................................................................5-7
Figure 5-4  Using SnapView on VMware ESX server volumes to backup replicas to a physical (native) server .................................................................5-7
Figure 6-1  Using SAN Copy to migrate data between two CLARiiON arrays using a single ESX Server .................................................................6-4
Figure 6-2  Using SAN Copy to migrate data between two CLARiiON arrays using two ESX Servers .................................................................6-5
Figure 6-3  Using SAN Copy to migrate data from a third-party storage system connected to native servers onto a CLARiiON array connected to ESX Servers ..........6-6
Figure 7-1  Using MirrorView for business continuity solution by transforming physical to virtual infrastructure .................................................................7-4
Figure 7-2  Using MirrorView to replicate virtual infrastructure environment ...............7-5
Table 2-1  Defining SnapView snapshot........................................................................2-11
This solution guide describes how the VMware ESX Server works with EMC CLARiiON storage systems and software technologies. This document focuses on the integration of VMware ESX Server with CLARiiON disk arrays, SnapView, MirrorView, and SAN Copy.

As part of an effort to improve and enhance the performance and capabilities of its product line, EMC from time to time releases revisions of its hardware and software. Therefore, some functions described in this guide may not be supported by all revisions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

Audience

The intended audience for this solution guide is storage administrators, system administrators, and VMware ESX Server administrators. This document can also be used by individuals who are involved in acquiring, managing, or operating EMC CLARiiON storage arrays and host devices.

Readers of this guide are expected to be familiar with:

- EMC CLARiiON system operation.
- SnapView, MirrorView, SAN Copy, and Navisphere Manager and/or CLI.
- VMware ESX Server operation.

Organization

The solution guide is divided into the following chapters:

Chapter 1, Introduction to VMware—This chapter introduces the reader to VMware and its technologies. VMware ESX Server technology is also discussed in this chapter.

Chapter 2, EMC Foundation Suites—EMC hardware and software technologies that enhance VMware ESX Server are discussed.

Chapter 3, Connectivity of VMware ESX Server to a CLARiiON Storage System—setup, and configuration of VMware ESX Server with EMC CLARiiON arrays are the
topics covered. This chapter also presents best practices when using EMC CLARiiON storage with VMware ESX Servers.

Chapter 4, CLARiiON Virtual LUN Technology on VMware ESX Server—This chapter discusses how CLARiiON metaLUNs and LUN migration can be used with VMware ESX Server.

Chapter 5, VMware ESX Server and EMC SnapView—This chapter discusses how SnapView Snapshots and SnapView clones (BCVs) can be used with VMware ESX Server to create point-in-time replicas.

Chapter 6, VMware ESX Server with EMC SAN Copy—Configuration, setup, and use cases of implementing SAN Copy with VMware ESX Server are discussed in this chapter.

Chapter 7, VMware ESX Server and EMC MirrorView—MirrorView when used in conjunction with VMware ESX Server can provide a powerful methodology for business restart processing on x86 platforms. This chapter discusses how MirrorView can be leveraged with VMware ESX Server to provide this functionality.

Appendix A provides references to other documents for additional details.

Examples provided in this document cover methods for performing various VMware ESX Server functions using CLARiiON systems with EMC software. These examples were developed for laboratory testing and may need tailoring to suit other operational environments. Any procedures outlined in this document should be thoroughly tested before implementing in a production environment.
This chapter presents these topics:

1.1 VMware infrastructure components ................................................................. 1-3
1.2 VMware ESX Server .......................................................................................... 1-6
Most organizations face three key challenges related to information management—growth of digital information, increased dependence on digital information, and changing value of digital information. Driven by growth in digitization of content, the amount of information continues to grow exponentially. Furthermore, highly effective organizations depend on the same information to automate and create efficiencies in business processing. The cyclic nature of business results in the challenge of addressing the changing value of information. To help customers with this challenge, EMC® introduced the concept of Information Lifecycle Management (ILM). ILM is not a product or a service in and of itself but a strategy. A successful ILM strategy is:

♦ Business-centric – Ties in closely with business’ key processes, applications, and initiatives.

♦ Centrally managed – Provides an integrated view into all the business’ information assets.

♦ Policy-based – Anchors in enterprise-wide information-management policies that span all processes, applications, and resources.

♦ Heterogeneous – Encompasses all types of platforms and operating systems.

♦ Aligned with the value of data – Assesses how valuable each type and unit of data is to the business at any given moment, matching it with the correct level of storage resources.

ILM enables organizations to plan for IT growth in alignment with business needs. It enables organizations to dynamically manage corporate information and resources according to its changing value over time.

VMware, Inc. was founded in 1998 to bring mainframe-class virtual machine technology to x86 processor-based workstations and servers. Server virtualization is the foundation of VMware’s core vision that transforms IT resources into a flexible, cost-effective pool of computers, storage, and networking resources. This pool of resources—called the virtual infrastructure—can be mapped to specific business needs. Figure 1-1 on page 1-3 shows the virtual infrastructure. In addition, the management tools provided by VMware allow resources to be changed dynamically as business requirements evolve. This capability allows VMware technologies to complement EMC’s overall vision of ILM.

This solution guide provides a general description of VMware technology as it relates to EMC CLARiiON® hardware and software products. EMC CLARiiON storage systems and software products enhance VMware functionality by providing technology to efficiently grow, clone, and/or remotely replicate virtual environments. Further information on VMware and its technologies can be found at http://www.vmware.com.
1.1 VMware infrastructure components

VMware offers a suite of products that support enterprise-class virtual infrastructure. These products enable server virtualization, migration to virtual infrastructure, and management of the virtualized environment. The product offerings can be broadly categorized into three components: platforms, management, and tools.

![Figure 1-1 Representation of virtual infrastructure](image)

1.1.1 VMware platforms

VMware platforms enable partitioning and resource management for optimal utilization and availability of the compute environment. In addition, these platforms—by virtualizing the compute environment—provide hardware independence.

These products virtualize x86-based computers and are the building blocks for VMware virtual infrastructure. Five different products are part of the platforms offered by VMware: VMware ESX Server, VMware Virtual SMP, VMware GSX Server, VMware Workstation, and VMware ACE. These products provide different virtualization solutions to meet diverse business needs.

- **VMware ESX Server** is a virtual infrastructure platform for enterprise data centers. ESX Server speeds business-solution deployments and adds management flexibility by partitioning x86 servers into a pool of secure, portable, and hardware-
independent virtual machines. Increased server utilization and simpler system administration enable customers to minimize total cost of ownership. ESX Server uses a unique architecture that inserts a small and highly robust virtualization layer between the x86 server hardware and the virtual machines. This approach gives ESX Server complete control over the server resources allocated to each virtual machine. In addition, performance overhead, availability concerns, and costs of server virtualization architectures built on a host operating system are avoided.

♦ **VMware Virtual SMP** is an add-on module to VMware ESX Server that makes it possible for a single virtual machine to span multiple physical processors. This enables scaling of the virtual infrastructure to handle the most resource-intensive applications.

♦ **VMware GSX Server** runs as an application within the Microsoft Windows or Linux operating system. Like the ESX Server, GSX Server transforms the physical computer into a pool of virtual machines. Operating systems and applications are isolated in multiple virtual machines that reside on a single piece of hardware. System resources are allocated to any virtual machine based on need, delivering maximum capacity utilization and control over computing infrastructure. Since the VMware GSX Server runs on top of a fully functional operating system, it provides much broader hardware support inherited from the host operating system.

♦ **VMware Workstation** is powerful desktop virtualization software primarily targeted for software developers and testers. VMware Workstation can be used to streamline software development, testing and deployment. VMware Workstation allows users to run multiple x86-based operating systems simultaneously on a single personal computer in fully networked and portable virtual machines.

♦ **VMware ACE** is an enterprise solution for IT desktop managers who want to provision secure, standardized PC environments throughout the extended enterprise. VMware ACE installs easily and improves the manageability, security, and cost effectiveness of any industry-standard personal computer. VMware ACE enables IT desktop managers to apply enterprise IT policies to virtual machines using Virtual Rights Management technology. The virtual machines containing an operating system, enterprise applications, and data create an isolated PC environment known as an assured computing environment (ACE). The Virtual Rights Management technology enables IT desktop managers to control ACE expiration, secure enterprise information on PCs, and ensure compliance with IT policies.

### 1.1.2 VMware Management

VMware Management products provide centralized management of the virtual infrastructure. Two products, VMware VirtualCenter and VMotion, constitute the management component of the virtual infrastructure.

♦ **VMware VirtualCenter** is enterprise-class software that provides a central point of control for enterprise-wide virtual infrastructure. It simplifies IT so companies leverage their storage, network, and computing resources to control costs and respond faster. VMware VirtualCenter can manage hundreds of physical x86-based servers from a central location, and allows instant provisioning to increase operational productivity.
♦ *VMotion* technology enables intelligent workload management. As mentioned previously, since VMware ESX Server runs directly on the physical hardware, it provides a level of control that is not available for other virtualization techniques. This control enables technology such as VMotion, which allows dynamic changes without impacting users. With VMotion, it is possible to migrate running virtual machines from one ESX Server to another server connected to the same information store. This allows rapid reconfiguration and optimization of resources across the virtual infrastructure to meet service-level requirements.

### 1.1.3 VMware Tools

VMware Tools are the integration toolkits for the virtual infrastructure. A key part of implementing a virtual infrastructure is virtualizing the existing server environment and plugging it into the current management software. VMware Tools enable quick integration of VMware Management and Platform software into an existing environment. VMware Tools consists of VMware P2V Assistant and VMware Developer Resources.

♦ *anonymous* is an enterprise-class migration tool that captures an existing physical system and moves it into a VMware virtual machine. VMware P2V Assistant helps reduce the complexity, risk, and downtime typically associated with migrating systems to the VMware virtual machine platform.

♦ *VMware Developer Resources* provides the developer community with industry-standard scripting interfaces, APIs, and SDKs to the Platform and Management products. The scripting API consists of two components: VmCOM and VmPerl. VmCOM is a Component Object Model (COM) interface for languages such as Microsoft Visual Basic, Microsoft Visual C++, and Jscript. VmPerl is an application programming interface (API) that uses Perl scripting language. The VMware SDK, on the other hand, provides the tools to develop client applications that can connect to the VMware VirtualCenter Web Service.
1.2 VMware ESX Server

VMware ESX Server consists of a base operating system that installs on hardware and provides a virtual infrastructure used for partitioning, consolidating, and managing systems in mission-critical environments. VMware ESX Server and VMware Virtual Infrastructure Nodes (VINs) provide a highly scalable virtual machine platform with advanced resource management capabilities that can be managed by VMware VirtualCenter. VMware ESX Server, Virtual SMP, VMware Virtual Center, and VMotion are anticipated to be deployed in large enterprise SANs. EMC CLARiiON technology provides the storage and storage-system-based functionality for these environments. This solution guide therefore focuses on how VMware uses CLARiiON capabilities.

