EMC RepliStor and VMware Software: Providing High Availability, Disaster Recovery, and Data Consolidation in Virtual Environments

Applied Technology

Abstract
This paper focuses on high availability, migration or consolidation, and disaster recovery solutions for Microsoft Windows environments using EMC® RepliStor® and VMware. This document provides an overview of each of these use cases and presents a simple solution that addresses each task.

June 2006
# Table of Contents

**Executive summary** ................................................................................................................. 4

**Introduction** ................................................................................................................................. 4
  - EMC RepliStor .............................................................................................................................. 4
  - VMware ......................................................................................................................................... 4
  - Audience ...................................................................................................................................... 5

**Overview** .................................................................................................................................... 5

**Theory of operations** ..................................................................................................................... 5
  - Providing high availability with EMC RepliStor and VMware .................................................... 5
  - Configuration requirements .......................................................................................................... 6
  - Installing and configuring EMC RepliStor for high availability .................................................. 6
  - Migrating or consolidating a physical server to VMware virtual servers .................................... 14
  - Configuration requirements ......................................................................................................... 14
  - Preparing target devices with boot sectors .................................................................................. 15
  - Presenting target devices to the Image Collector .......................................................................... 16
  - Installing and configuring EMC RepliStor ................................................................................... 16
  - Converting the physical OS replica to a virtual machine ............................................................... 17
  - Running P2V on the helper machine ............................................................................................. 18
  - Creating the virtual machine ........................................................................................................ 22
  - Disaster recovery options ............................................................................................................. 23

**Conclusion** .................................................................................................................................. 23

**References** ................................................................................................................................. 23
Executive summary

Every IT organization is responsible for providing a predefined level of service to its end users. These requirements are usually defined in a Service Level Agreement (SLA). The two prime components of any SLA are typically Recovery Point Objectives and Recovery Time Objectives, or RPO and RTO, respectively. RPO defines the amount of data loss that can be tolerated, and RTO defines the maximum amount of downtime that is acceptable based on your businesses requirements. Inevitably, the level of service that can be provided will be influenced by resource availability, both human and computing.

Common IT