1.2.1 VMware ESX architecture

The three key elements to the VMware ESX architecture are:

- The hardware interface component, which enables hardware-specific service delivery while hiding the differences from the virtualization layer and the resource manager.

- The virtualization layer, which provides the idealized hardware environment and virtualization of underlying physical resources that are presented to the virtual machines.

- The resource manager, which is responsible for partitioning and meeting service-level guarantees for CPU, memory, network, and disk bandwidth to each virtual machine hosted on the physical server.

![VMware ESX Server architecture](image)

Figure 1-2 VMware ESX Server architecture

These key elements are schematically depicted in Figure 1-2. As the figure illustrates, in addition to the three key elements just discussed, the ESX Server architecture includes a service console that provides bootstrapping, management, and other functionality. The
service console can be used, for example, to run the Navisphere® CLI software for control and management of EMC CLARiiON storage systems.

### 1.2.2 VMware ESX Server virtualization layer

Virtualization can be broadly defined as the use of software to emulate hardware or a total computer environment different from the one in which the software is actually running. This class of software is sometimes referred to as a virtual machine. A virtual machine may exist in an environment that is also running other applications and is not part of the virtual machine. This kind of virtualization has been defined as allowing multiple execution environments.

Figure 1-2 shows how the VMware ESX Server virtualization layer brings hardware virtualization to the standard Intel server platform. The virtualization layer is common among all of the VMware Platform product set, providing a consistent platform for development, testing, delivery, and support of applications from the developer desktop to the enterprise-class servers.

The VMware virtual machine offers complete hardware virtualization. The guest operating system and applications that run inside a virtual machine cannot determine the specific underlying physical resources they are accessing. The virtualization layer provides virtual devices to each virtual machine that is isolated from all other virtual machines on the system. The virtual devices include CPU, memory, I/O buses, network interfaces, storage adapters, and human interface devices.

Each virtual machine runs its own operating system and applications. They cannot communicate to each other except via peer-to-peer networking mechanisms similar to those used to connect separate physical machines. This leads many users of VMware software to build internal firewalls or other network isolation environments, allowing some virtual machines to connect to the external network while others are connected through other virtual machines.

### 1.2.3 VMware ESX Server disk provisioning methods

There are many terms for describing disks and disk arrays. The term *device* can refer to the LUN or disk itself. Physical disks presented to an ESX Server can reside on local storage or on a disk array usually attached to a SAN. A logical unit number (LUN) is a 4-bit identifier used on a SCSI bus to distinguish 16 devices (logical units) with the same SCSI target ID.

LUNs can be presented to virtual machines by creating virtual disks. To the virtual machine, the virtual disk appears as a physical disk. Each virtual machine has an accompanying configuration file, the .vmx file, which VMware ESX Server uses to access disk image files and set up the virtual hardware. When the virtual machine is created, a configuration file with .vmx extension is generated. This file contains the location of virtual disk, memory size, and some basic hardware setup information (CD-ROM drive, floppy drive, network connections) for the virtual machine.

A CLARiiON LUN can be provisioned to virtual machines using raw disks, VMFS volumes, or raw device mappings, as described next.
♦ Raw disks

A VMware raw disk (LUN) assigned to a virtual machine is directly mapped to a physical disk drive on the VMware ESX Server. A virtual machine’s disk can be stored as a file called a virtual disk file or on a raw disk device. When a virtual machine is configured to use a raw disk, the virtual machine directly accesses the local disk/partition as a raw device.

♦ VMFS

CLARiiON LUNs presented to an ESX Server can be used as a VMFS (VMware ESX Server File System) volume. VMFS is a simple, high-performance file system on physical SCSI disks and partitions. It is used for storing large files such as the virtual disk images for one or more virtual machines and, by default, the memory images of suspended virtual machines. VMFS also stores the redo log files for virtual machines in nonpersistent, undoable, or append disk modes.

To create a virtual machine on VMFS, a special file with vmdk extension must be created on the VMFS volume. The .vmdk file, or image file, is the virtual disk containing the operating system and/or data and applications. To the virtual machine, the vmdk file appears as a physical disk. The vmdk file is an encapsulation of the information created by a virtual machine.

♦ Raw device mappings

VMware ESX Server 2.5 and later improved support for raw disks as virtual machine disks by introducing a new technology called raw disk mapping (RDM). This technology enables raw disks to be managed as easily as virtual disk files on VMFS. Furthermore, virtual machines that use RDM can be migrated to another ESX Server using VMotion. The use of RDM in the virtual machines enables:

• Use of SAN replication software inside virtual machines.

• Solutions to offload backups so that ESX Servers can be backed up faster without any load placed on the virtual machines or on the Service Console.

• Use of redo log files for raw disks configured in nonpersistent, undoable, or append disk mode. Use the virtual compatibility mode to enable this feature.

A raw device mapping (RDM) volume contains a pointer, which is a .vmdk file that resides on a VMFS volume. This VMFS volume can be on the SAN or on a local disk. Raw disk mappings are only supported on SAN LUNs. Therefore, raw disk mappings will work when the Fibre Channel HBA used is dedicated to the virtual machine. In the case of a raw disk mapping, the `vmkfstools -i` (for import) and `-e` (for export) command options are available for mobility.

Figure 1-3 on page 1-9 shows a VMware ESX Server configured with SAN-attached storage. It depicts four virtual machine configurations using the storage presented from the CLARiiON storage system connected through the SAN. Virtual Machine 1 is configured with a raw disk through the virtualization layer. Virtual Machines 2 and 3 are presented virtual disks created on one VMFS volume. Virtual Machine 4 is configured to use raw disk mapping volumes through the virtualization layer.
Figure 1-3  VMware ESX Server with SAN-attached storage
This chapter presents these topics:

2.1 EMC CLARiiON .......................................................... 2-3
2.2 EMC CLARiiON management ........................................ 2-4
2.3 CLARiiON virtual LUN technology .............................. 2-6
2.4 EMC SnapView ............................................................ 2-9
2.5 EMC SAN Copy .......................................................... 2-13
2.6 EMC MirrorView ......................................................... 2-15
EMC provides many hardware and software products that support application environments on CLARiiON storage systems. The following products were used and/or tested with the VMware products discussed in this document:

♦ **EMC CLARiiON** – EMC offers an extensive product line to deliver fast, easy connectivity and data integration, continuous data availability, and compatibility with existing technology. The CLARiiON product line includes the CX and AX series family. EMC CLARiiON is a fully redundant, high-availability storage processor providing nondisruptive component replacements and code upgrades.

♦ **Navisphere Manager and Navisphere CLI** – Navisphere® Manager allows you to discover, monitor, and provision storage securely on multiple CLARiiON storage systems from a browser anywhere, anytime. The software required to manage the storage system runs on CX and AX series storage systems and can manage all of the iSCSI and SAN-based CLARiiON storage systems in your environment, whether they are located at your primary location or satellite facilities. Navisphere CLI is used for writing scripts, issuing commands to a storage system, requesting storage-system status, recording commands and the resulting output, and as a tool for problem resolution.

♦ **CLARiiON Virtual LUN technology** – This technology comprises two components: CLARiiON metaLUNs and CLARiiON LUN migration:

  • **CLARiiON metaLUNs** – This technology allows users to dynamically grow existing CLARiiON LUNs and add capacity while the LUN is online. This can be done using two methods: striping and concatenation. When using striping, the data being written to the new metaLUN is striped across several LUNs of the same RAID type and size. Concatenation allows users to add a LUN of the same RAID-protection type (protected or unprotected) and the same disk type to an existing LUN or metaLUN. In either case, using striping or concatenation, the new metaLUN retains all attributes of the original LUN information to ensure this process is transparent to the host.

  • **CLARiiON LUN migration** – The LUN migration technology allows customers to migrate data to another LUN while applications are running. LUNs can be migrated to the same or different RAID levels and disk types. This gives customers control over the level of data protection needed for any given application, the number of spindles required for application performance, and better usage of disk space.

♦ **EMC SnapView** – The SnapView™ family of products enables LUN-based replication within a single CLARiiON storage system. Replicas of source CLARiiON LUNs are created using storage-system resources without using host CPU or I/O. The SnapView family has two separate and distinct software products: SnapView clones (BCVs) and SnapView snapshots.

  • SnapView clones allow users to make copies of data simultaneously on multiple target LUNs from a single source LUN. The data is available to a target’s host after the clone is fractured from the source LUN. Data may be copied from a single source LUN to as many as eight target LUNs.
• SnapView snapshots are pointer-based replicas that provide users space-saving copies of data from a single source LUN. The data is available to a target's host immediately upon creation. Data may be copied from a single source LUN to as many as eight virtual snapshots. The source can be either a standard CLARiiON LUN or SnapView clones (BCVs).

Using the consistency group technology available with FLARE™ Release 19, both SnapView clones and snapshots can provide data consistency across a user-defined collection of related CLARiiON LUNs.

♦ EMC MirrorView – MirrorView™ is a business-continuity software solution that replicates and maintains a mirror image of data at the storage block level in a remote CLARiiON storage system. The MirrorView family has two separate software products: MirrorView/Synchronous and MirrorView/Asynchronous.

• MirrorView/Synchronous (MirrorView/S) provides highly available data storage mirroring for disaster recovery. By maintaining synchronous data mirroring between EMC CLARiiON systems, MirrorView/S ensures data availability of byte-for-byte mirrored images.

• MirrorView/Asynchronous (MirrorView/A) provides disaster recovery via periodic updates of the secondary LUN. MirrorView/A gives users the ability to schedule how often they want the secondary mirror to be updated: from minutes to hours.

Using the consistency group technology, both MirrorView/S and MirrorView/A can provide data consistency across a user-defined collection of related CLARiiON LUNs.

♦ EMC SAN Copy – SAN Copy™ provides users a method to replicate data across multiple storage-system devices and/or within a single CLARiiON storage system. SAN Copy is completely storage-system based and uses no host cycles. SAN Copy can run in full or incremental mode. Full mode pushes or pulls all of the data in a volume, regardless of when it was last modified. Incremental mode allows users to update only the changed data after the first full volume copy.

2.1 EMC CLARiiON

EMC provides a mid-tier fault-tolerant storage solution with no single points of failure—a product that delivers industry-leading performance for mission-critical applications and databases. All CLARiiON storage systems provide advanced data replication capabilities, with open systems support and connectivity options, including Fibre Channel and iSCSI.

Interoperability between CLARiiON storage systems enables current customers to perform data-in-place upgrades of their storage solutions from one generation to the next, protecting their investment as their storage demands expand.
The CLARiiON on-board data integrity features include the following:

- Centralized and simplified storage management
- Data availability and protection for servers
- Nondisruptive hardware and software upgrades
- Automatic diagnostics and phone-home capabilities

The CLARiiON CX700, CX500, and CX300 are the latest generation of CLARiiON CX series storage systems. The current CLARiiON line is the next generation of the original CLARiiON CX600, CX400, and CX200 storage systems. The AX100 is an entry-level system that consists of a single-controller and dual-controller model. It provides a raw capacity of about 3 TB for up to eight connected hosts. CLARiiON CX series storage systems can combine any mix of RAID configurations (RAID, 0, 1, 3, 1/0, and 5) simultaneously—in a single chassis—offering the widest choice of RAID options.

CLARiiON systems use industry-standard Fibre Channel disk drives and support ATA (serial and parallel) disk drives, allowing them to keep pace with customer needs as technology enables increased capacities and improved performance.

2.2 EMC CLARiiON management

EMC CLARiiON software products simplify and automate the management of CLARiiON environments. Navisphere Manager and CLI provide a balanced set of capabilities that meet the ease-of-management and security requirements of today’s operating environments. They also manage optional software packages like SnapView, MirrorView, and SAN Copy.

2.2.1 Navisphere Manager

Navisphere Manager is a web-based interface that allows you to discover, monitor, and provision storage securely on multiple CLARiiON storage systems from a browser anywhere, anytime.

The Access Logix™ feature integrated in Navisphere Manager provides flexible, intuitive, easy-to-implement data protection, shared storage access, and security in a CLARiiON storage system. It provides secure, shared, or selective access to the EMC CLARiiON CX series storage systems in both mixed and homogeneous platform environments. Access Logix controls access to both reading and writing data, configuration changes, and management of storage-system resources. The Access Logix feature lets you enable data access and create storage groups on storage systems. A storage group is a collection of one or more LUNs to which you connect one or more servers. A server has only access the LUNs in the storage group to which it is connected. It cannot access the LUNs assigned to other servers unless those LUNs are shared between the storage groups.
2.2.1.1 Domains and multidomains

Navisphere Manager lets you create storage-system domains and multidomain environments. A domain lets you manage and monitor a group of storage systems using a single instance of Navisphere Manager and a single login; a multidomain environment lets you manage and monitor a group of domains (potentially all CLARiiON storage systems in the enterprise). Domains and multidomain environments can include both AX series and CX series storage systems.

All storage systems within a domain must be running the storage management server software, and must be connected to the IP network. Each storage system can belong to only one domain, but a domain can belong to more than one multidomain environment. Each domain has a master node (master storage system) that maintains the master copy of the domain data—the storage systems and global user accounts that make up the domain. All domain and global/account information is duplicated on all systems in the domain, so if a system fails, the information is retained and other systems in the domain remain accessible. If the system that fails is the master node, no global updates are allowed until you choose a new master or the failed system is replaced.

The multidomain feature lets you use the same instance of Navisphere Manager to manage and monitor any or all CX series and AX series storage systems in the storage enterprise, even if they are in separate domains. A multidomain environment consists of a local domain (domain from which you will manage and monitor all other domains) and gateway domains (domains managed by the local domain).

2.2.1.2 Event notification

With its Event Monitor tool, Navisphere Manager provides storage event notification software for enterprises running EMC CLARiiON systems. Administrators are notified automatically when failures or status changes occur on EMC CLARiiON systems. The user can easily program the software to launch custom responses after an event has occurred. It is customizable to the administrative environment and the user can configure it to email, send an SNMP trap, or page selected personnel—such as the system administrator or service provider—when a system’s status changes.

2.2.2 Navisphere CLI

Navisphere CLI provides a set of text-based commands that can be run in a non-graphical environment or from a remote location. Navisphere CLI is used for writing scripts, issuing commands to a storage system, requesting storage-system status, recording commands and the resulting output, and as a tool for problem determination. Navisphere CLI product consists of three kinds of CLI commands: Classic CLI, Java CLI, and Secure CLI.

Classic CLI allows users to configure and manage any storage system supported by Navisphere CLI version 6.x. You do not need to install a JRE to run Classic CLI commands.

Java CLI is implemented in Java and runs at the command prompt. Each Java CLI consists of a Java command (jar navicli.jar) and requires a valid username, password, and scope for security purposes.
Secure CLI is a comprehensive solution that provides one application and one security model for all CLI commands. Similar to classic CLI, you do not need to install a JRE to run secure CLI commands. Secure CLI implements the secure features of Java CLI, providing role-based authentication, audit trails of CLI events, and SSL-based data encryption.

2.2.3 Navisphere host utilities

Navisphere Agent (for CX) or Server Registration Utility (for AX) installed on a host system is a communication bridge between the CLARiiON system and any attached hosts. The agent registers hosts and HBAs and provides drive-mapping information over the IP-based network for display in Navisphere Manager.

Navisphere Server Utility, a new host-based tool, registers hosts and HBAs but does not send drive-mapping information across an IP-based network. It only runs when invoked by a user.

Navisphere Initialization Utility is host-based software used to initialize a CX or an AX series storage system. The host on which this utility is installed must reside on the same subnet as the storage system itself. This new utility simplifies storage-system initialization because serial-line connectivity or use of crossover Ethernet cables is no longer required to configure the storage system.

2.2.4 Navisphere Analyzer

Navisphere Analyzer is a performance-analysis tool that is fully integrated with Navisphere Manager and CLI. It enables users to investigate performance patterns and trends in normal operation mode, as well as in benchmarks and performance tests. It helps find performance bottlenecks, which can be addressed by fine-tuning parameters of storage systems or by adding hardware components, such as cache memory or disks. You can connect to multiple hosts and collect performance data from CLARiiON storage systems connected to each host in the enterprise. Navisphere Analyzer can be used to continually monitor and analyze performance and to determine how to fine tune storage-system performance for maximum utilization.

2.3 CLARiiON virtual LUN technology

CLARiiON virtual LUN technology provides an additional layer of abstraction between the host and back-end disks. This abstraction provides extensive flexibility in terms of initial configuration, adjustments, and tuning. It consists of two components: CLARiiON metaLUNs and CLARiiON LUN migration.

2.3.1 CLARiiON metaLUNs

CLARiiON metaLUNs are a collection of individual LUNs that act in concert and are presented to a host or application as a single storage entity. MetaLUNs allow users to expand existing volumes on the fly. They are created by taking new and/or preexisting FLARE LUNs (FLUs) and fusing them together. A FLARE LUN is a logical partition of a FLARE RAID group that serves as the building blocks for metaLUN components.

Existing LUNs can be concatenated from heterogeneous components, or they can be
restriped across homogenous components. The next two sections describe in detail the two types of expansion that are possible when using metaLUNs.

### 2.3.1.1 Stripe expansion

Figure 2-1 depicts a striped metaLUN before and after expansion. This is represented both graphically and as it appears in Navisphere Manager. The graphical depiction shows that after the striping process, the data—which was contained on FLU 27—is now spread evenly across all three of the LUNs in the component. Note, too, that since we have only conducted striped expansion, there is only one component—Component 0—that comprises the new metaLUN.

Having the data distributed in this manner allows the involvement of more physical spindles in a typical set of I/O operations. The additional capacity of the added FLUs is available to the host after the restriping process has taken place. Also, the restriping process will affect concurrent I/O, reducing throughput and increasing response time. Therefore, the recommendation is to perform striping during periods of low demand.

![Figure 2-1 MetaLUN expansion using striping method](image)

The rules for conducting striped LUN expansion are:

- All FLUs in the striped component must be of the same RAID type.
- All FLUs in the striped component must be of the same user capacity.
- All FLUs in a metaLUN must reside on the same disk type—either all Fibre Channel or all ATA.

### 2.3.1.2 Concatenate expansion

Figure 2-2 on page 2-8 depicts a concatenated metaLUN before and after expansion. In concatenate expansion, data residing on the base LUN remains in place. Additional capacity added in this fashion is simply appended to the end of the addressable space.
Additional spindles are only used as the host moves into the logical block address (LBA) range that is assigned to the additional FLUs. The tradeoff is that access to the additional space is near-instantaneous, since no data manipulation is required on the back end of the storage system.

![Figure 2-2 MetaLUN expansion using concatenation method](image)

Concatenate expansion also offers more flexibility in terms of the attributes of the LUNs that compose the metaLUN, as FLUs can be of different RAID types and user capacities. Also, the ability to quickly piece together noncontiguous space in this fashion allows users to maximize capacity utilization within the storage system.

The following are expansion rules (such as they are) for concatenated expansion:

- All FLUs in a concatenated metaLUN must be either protected (parity or mirrored) or unprotected. RAID types within a metaLUN can be mixed. For example, a RAID 1/0 FLU can be concatenated with a RAID 5 FLU. A RAID 0 can be concatenated with another RAID 0, but not with a RAID 5 FLU.
- All FLUs in a concatenated metaLUN must reside on the same disk-drive type—either all Fibre Channel or all ATA.

### 2.3.2 CLARiiON LUN migration

CLARiiON LUN migration allows users to change performance and other characteristics of an existing LUN, without disruption to host applications. It moves data—with the change characteristics that the user has selected—from a source LUN to a destination LUN of the same or larger size.

The LUN migration driver is an additional driver that leverages the existing FLARE operating environment. The technology can be used for hot-spot migration, archival, and consolidation purposes. Once the destination LUN is selected for migration purposes, the ownership of the destination LUN is changed to source LUN so that the migration process is managed by the controlling SP. During the migration process, the source LUN remains online. If a host write is received by the source LUN to a region that has been synchronized, then that write is automatically replicated to the destination.
LUN. The destination LUN, upon completion, assumes the source LUN’s name, WWN, and LUN ID.

LUN Migration is managed through Navisphere Manager. A Migrate option has been added to the existing LUN object menu. The Migrate option brings the user to the properties of the migration session properties, which allows the user to select the destination and rate of the migration session. A set of CLI commands are available as an alternate means of managing this technology.

The following migration rules apply:

♦ Source and destination LUNs must reside on the same storage system.

♦ Source and destination LUN can be in the same or different RAID groups.

♦ Any public FLARE LUN or metaLUN can migrate to any FLARE LUN or metaLUN of equal or larger size.

♦ RAID type of source and target LUN can be different.

♦ The source and target LUNs can be on disks of different type (Fibre Channel or ATA).

2.4 EMC SnapView

Navisphere Manager and CLI allow users to manage SnapView replicas. This section specifically describes the functionality of:

♦ SnapView clones (BCVs) – Point-in-time full copies of a source LUN, synchronized incrementally after initial creation.

♦ SnapView snapshots – Pointer-based copies that store pointers to the original data changed from the source LUN, rather than a full copy of the data.

Depending on your application needs, you can create clones, snapshots, or snapshots of clones.

2.4.1 SnapView clones

A clone is a complete copy of a source LUN. You specify a source LUN when you create a clone group. The copy of the source LUN begins when you add a clone LUN to the clone group. While the clone is part of the clone group and unfractured (not accessible to a secondary server), any server write requests made to the source LUN are simultaneously copied to the clone. Once the clone contains the desired data, you can fracture the clone. Fracturing the clone breaks it from its source LUN and makes it available to a secondary server. The source and clone must be equal in size to the source LUN. SnapView clone driver has the ability to create up to eight copies from a source LUN.
2.4.1.1 Clone private LUN

Clone private LUNs record information that identifies data extents on the source LUN and clone LUN that have been modified after you fracture the clone. A modified data extent is a chunk of data that a server changes by writing to the clone or source LUN. A log in the clone private LUN records this information, but no actual data is written to the clone private LUN. You must allocate one clone private LUN for each SP before you can create a clone group.

Clone fracture operations

Fracturing a clone detaches the clone from its source LUN and makes the clone ready for host access. When fracturing a clone, the system needs to perform housekeeping tasks that may require a few seconds on a busy CLARiiON storage system. These tasks involve certain steps that result in separation of the clone from its paired standard:

1. I/O is suspended briefly to the source LUN.
2. The clone is fractured from the source LUN.
3. If you have not already done so, put the clone into a storage group for a secondary server.
4. The clone is ready to be brought online.

Clone-consistent fracture

Clone-consistent fracture allows users to split off a dependent write-consistent, restartable image of an application with no interruption to online services. Consistent fracture helps to avoid inconsistencies and restart problems that can occur when splitting a group of clone without first quiescing or halting the application.

The consistent fracture operation can be processed on a group belonging to different source LUNs. All writes to the source LUNs are pended until the clone is fractured. Read activity to the device is not affected unless attempting to read from a device which has a write queued against it. Once the CLARiiON storage system acknowledges that the fracture is complete, I/O is allowed into the LUNs. Pending writes are acknowledged back to the host.

Restore operations

A clone can be used incrementally to restore data on the source LUN. A reverse-synchronization operation copies the contents of the clone to the source LUN. The incremental reverse-synchronization process accomplishes the same thing as the full-restore process with a major time-saving exception: the clone copies to the source LUN the new data that was updated on the clone while the clone pair was synchronized. Any changed tracks on the source LUN are also overwritten by the data on the corresponding tracks of the clone. This maximizes the efficiency of the resynchronization process. This process is useful for example if after testing or validating an updated version of a database or a new application on the clone is completed, a user wants to migrate and utilize a copy of the tested data or application on the production standard device.
Note: An incremental restore of a BCV volume to a source LUN is only possible when
the two volumes have an existing clone relationship.

The clones now contain a restartable copy of the production data that is consistent to the
point of the fracture. The production application is not aware that the fracture or
suspend/resume operation occurred. The application on the secondary host is started
using the clones. The application on the secondary host views the BCV copy as a
crashed instance and proceeds to perform the normal crash recovery sequence to restart.

2.4.2 SnapView snapshots

A snapshot is a virtual LUN that provides a point-in-time view of a source LUN. The
point-in-time reference is based on when the SnapView session is started. The session
keeps track of the source LUN’s data at a particular point in time.

2.4.2.1 The reserved LUN pool

The reserved LUN pool consists of one or more private LUNs and supports SnapView
sessions and snapshots. The reserved LUN pool stores the original source LUN data
chunks that have been modified since the start of the session. For any one session, the
contents of a reserved LUN(s) and any unchanged source LUN(s) blocks compose the
SnapView session.

Server writes made to an activated snapshot are also stored on a reserved LUN in the
SP’s LUN pool. When you deactivate the snapshot, the reserved LUN space is freed and
all server writes are destroyed.

Table 2-1 summarizes some of the SnapView snapshot components.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session</td>
<td>A SnapView session is a point-in-time copy of a source LUN. The session keeps track of how the source LUN looks at a particular point in time. As the production server writes to the source LUN, the software stores the contents of the original data in the reserved LUN pool. This is referred to as the copy-on-first-write technique and occurs only once.</td>
</tr>
<tr>
<td>Snapshot</td>
<td>A snapshot is a virtual LUN that allows a secondary server to view a point-in-time copy of a source LUN. You can create a snapshot before or after you start a session; however, the snapshot has no use until a secondary server activates it to a session.</td>
</tr>
<tr>
<td>Activated Snapshot</td>
<td>An active snapshot allows a secondary server to view a SnapView session. Once a secondary server activates a snapshot to a session, this server can write to the activated snapshot.</td>
</tr>
</tbody>
</table>
Activating the snapshot to a session makes the snapshot viewable to the host. Unless the data is changed by the host accessing the snapshot, it always presents a frozen point-in-time copy of the source device at the point of activation. When the information is no longer needed, the session can be deactivated from a SnapView session, which destroys any secondary writes made to the snapshot. The session and snapshot still exist but are not visible to the secondary server. You have the option to destroy the session using the stop session operation. The snapshot object can be destroyed with the destroy snapshot operation.

You can create eight sessions per source LUN. You can also use the deactivate and activate functions to change the focus of a snapshot from one session to another. You must deactivate a snapshot before you can activate it to another session. You can create up to eight snapshots and activate each snapshot to a single session provided there is a different server for each snapshot. Only one snapshot at a time can activate a session. SnapView snapshot operations are controlled from the host by using the `admsnap` command to create, activate, and deactivate SnapView sessions, and can be scripted for automation.

2.4.2.2 Modes to start SnapView sessions

A SnapView session can be started using consistent mode, persistent mode. A SnapView session can also be started using both modes. The two modes are discussed in detail next.

**Consistent mode** – Preserves the point-in-time restartable copy across a set of source LUNs. The SnapView driver will delay any I/O requests to the set of source LUNs until the session has started on all LUNs, thus preserving the point-in-time restartable copy on the entire set of LUNs. In the event of a failure, the software will not start the session on any source LUN and will display an error message. Consistent mode also prevents you from adding other LUNs to the session.

**Persistent mode** – Creates a session that can withstand the following disruptions:

- SP reboot or failure
- Storage-system reboot or power failure
- Server I/O trespassing LUN to the peer SP

The persistence feature is available on a per-session basis (not per snapshot or source LUN). In the event of a failure, reserved LUNs along with the source LUNs will trespass to the other SP. Depending on your failover software, once the failed SP is restored, you may need to issue a restore command to restore the proper source LUNs and reserved LUNs back to their original SP.

**Rollback operation**

A rollback operation lets you restore the point-in-time copy of a SnapView session to the source LUN(s). You can roll back any persistent SnapView session. When you start a rollback operation, you have the option of starting a recovery session. A recovery session allows you to undo the rollback operation because you can roll back the recovery
session. The recovery session contains the point-in-time data of your source LUN(s) before you started your original rollback.

2.5 EMC SAN Copy

EMC SAN Copy software runs on a CLARiiON storage system and copies data between CLARiiON storage systems, within CLARiiON storage systems, between CLARiiON and Symmetrix® storage systems, and between CLARiiON and qualified non-EMC storage systems. SAN Copy copies data directly from a source logical unit on one storage system to destination logical units on other systems, without using host resources. It connects directly or through a SAN, and supports protocols that let you use the IP SAN to send data over extended distances.

SAN Copy can perform multiple copies—each in its own copy session—simultaneously. When SAN Copy is installed on a storage system, the storage-system SP ports become initiators and therefore behave much like host initiators. If SAN Copy is installed on other storage systems, the SP ports may behave as either initiators or targets. For example, they can be added to storage groups, and they must be part of the SAN Copy zoning configurations.

You can use SAN Copy to create full and incremental copies of a source LUN. A full SAN Copy session is a bit-for-bit copy of all the data on the source LUN to a destination LUN. During a full SAN Copy session, the source is offline until the session completes. An incremental SAN Copy session copies only the data that has changed since the last copy session. This can significantly reduce the time needed to copy the data, thereby allowing the copy operation to be performed more frequently and more effectively. Unlike full-copy sessions, the source logical unit for an incremental session can remain online during the copy process. You must, however prepare the source logical unit prior to starting the session.

SAN Copy/E copies data from CX300 and AX series storage systems to CX series storage systems running SAN Copy. You can use SAN Copy/E to create full and incremental copies of a source logical unit.

SAN Copy and SAN Copy/E can be managed using Navisphere Manager and CLI. The admhost utility available for the Windows servers provides a command line executable that lets you execute certain commands (lun_activate, lun_deactivate, lun_flush, lun_list) when managing copy sessions.

2.5.1 Copying data between LUNs within a CLARiiON CX storage system

If you will be copying data from one LUN to one or many LUNs within the same CLARiiON storage system, the following requirements must be met before you start a SAN Copy session:

♦ The storage system must be a SAN Copy storage system.
♦ The source and all destination LUNs participating in a copy session must belong to the same SP.
♦ The destination LUN must be a size equal or greater than the source LUN.
2.5.2 Copying data between CLARiiON, Symmetrix, and supported third-party storage systems

To copy data between CLARiiON storage systems, or between CLARiiON and Symmetrix storage systems, the following requirements must be met before you start a copy session:

♦ The source logical unit, destination logical units, or both must reside on a SAN Copy storage system.

♦ The destination LUN must be a size equal or greater than the source LUN.

♦ All CLARiiON storage systems must be running Access Logix software.

♦ You must correctly zone SAN Copy storage system ports to remote storage systems so that SAN Copy can have access to these systems.

♦ In order for the logical units to participate in a SAN Copy session, you must make the logical units accessible to the participating SAN Copy storage-system port.

♦ For incremental copy sessions:

   • The source logical unit must reside on the SAN Copy storage system. It cannot reside on a remote storage system.

   • You must configure the reserved LUN pool before you start an incremental copy session.

   • The source logical unit cannot be a SnapView snapshot.

For information on copying data between CLARiiON, Symmetrix, and third-party storage systems, refer to the SAN Copy and SAN Copy/E release notes and administrator guides.

2.5.3 Integration of EMC SnapView with SAN Copy

SnapView can be used with SAN Copy to create a snapshot or a clone of the destination LUN, so that the SnapView replica can be put in the secondary server storage group, rather than the SAN Copy destination logical unit. This allows the SAN Copy destination logical unit to maintain consistency with its source, and be available on an ongoing basis for incremental updates. A full SAN Copy session can be started on the SnapView replica on the source LUN so as to avoid the source LUN from remaining offline during the entire copy process.
2.6 EMC MirrorView

EMC MirrorView is a business continuity solution that provides a host-independent, mirrored data storage solution for duplicating production site data to one or more physically separate target CLARiiON storage systems.

MirrorView replicates production or primary (source) site data to a secondary (destination) site transparently to users, applications, databases, and host processors. The primary (remote) image on the primary CLARiiON storage system is configured in a mirror relationship with the secondary image on a secondary CLARiiON storage system. In the mirrored state, the secondary image is read and write disabled for host access. After the secondary image becomes synchronized with its remote image, the secondary image can be fractured from the remote image. After the fracture, the secondary image contains valid data and can be snapped consistently using SnapView snapshots in order to have a fully accessible copy available for performing business continuity tasks. Note that fracturing the secondary image is not a recommended operation.

2.6.1 MirrorView products

The MirrorView family consists of MirrorView/Synchronous and MirrorView/Asynchronous.

♦ **MirrorView/Synchronous (MirrorView/S)** provides real-time mirroring of data between the primary CLARiiON system(s) and the secondary CLARiiON system(s). Data is written to both storage systems before a write is acknowledged to a host, thus ensuring the highest possible data availability. Data must be successfully stored in both the local and remote CLARiiON units before an acknowledgment is sent to the local host. This mode is used mainly for metropolitan area network distances less than 200 km over dark fibre.

♦ **MirrorView/Asynchronous (MirrorView/A)** maintains a dependent write-consistent copy of data at all times across any distance with no host application impact except during the update. MirrorView/A delivers high-performance, extended-distance replication and reduced telecommunication costs while leveraging existing management capabilities.

MirrorView/S and MirrorView/A operations can be managed with both Navisphere Manager and CLI.

2.6.2 MirrorView terminology

This section describes various terms related to MirrorView operations.

2.6.2.1 Synchronization operation

The *synchronization* operation occurs when the software copies data from a primary image to a secondary image. The synchronization operation can be a full or incremental sync. The synchronization process is needed during the following three cases:

♦ The secondary image is newly defined and needs to be synchronized with the primary image.
♦ The primary image loses contact with the secondary image. At this point, the secondary image would be system-fractured.

♦ The secondary image is admin-fractured and needs to be synchronized with the primary image.

The synchronization operation can be triggered automatically or explicitly, depending on the recovery policy, which can be set to automatic or manual. The synchronization rate can be set to low, medium or high. High completes faster, but may significantly affect storage system performance for server I/O request—particularly when multiple concurrent synchronizations are occurring.

2.6.2.2 Fracture operations

The fracture operation stops mirroring I/O from the primary image to the secondary image for MirrorView/S. For MirrorView/A, while in the midst of an update, the update is stopped when a fracture operation is issued. A system-fracture occurs automatically when there is a failure in the path to the secondary image and an administrative-fracture occurs when the administrator explicitly issues a fracture command.

When a secondary image is fractured, the primary image system does not forward any writes to the secondary system. Therefore, if there are writes going to the primary LUN at this time, those writes will not be propagated to the secondary image.

2.6.2.3 Failover and failback operations

Traditional disaster recovery routines involve customized software and complex procedures. Offsite media must be either electronically transmitted or physically shipped to the recovery site. Time-consuming restores and the application of logs usually follow. MirrorView failover/failback operations significantly reduce the recovery time by incrementally updating only the specific tracks that have changed. This accomplishes in minutes what might take hours for a complete load from dumped database volumes.

Practical uses of failover and failback operations usually involve the need to switch business operations from the production site to a remote site (failover) or vice versa (failback). Both these operations are controlled by the promote operation, discussed next. Once failover occurs, normal operations continue using the secondary copy at the disaster site. Scheduled maintenance at the production site is one example of where failover to the secondary or disaster site might be needed.

2.6.2.4 Promote operations

The promote operation causes the primary image to become a secondary image, thus swapping the role of the primary and secondary LUNs. The promote operation allows MirrorView LUNs acting as secondary images to take over operations while retaining remote mirror images.
2.6.3 MirrorView/S operations

MirrorView/S maintains synchronous data between two CLARiiON systems. It ensures that an up-to-date exact copy of the data is always available. Secondary data access facilitated by SnapView provides data, or backup capability, at remote locations while maintaining synchronous data availability.

The MirrorView/S driver contains built-in mechanisms to maintain data integrity in the event of a disruption to the communication link between the primary and secondary storage systems. These mechanisms track changed regions so that when the CLARiiON storage systems are able to communicate again, they can resynchronize incremental changes without having to perform a full synchronization. This is accomplished by using the Fracture Log.

2.6.3.1 MirrorView/S states operations

This section describes the states of the secondary image with respect to the primary image defined in a MirrorView pair:

♦ **Synchronizing** state refers to the operation that is initiating a data copy from the primary image to the secondary image.

♦ **Synchronized** state refers to the state in which the secondary image is identical to the primary image.

♦ **Consistent** state refers to the secondary image being identical to the primary image or to some previous instance of the primary image. This means the secondary image is available for recovery when you promote it.

♦ **Out-of-Sync** state means that the secondary image needs synchronization with the primary image. The secondary image is not available for recovery.

2.6.4 MirrorView/A operations

MirrorView/A provides a dependent write-consistent, point-in-time image on the secondary image, which is based on some point-in-time copy of the primary image. Unlike MirrorView/S, MirrorView/A transfers data to the secondary storage system in predefined timed cycles or delta sets. Before each update, a point-in-time copy of the secondary image is created so that in case of a primary site disaster, the secondary image can be promoted to the data state it was in before the update started.

MirrorView/A provides a long-distance replication solution with minimal impact on performance that preserves data consistency of application data in the specified business process. This level of protection can be leveraged for DR environments that always need a restartable copy of data at the secondary or disaster site. In the event of a disaster at the primary site or if the MirrorView links are lost during data transfer, a partial delta set of data will be discarded, preserving consistency on the disaster site.
2.6.4.1 MirrorView/A state operations

For MirrorView/A, a single LUN or group of LUNs under a consistency group can be part of the MirrorView/A session. A periodic update is sent to the secondary site. This section describes the states of the secondary image with respect to the remote or primary image defined in a MirrorView pair:

♦ **Synchronizing** state refers to two types of synchronization operations. Initial synchronization is used to bring the primary and secondary in a baseline synchronized state. Periodic synchronization occurs when the secondary mirror is updated with the changes on the primary mirror on a periodic basis.

♦ **Consistent** state refers to the secondary image being a consistent point-in-time copy of the primary image. This means the secondary image is available for recovery when you promote it.

♦ **Out-of-Sync** state means that the secondary image needs synchronization with the primary image. The secondary image is not available for recovery.

2.6.5 MirrorView consistency groups

When the amount of data for an application becomes very large, the time and resources required for host-based software to protect, back up, or run decision-support queries on these databases becomes a critical factor. The time required to quiesce or shut down the application for offline backup is no longer acceptable. MirrorView consistency groups allow users to remotely mirror the largest data environments and automatically split off dependent write-consistent, restartable copies of applications in seconds, with no interruption to online service.

A MirrorView consistency group is a group of LUNs that act in unison to maintain the integrity of applications. Its purpose is to provide data integrity for applications that span multiple LUNs. All operations such as synchronize, fracture, and promote are performed on the entire group. If a primary (remote) LUN in the consistency group cannot propagate changed data to its corresponding secondary LUN, MirrorView suspends data propagation from all LUNs in the consistency group. This suspension ensures a dependent write-consistent copy of the data on the secondary storage system.

2.6.6 Integration of EMC SnapView and EMC SAN Copy with MirrorView

SnapView and SAN Copy can be used to create replicas of the MirrorView secondary image, which is not viewable to any hosts to perform data verification and run parallel processes. While in a MirrorView relation, the secondary image can be snapped to allow access to the data at a secondary site. You cannot run SAN Copy full copy sessions on MirrorView secondary images. You can however run SAN Copy incremental sessions on MirrorView secondary images. The secondary image must be either synchronized or in a consistent state to ensure a consistent replica.
Chapter 3  Connectivity of VMware ESX Server to a CLARiiON Storage System

This chapter presents these topics:

3.1  Booting ESX Server from CLARiiON ................................................................. 3-2
3.2  Booting guest operating systems on CLARiiON .............................................. 3-2
3.3  High availability when using VMware ESX Server with CLARiiON .............. 3-3
3.4  Optimizing CLARiiON LUN layout with VMware ESX Server ..................... 3-6
3.1 Booting ESX Server from CLARiiON

VMware ESX Server Version 2.5 and later supports booting of the VMware ESX Server from a CLARiiON array. QLogic HBAs exposed to CLARiiON LUNs can be used to bootstrap the service console. If the ESX Server has more than one HBA, all its HBAs must be the same model. The BIOS settings of the server must be configured to use the CLARiiON LUN as the boot device. Ensure that the boot LUN is always /dev/sda and ID 0—the lowest-numbered LUN visible to the ESX Server. This can be accomplished using Navisphere Manager or CLI software.

The internal SCSI device (controller) must be disabled for the CLARiiON LUN to map as /dev/sda. In addition, the LUN from which the service console will boot should be presented on the lowest numbered path from the server to the CLARiiON array. Install the VMware ESX Server software on the CLARiiON LUN using the boot-from-SAN option. When installing the VMware ESX Server software, ensure that the Fibre Channel HBAs are shared between the virtual machine (VMkernel) and the ESX Service Console. If the ESX Server is not booting from SAN, it is recommended to have the Fibre Channel HBAs dedicated to the virtual machine. Note that only VMware ESX Server 2.5 or later supports booting the ESX Server from SAN.

3.2 Booting guest operating systems on CLARiiON

CLARiiON storage systems are connected to the VMware ESX Server (service console), hence the virtual machines running guest operating systems are unaware of the connectivity to the CLARiiON storage system. The VMkernel assigns LUNs to the individual virtual machines. Virtual SCSI adapters like Bus Logic and LSI Logic are assigned to virtual machines to recognize these LUNs. As a result, when using Access Logix on a CLARiiON storage system, a storage group is created for the ESX Server and not for individual virtual machines.

Users can boot their guest operating systems from a CLARiiON instead of booting from internal or local disks. This is a requirement when using VMware VMotion. For booting guest operating systems from a CLARiiON storage system, CLARiiON LUNs presented to the VMware ESX Server can be assigned to an already-created virtual machine using the management user interface (MUI). VirtualCenter or Remote Console can be used to install the guest operating system on the assigned CLARiiON LUN using a CD/ISO image or templates.

Once the virtual machine is up and running, it is highly recommended that VMwareTools be installed on each virtual machine. The use of the VMware-tools will optimize the use of the VMware ESX Server resources. The VMware Tools also provide a VGA device driver and a heartbeat mechanism for the virtual machine to communicate with the VMkernel.

3.2.1 Presenting LUNs to virtual machines

LUNs presented from a CLARiiON storage system can be added nondisruptively using the Rescan SAN option available in the Storage Management tab, as shown in Figure 3-1 on page 3-3. Although a new device can be presented to the ESX Server online, in order to add a LUN to a virtual machine, that virtual machine must be shut down.
3.2.2 Integration of Navisphere host utilities with VMware ESX Server

Navisphere Agent (CX series) or the Server Utility must be installed on the ESX service console to register the ESX Server with the CLARiiON storage system.

Navisphere CLI and array initialization software for the CX and AX series storage systems can run on the ESX Server console, as well as the individual virtual machines.

3.3 High availability when using VMware ESX Server with CLARiiON

This section discusses multipathing and failover support available within the ESX Server to maintain high availability in case of failure.

3.3.1 Multipathing and failover functionality in VMware ESX Server

With the native failover, functionality incorporated into the VMkernel, VMware ESX Server Version 2.1.x and later supports multiple paths and failover when attached to CLARiiON storage systems. VMware ESX Server does not support dynamic load balancing. Static load balancing can be achieved by balancing CLARiiON LUNs across the two SPs and HBAs.

Although the VMkernel sees multiple paths to the same or alternate CLARiiON storage processors, I/O routes only to a single path at a time. A maximum of eight paths to a CLARiiON SP are supported when using VMware’s native failover.
3.3.2 Configuring CLARiiON storage with VMware failover software

PowerPath® is not supported on the ESX Server service console or in the virtual machines. VMware ESX Server multipathing needs to be used to provide access to multiple paths to a storage device.

The most recently used (MRU) policy is the default policy for active/passive storage devices. The policy for the path should be set to MRU for CLARiiON storage systems. Using the fixed policy may cause path thrashing and significantly reduce performance. When using the MRU policy, the preferred path is displayed, but the ESX Server does not use it to access the disk. The preferred path is only used with the fixed-policy option. The active path will be the path used by the ESX Server to route the I/O.

The native failover software provides a listing of the paths—whether active or passive—from the VMware ESX Server to the CLARiiON storage system. The command, `vmkmultipath –q`, provides details on a particular device and the number of paths attached to that device. A sample output from the `vmkmultipath –q` command is shown in Figure 3-2.

![Figure 3-2 VMware ESX Server path information using CLI](image)

The figure shows two devices attached to the CLARiiON storage systems: vmhba0:0:0 and vmhba1:0:1. The ESX Server has two HBAs installed. Each HBA has a path to each SP, meaning that each device is accessed by both HBAs and has four paths. The active path indicates that this is the actual path used by the ESX Server to access the disk. Disregard the preferred path when using the MRU policy. You can also display path information by going to the main page and selecting: Options > Storage Management > Failover Paths, as shown in Figure 3-3 on page 3-5.
As mentioned previously, the MRU policy uses the most recent path (active path) to the disk until this path becomes unavailable. In case of a failure, the ESX Server fails over to a working path that could be a path to the same SP or a different SP. The native failover software does not automatically revert to the original path (when available), but a manual restore is required.

In the case of a path or SP failure, I/O freezes for 30 to 60 seconds until the SAN driver detects that a failure has occurred, and then fails over to the alternate path. The failover time can be adjusted at the HBA, ESX, and virtual machine level. The recommended settings for failover time at the HBA and virtual machine levels can be found in the document “Using Multipathing in ESX Server” available on the VMware website.

The ESX Server proactively evaluates the state of each path periodically. The default evaluation period is 300 seconds. This can be changed by modifying the `/proc/vmware/config/disk/PathEvalTime vmkernel config` value. This can also be done through the MUI by going to Advanced Settings and changing the Disk.PathEvalTime parameter. The evaluation period can be set to any value between 30 and 1500 seconds. Note that reducing the PathEvalTime causes path evaluation to run more frequently. This puts a slightly higher CPU load on the system. Reducing this value (to 90 for example) will help improve failover time (keeping in mind the caveat just mentioned).

If multipathing is being used with multiple Fibre Channel HBAs, then `vmkfstools` (or equivalent) must be run on all of the Fibre Channel HBAs when adding or removing devices. The MUI automatically does this when the SAN fabric is scanned for changes.
3.4 Optimizing CLARiiON LUN layout with VMware ESX Server

When configuring a virtual environment on a CLARiiON array, the disk layout for OS and application data must be considered. The best practice is to separate OS image and application data on separate set of LUNs, depending on the performance requirements of the application.

When installing a guest operating on a CLARiiON LUN, configure the LUN to use RAID 5 or RAID 1/0, depending on cost/redundancy. With VMFS volumes, you can configure a single LUN as a VMFS volume and present the entire LUN to one or more ESX Servers. If using VMFS volumes do not present an entire metaLUN and boot all your virtual machines on that LUN. For improved performance, align VMFS volumes at the ESX and virtual machine level.

The disk layout on the SAN should map to the best performance characteristics of the application as if the virtual layer was not in place. Follow the best practice recommendations applied to a native (physical) server for configuring applications on the ESX Server. For I/O-intensive applications, the use of RDM volumes is preferred since a single LUN is assigned per virtual machine to provide application integration and deliver better performance. However, note that an ESX Server has a limit of 128 SCSI disks. This limit includes both local devices and SAN LUNs. Disks configured as RDM volumes should be aligned at the virtual machine level.

When configuring raw device mapping, the recommendation is to create one VMFS volume that contains the mapping file information for all RDM volumes. A mix of VMFS and RDM volumes can be used on the ESX Server.
This chapter presents these topics:

4.1 Introduction .........................................................4-2
4.2 Expanding LUNs used as raw device mapping (RDM) .......................4-2
4.3 Expanding VMFS volumes ........................................4-3
4.4 Migrating VMFS and raw device mapping volumes ......................4-4
4.1 Introduction

CLARiiON virtual LUN technology provides an additional layer of abstraction between the host and back-end disks. It consists of two components: CLARiiON metaLUNs and CLARiiON LUN migration. Section 2.3 on page 2-6 provides additional information.

CLARiiON metaLUNs provide LUN expandability by growing a LUN nondisruptively using concatenation or striping method. When using metaLUNs with VMware ESX Server, remember that both the ESX Server and the virtual machine must be able to see the added space.

CLARiiON LUN migration allows users to change performance and other characteristics of an existing LUN, without disruption to host applications. When using LUN migration with VMware ESX Server, the process is seamless.

4.2 Expanding LUNs used as raw device mapping (RDM)

A LUN presented to a VMware ESX Server and to a virtual machine can be expanded with metaLUNs using the striping or concatenation method. After the expansion completes on the CLARiiON array, scan the HBAs using the Rescan SAN option in the MUI or command line interface to ensure the ESX service console and VMkernel see the additional space. Since the LUN is presented to the virtual machine, expansion must take place at the virtual machine level.

4.2.1 Guest OS considerations

LUNs expanded using the metaLUNs technology and presented to a virtual machine can be expanded using the native tools available with the virtual machine. The methods for Windows and Linux virtual machines are discussed next.

4.2.1.1 Windows guest OS considerations

To expand basic disks, Microsoft’s `diskpart` utility is required. After the LUN is expanded at the storage-system level, use the `diskpart` utility to extend the file system by using the extra space available in the expanded LUN. Host I/O should be stopped before executing this procedure. A full backup should be taken before executing the expansion procedure. For dynamic disks, the expansion can be performed online using Windows Disk Management utility. The disk containing the OS image can be expanded using utilities supported by Microsoft, such as Symantec’s Server Magic.

4.2.1.2 Windows Linux guest OS considerations

To expand a Linux file system on a Linux guest OS, unmount the volume before performing any kind of expansion. A full backup copy should be created before performing the expansion.
As an example, consider the expansion of partition 1 of the block device sdj. The following steps can be used to expand this partition after the CLARiiON LUN expansion has been performed:

1. Unmount the file system on the device /dev/sdj.
2. Using the `fdisk` command on the /dev/sdj device, execute the `w` (write) option. The `w` option for the `fdisk` command performs an `ioctl` on the device (LUN) and sees the expanded space. After the `w` is executed, you must run the `fdisk /dev/sdj` at the command prompt.
3. Delete partition (1) from /dev/sdj.
4. Create a new partition on /dev/sdj with the same partition number (1) that has the same start cylinder as the previous partition, but that now uses up all the available space on the volume now that it has grown.
5. Write the new partition to the partition table using the `w` option.
6. For reiserfs file system, use `resize_reiserfs /dev/sdj1` to resize the file system. For ext2 and ext3 file system, use `resize2fs /dev/sdj1` to resize the file system.
7. Mount /dev/sdj1. The data should be intact and the `df -h` command should reflect the expanded space.

### 4.3 Expanding VMFS volumes

VMware supports volume management functions where two or more CLARiiON LUNs configured as VMFS volumes can be concatenated together. This procedure is also called VMFS spanning and is done at the ESX Server level.

A CLARiiON LUN configured as a VMFS volume and presented to the virtual machine can be expanded by adding a new CLARiiON LUN and concatenating the two using VMFS spanning at the ESX Server level.

The other option is to expand the VMFS volume using CLARiiON metaLUNs and span the additional space with the original VMFS volume available before expansion. Refer to the emc128545 primus case for additional details.

To expand an existing virtual disk:

1. Power down the virtual machine using the disk.
2. Use `vmkfstools --extendfile` command to expand the .vmdk file.
3. Power on the virtual machine.
4. Expand the file system at the virtual machine level using the methods described in Section 4.2.1 on page 4-2.
4.4 Migrating VMFS and raw device mapping volumes

CLARiiON virtual LUN technology allows a user to migrate data from one LUN (metaLUN) to another LUN (metaLUN) while the application is online. LUN migration works on VMFS and RDM volumes and is transparent to the guest OS.

For VMFS volumes, if the destination LUN is larger than the source LUN and additional space is required, create a VMFS volume on the additional space and use VMFS spanning to increase the size of the original LUN. To expand the LUN at the virtual-machine level, use the procedure described in Section 4.3 for VMFS volumes.

For RDM volumes, if additional space is required, use the procedure described in Section 4.2 on page 4-2 to increase the size of the original LUN if the destination LUN is larger than the source LUN after the migration process completes.
This chapter presents these topics:

5.1 Introduction ............................................................................................................ 5-2
5.2 Configuring SnapView with VMware ESX Server ................................................ 5-2
5.3 Using SnapView with VMware ESX Server .......................................................... 5-4
5.1 Introduction

The EMC SnapView family of products provides different technologies to enable users to nondisruptively create and manage local point-in-time copies of data. The copy of the data can be used for parallel operational processes, such as backup, reporting, and application testing. With Release 19 of FLARE, SnapView snapshots and SnapView clones were qualified with VMware ESX Servers. This section discusses the integration of the SnapView products with VMware.

5.2 Configuring SnapView with VMware ESX Server

VMware ESX Server supports the use of VMFS and RDM volumes. A CLARiiON LUN presented to the VMware ESX/virtual machine can be configured as a VMFS or RDM volume. SnapView replication is supported on both VMFS and RDM volumes.

5.2.1 Replicating VMFS volumes using SnapView (clones and snapshots)

The following points outline the guidelines/restrictions when replicating VMFS volumes using SnapView replication software:

♦ The virtual disks in a VMFS volume must be in persistent mode during the SnapView replication process.

♦ When using VMFS volumes, the replica of a primary ESX Server cannot be presented back to the same ESX Server. Furthermore, the target ESX Server must not already have access to the original source VMFS volume. For example, an ESX Server participating in VMotion with the primary ESX Server would have access to the original source LUNs. Hence, this ESX Server should not be a target where a SnapView replica is presented.

♦ When replicating an entire VMFS volume that contains a number of virtual disks on a single CLARiiON LUN, the granularity of SnapView replication is the entire LUN with all its virtual disks.

♦ CLARiiON VSS provider is not supported on VMFS volumes.

♦ Ensure that the snapshot or clone is not in a device-not-ready state when presenting it to the ESX Server. For SnapView snapshots, the snapshot must be is activated before presenting it to the ESX Server. For SnapView BCVs (clones), ensure the clone is fractured before presenting it to the ESX Server.

♦ When making copies of VMFS volumes that span multiple CLARiiON LUNs, use the consistency technology available on SnapView.

♦ ESX Server-based VM snapshot copies should not be used with CLARiiON SnapView copies on the same VMFS volume.

♦ Creation of SnapView replicas of VMFS volumes is not supported on an AX100 running Navisphere Express.
5.2.2 Replicating RDM volumes using SnapView (clones and snapshots)

The following points outline the guidelines/restrictions when replicating VMFS volumes using SnapView replication software:

♦ Configure the LUNs to use the physical compatibility mode option when replicating RDM volumes using SnapView.

♦ VMware ESX Servers do not write a signature on RDM volumes presented to it. Hence, SnapView copies can be presented back to the same VMware ESX Server for use. The copies (snapshots or BCVs) cannot be used on the source virtual machines unless the guest OS supports this feature. However, they can be assigned as raw devices to another virtual machine.

♦ CLARiiON VSS provider is supported on RDM volumes.

♦ Ensure that the snapshot or clone is not in a device-not-ready state when presenting it to the ESX Server. For SnapView snapshots, the snapshot must be is activated before presenting it to the ESX Server. For SnapView BCVs (clones), ensure the clone is fractured before presenting it to the ESX Server.

♦ For AX100 running Navisphere Express, the SnapView replica must be presented to a native (physical) server.

♦ RDM volumes are not supported on VMware ESX 2.5.x when the ESX Server itself is booting from SAN.

5.2.3 Installing and configuring admsnap on virtual machines

The ESX service console does not create a device file for an unfractured clone or deactivated snapshot. Hence, utilities like admsnap are not supported on the ESX service console. This restriction only applies at the ESX service console level and not the virtual-machine level. As a result, admsnap can be installed on the virtual machines.

Use of RDM volumes on virtual machines can provide added software functionality when compared to VMFS volumes. The admsnap utility must be installed on virtual machines when using the SnapView functionality. There are no special considerations for installing and using admsnap under virtual machines. At the virtual-machine level, admsnap operations will function exactly as they would on a native (physical) server when issued on RDM volumes.

Most of the admsnap commands when issued on VMFS volumes will fail since VMFS volumes do not support SCSI pass-through commands to communicate with the CLARiiON storage system. Use Navisphere Manager or Navisphere CLI instead. The only admsnap command that will work is admsnap flush.
5.3 Using SnapView with VMware ESX Server

This section provides details on how SnapView technology can be used with VMware ESX Server. It depicts a few configurations where customers can deploy this technology with VMware ESX Server.

5.3.1 Implementing SnapView within a single VMware ESX Server

Figure 5-1 on page 5-5 depicts a scenario where a VMware ESX Server is running Windows and Linux virtual machines. Each virtual machine contains a source LUN from a CLARiiON storage system and is configured as a RDM volume. The source LUNs could contain the OS image, as well as the application data. For performance reasons, it is best to separate the guest OS image from application data.

This source LUN can be replicated presenting SnapView snapshots or SnapView clones to the same ESX Server but to a different virtual machine for testing, reporting, or backup purposes. To maintain consistency of write-order dependent LUNs, the consistency technology available with SnapView should be leveraged to replicate application data spanned across multiple LUNs. The consistency technology can also be used to replicate OS image (including application, active directories, and such) and application data at the same time to ease management tasks. When replicating the guest OS image, the best practice is to power off the virtual machine when taking a replica to ensure a consistent copy. A crash-consistent copy would be available if the virtual machines are not shut down during the replication process. Replicating a suspended virtual machine also results in a crash-consistent copy. For application data, use tools available on the guest OS to quiesce the application in order to take a consistent replica.

Ensure that the snapshot or clone is not in a device not-ready state when presented to the ESX Server since the ESX Server does not create a device file for a device in a not-ready state. In other words, ensure the snapshot is activated or clone fractured before assigning them to the ESX Server. Admsnap commands like start session, stop session, activate, and clone_activate can function from the virtual machine when using RDMs.
5.3.2 Implementing SnapView with two or more VMware ESX Servers

Figure 5-2 on page 5-6 depicts a scenario of a VMware ESX Server, which consists of two virtual machines running Windows and Linux. A source LUN, which may contain OS image and/or application data residing on a CLARiiON storage system, is presented to these virtual machines. A best practice is to separate the guest OS image from application data on different CLARiiON LUNs. The source LUN can be configured as a VMFS or RDM volume.

This source LUN can be replicated by presenting SnapView snapshots or SnapView clones to a backup ESX Server for testing, reporting, or backup purposes. The consistency technology available with SnapView can be used to replicate application data residing on several LUNs to provide consistency for write-order dependent applications. The OS image and application data can be replicated using the consistency technology at the same time, if they reside on separate LUNs. When replicating the guest OS image, the best practice is to power off the virtual machine when taking a replica. A crash-consistent copy would be available if the virtual machines are not shut down during the replication process. Replicating a suspended virtual machine also results in a crash-consistent copy. For application data, use tools available on the guest OS to quiesce the application in order to take a consistent replica.
5.3.3 Implementing SnapView to test application data replicas of native (physical) servers on virtual machines

Figure 5-3 on page 5-7 depicts a scenario where two native servers (Windows or Linux) contain a source LUN from a CLARiiON storage system. The source LUN containing application data can be replicated and presented to an ESX Server (virtual) for testing or backup purposes. The replica presented to the ESX Server must be configured as an RDM volume.

Note that replicating OS images of a native server and presenting them to an ESX Server is a one-way process since the restoration of the native OS image from a virtual or physical environment would be a manual process and is not something that has been tested. There are third-party tools available that provide the V2P (virtual-to-physical) conversion; however, they are not currently qualified by EMC.

Replication of OS images from a native to ESX Server is only recommended when a one-time migration or duplication of characteristics of the physical server to the virtual server is desired using SnapView clones. For Windows systems, the conversion from a physical OS to virtual OS can be performed on the clone using the VMware P2V tool. For Linux systems, force the native server to load the *buslogic* or *LSIlogic* driver by editing the modules.conf file since virtual machines running Linux use the bus logic adapter or LSI Logic. Create a clone of the OS image and present this replica to boot the Linux virtual machine. SnapView snapshots can be used to test the conversion process from a physical-to-virtual environment before performing the final migration.
5.3.4 Implementing SnapView to back up virtual machine data to a native (physical) server

Figure 5-4 depicts a scenario where a VMware ESX Server is running multiple virtual machines (Windows or Linux) and contains LUNs presented from a CLARiiON storage system. These LUNs contain application data of the Windows and Linux virtual machines. The application data LUNs can be replicated using SnapView and presented to a backup physical (native) server that is connected to a tape for archival purposes. The source LUNs presented to the ESX Server must be configured as RDM volumes. We do not recommend replicating the OS images of the individual virtual machines on the ESX Server using SnapView in this case.
This chapter presents these topics:

6.1 Introduction ............................................................................................................6-2
6.2 Configuring SAN Copy with VMware ESX Server ...............................................6-2
6.3 Using SAN Copy with VMware ESX Server..........................................................6-3
6.1 Introduction

EMC SAN Copy technology provides users the ability to distribute data locally and geographically from one CLARiiON array to another. This enables parallel operational processes, such as backup, reporting, and application testing at a remote or local site. With Release 19 of FLARE, SAN Copy was qualified with VMware ESX. This section discusses the integration of the SAN Copy with VMware ESX Server.

6.2 Configuring SAN Copy with VMware ESX Server

SAN Copy can copy data to a destination LUN by starting a full or incremental copy session. If using the full session option with SAN Copy, the source LUN can be a snapshot, clone or mirror image. Using the incremental SAN Copy session option, the source LUN can be a clone or mirror image.

Source LUNs participating in a full SAN Copy session can be configured as a VMFS or RDM volume. The source LUNs must be offline during the full copy operation. For incremental SAN Copy sessions, the source LUNs can be configured as VMFS or RDM volumes.

6.2.1 Replicating VMFS volumes using SAN Copy

The following points outline the guidelines/restrictions when replicating VMFS volumes using SAN Copy replication software:

♦ The virtual disks in a VMFS volume must be in persistent mode during the SAN Copy replication process.

♦ When using VMFS volumes, the replica of a primary ESX Server cannot be presented back to the same ESX Server. The target ESX Server must not already have access to the original source VMFS volume. For example, an ESX Server participating in VMotion with the primary ESX Server would have access to the original source LUNs. Hence, this ESX Server should not be a target where a SAN Copy replica is presented.

♦ When replicating an entire VMFS volume that contains a number of virtual disks on a single CLARiiON LUN, the granularity of SAN Copy replication is the entire LUN with all its virtual disks.

♦ ESX Server-based VM snapshot copies should not be used with CLARiiON SAN Copy copies on the same VMFS volume.

6.2.2 Replicating RDM volumes using SAN Copy

Note the following guidelines/restrictions when replicating VMFS volumes using SAN Copy replication software:

♦ Configure the LUNs to use the physical compatibility mode option when replicating RDM volumes using SAN Copy.
♦ VMware ESX Servers do not write a signature on RDM volumes presented to it. Hence, SAN Copy replicas can be presented back to the same VMware ESX Server for use. The replicas cannot be used on the source virtual machines unless the virtual machine (for example, Windows 2000) supports this feature. However, they can be assigned as RDM devices to another virtual machine.

♦ RDM volumes are not supported on VMware ESX 2.5.x when the ESX Server itself is booting from SAN.

6.2.3 Installing and configuring admhost on Windows virtual machines

Use of RDM volumes on virtual machines can provide added software functionality like the admhost utility. The admhost utility for SAN Copy is installed on Windows virtual machines and can be used to flush, deactivate, and activate a LUN. There are no special considerations for installing and using admhost under virtual machines. The VMware ESX Server masks the virtual environment from the guest operating system and any software that runs on it.

Most of the admhost commands will fail when issued on VMFS volumes since VMFS volumes do not support SCSI pass-through commands to communicate with the CLARiiON storage system. Use Windows native tools (such as mount_vol and diskpart) to bring the LUN online/offline. The only admhost command that will work is admhost flush.

For Linux systems, the mount and umount commands can be used to perform the tasks available with admhost on Windows systems.

6.3 Using SAN Copy with VMware ESX Server

This section depicts a few examples of how customers can deploy SAN Copy with VMware ESX Server.

6.3.1 Implementing SAN Copy to transfer data from one CLARiiON array to another using a single VMware ESX Server

As shown in Figure 6-1 on page 6-4, SAN Copy can be used to move data from a CX series storage system to a CX or AX series storage system. This scenario depicts a case in which the source LUN, which may contain OS image and/or application data for a Windows or Linux virtual machine on a CX series storage system, is copied to a destination LUN on a CX300. The destination LUN residing on a CX300 is presented to the same ESX Server but to a different virtual machine. In this case, the source LUN must be configured as an RDM volume for both full and incremental SAN copy sessions since same-host access support for VMFS volumes is not available due to disk signature conflicts.

The other consideration in this solution is to ensure the correct data volumes are presented and assigned to the secondary VMware ESX Servers and the virtual machines, respectively. This requires proper mapping of the host IDs (HLUs) of the LUNs on the primary CLARiiON storage system to the target CLARiiON LUNs. The virtual machine that contains the replica must see the LUNs in the same order as the source virtual machine.
6.3.2 Implementing SAN Copy to transfer data from one CLARiiON array to another using two VMware ESX Servers

In the Figure 6-1 example, SAN Copy is used to copy data between two CX series storage systems far apart from each other. The source LUN on the production ESX Server on a primary CLARiiON storage system can be copied to a destination LUN on a secondary CLARiiON storage system using full or incremental SAN Copy. A replica (snapshot or clone) can be used as a SAN Copy source to transfer the data to the SAN Copy destination LUN.

For both full and incremental copy sessions, the source LUN or replica (snapshot or clone) can be configured as a VMFS or RDM volume.

After the full SAN Copy session completes, the destination LUN can be presented directly to the target ESX Server at a remote site. For incremental SAN Copy sessions, the best practice would be to do the following:

1. Create a replica (snapshot or clone) of the destination LUN.
2. Present the replica to the ESX Server at a remote site to avoid modification of the SAN Copy destination LUN, thus preserving a gold copy at the remote site.

It is critical to ensure the correct data volumes are presented and assigned to the secondary VMware ESX Servers and virtual machines, respectively. Section 6.3.1 on page 6-3 provides more details.
6.3.3 Migrating physical servers to virtual servers from a third-party storage system to a CLARiiON array using SAN Copy

SAN Copy software can migrate data from a supported third-party storage system to a CLARiiON array using the full SAN Copy option. The physical servers connected to the third-party storage systems can also be migrated to VMware ESX Servers as depicted in Figure 6-3 on page 6-6. Please see the EMC Support Matrix for the third-party storage systems that are qualified with SAN Copy.

If Windows and Linux OS images reside on the third-party storage system, those images can be migrated to the CLARiiON array using SAN Copy. The replicas can then be presented to the ESX Server where tools like P2V can be used to convert a physical image to a virtual image for Windows virtual machines. For Linux systems, force the native server to load the buslogic or LSIlogic driver by editing the modules.conf file. The replicas for OS images presented to an ESX Server could have a VMFS partition or be configured as RDM volumes. Application data LUNs residing on the third-party storage system can be replicated using SAN Copy and presented to a virtual machine. The application data LUNs presented to the virtual machine can be configured as RDM volumes on the ESX Server.

The other consideration in the solution is to ensure the correct data volumes are presented and assigned to the VMware ESX Servers and the virtual machines, respectively. This requires proper mapping of the third-party storage device numbers on the target CLARiiON array to the canonical name assigned by the VMkernel. For example, if the physical server has its boot disk at \\PHYSICALDRIVE0 and three application data disks, \\PHYSICALDRIVE1, \\PHYSICALDRIVE2, and \\PHYSICALDRIVE3 that correspond to third-party storage, these four devices are replicated on the CLARiiON storage system to devices 001, 002, 003, and 004, respectively. Then, the virtual machine should be
presented four SCSI disks: 0:0, 0:1, 0:2, and 0:3. SCSI targets 1, 2, and 3 should map to devices 002, 003, and 004, respectively, on the CLARiiON array.

Figure 6-3 Using SAN Copy to migrate data from a third-party storage system connected to native servers onto a CLARiiON array connected to ESX Servers
This chapter presents these topics:

7.1 Introduction ............................................................................................................7-2
7.2 Configuring MirrorView with VMware ESX Server .............................................7-2
7.3 Using MirrorView with VMware ESX Server .......................................................7-3
7.1 Introduction

The CLARiiON MirrorView products (MirrorView/S and MirrorView/A) provide host-independent technology to propagate business-critical data to a remote location. With Release 19 of FLARE, the MirrorView family of products was qualified with VMware ESX. This section discusses the integration of the MirrorView products with VMware.

7.2 Configuring MirrorView with VMware ESX Server

The integration of MirrorView with VMware technology enables consolidation of multiple stand-alone systems in the primary data center to a virtual infrastructure in the remote location. SnapView snapshot in the remote data center can be used for other operational processes, such as offsite backup and vaulting. Furthermore, integrating the solution with the MirrorView/Consistency Group product enables customers to create business-consistent point-in-time data in the remote location. The MirrorView architecture supports the use of VMFS and RDM volumes.

7.2.1 Replicating VMFS volumes using MirrorView (Synchronous and Asynchronous)

Note the following guidelines/restrictions when replicating VMFS volumes using MirrorView replication software:

♦ The virtual disks in a VMFS volume must be in persistent mode during the SnapView replication process.

♦ When using VMFS volumes, the replica of a primary ESX Server cannot be presented back to the same ESX Server. The target ESX Server must not already have access to the original source VMFS volume. For example, an ESX Server participating in VMotion with the primary ESX Server would have access to the original source LUNs. Hence, this ESX Server should not be a target where a SnapView replica is presented.

♦ When replicating an entire VMFS volume that contains a number of virtual disks on a single CLARiiON LUN, the granularity of MirrorView replication is the entire LUN with all its virtual disks.

♦ Use the consistency technology available on MirrorView when making copies of VMFS volumes that span multiple CLARiiON LUNs.

♦ ESX Server based VM snapshot copies should not be used with CLARiiON MirrorView copies on the same VMFS volume.
7.2.2 Replicating RDM volumes using MirrorView (Synchronous and Asynchronous)

The following outline the guidelines/restrictions when replicating VMFS volumes using MirrorView replication software:

♦ Configure the LUNs to use the physical compatibility mode option when replicating RDM volumes using MirrorView.

♦ VMware ESX Servers do not write a signature on RDM volumes presented to it. Hence, MirrorView copies can be presented back to the same VMware ESX Server for use. The copies cannot be used on the source virtual machines unless the virtual machine (for example, Windows 2000) supports this feature. These copies can be assigned as RDM devices to another virtual machine on the same ESX Server.

♦ RDM volumes are not supported on VMware ESX 2.5.x when the ESX Server itself is booting from SAN. For ESX boot from SAN configuration, the HBAs must be shared between the service console and virtual machines.

7.3 Using MirrorView with VMware ESX Server

This section depicts two configurations that customers can deploy the MirrorView technology with VMware ESX Server.

7.3.1 MirrorView from a physical-to-virtual infrastructure

Figure 7-1 on page 7-4 is a schematic representation of the business-continuity solution that integrates physical infrastructure with virtual infrastructure using CLARiiON MirrorView technology.

The physical infrastructure at the production site can be replicated using MirrorView, where the replica can be presented to a virtual machine on a VMware ESX Server at the remote site in case of disaster.

Note that replication of OS images using MirrorView from a physical to virtual environment is a one-way process since there are no tools currently qualified by EMC to convert a virtual machine back to a physical server during the failback process. Without V2P tools, the failback process can be cumbersome. Hence, replicating physical machine OS images for conversion to virtual machines on a VMware ESX Server is currently not supported with MirrorView.

The LUNs containing application data on a physical server need no reconfiguration during the failover or failback process and are thus supported for replication with MirrorView. The replica presented to the virtual machine must be configured as an RDM volume. Ensure the correct application data volumes are presented and assigned to the VMware ESX Servers and virtual machines, respectively. This requires proper mapping of the CLARiiON device numbers on the target CLARiiON storage system.

To maintain data consistency for dependent write-order LUNs, EMC strongly recommends using the MirrorView/Consistency Group product with the solution. The secondary images on the target CLARiiON storage system are normally presented as read and write disabled, and hence cannot be seen by the VMware ESX Server unless those images are promoted. Copies of the application data can be obtained on the remote
site by replicating secondary images using SnapView snapshots. These copies can be used for ancillary operation processes such as QA or backup. The snapshots must be in an activated state before presenting them to the ESX Server.

![Diagram](image.png)

**Figure 7-1 Using MirrorView for business continuity solution by transforming physical to virtual infrastructure**

### 7.3.2 MirrorView virtual-to-virtual infrastructure

Figure 7-2 on page 7-5 is a schematic representation of the business-continuity solution that integrates VMware virtual infrastructure and CLARiiON MirrorView technology.

The solution provides a great opportunity to consolidate the virtual infrastructure at the remote site. It is possible to run VMware virtual machines on any VMware ESX Server. This capability also allows the consolidation of the production VMware ESX Servers to a smaller set of VMware ESX Servers at the remote site. Doing so, however, creates a potential for duplicate virtual machine IDs when multiple virtual machines are consolidated in the remote site. If this occurs, the virtual machine IDs can be easily changed at the remote site. Both VMFS and RDM volumes can be replication using the MirrorView software.

VMware ESX Servers maintain a configuration file (a flat file with a .vmx extension) that records the hardware configuration for the virtual machines. The configuration file includes information such as memory size, network configuration (including virtual MAC address), and SCSI disk information of the virtual machine. The configuration file is created when a virtual machine is initially created.

It is possible to use the same configuration file across separate VMware ESX Servers. Due to the consolidation of VMware ESX Servers at the remote site, the configuration of the virtual machines is...
anticipated to be significantly different than the production site. Copying the production configuration files to the remote site is therefore not recommended.

Both OS and application data can be replicated using MirrorView. The consistency technology available with MirrorView can be used to replicate application data spanning multiple LUNs to provide consistency for write-order-dependent LUNs. The OS image and application data can be replicated using the consistency technology at the same time. Copies of both OS and application data can be obtained on the remote site by replicating secondary images using SnapView snapshots for testing or backup purposes. Ensure the snapshots are activated before they are presented to the ESX Server.

Figure 7-2 Using MirrorView to replicate virtual infrastructure environment
Appendix A  References

This appendix presents these topics:

A.1  EMC references ................................................................. A-2
A.1  VMware references ............................................................ A-2
A.1 EMC references

- Host Connectivity Guide for VMware ESX Server v2.x (P/N 300002304)
- Navisphere Manager Administration Guide (P/N 069001125)
- EMC SnapView Administration Guide (P/N 069001180)
- CLARiiON Reserved LUN Pool Configuration Considerations (P/N H1585)
- EMC SAN Copy Administration Guide (P/N 069001188)
- EMC SAN Copy/E Administration Guide (P/N 300-002-664)
- EMC MirrorView Synchronous Administration Guide (P/N 069001161)
- EMC MirrorView Asynchronous Administration Guide (P/N 300-001-333)
- Replication Local and Remote- A Case Study (P/N H1426)
- Primus Database, found at:
  http://csexplorer.isus.emc.com/eservice/iviewcs/ui/eserver.asp
- EMC Support Matrix, found at:
  http://www.EMC.com

A.1 VMware references

- VMware ESX Administrator Guide, found at:
- VMware VirtualCenter documentation, found at:
- P2V User Guide, found at:
  http://www.vmware.com/support/p2v21/doc/index.html
- SAN Compatibility Guide, found at:
- CLARiiON integration with VMware, found at: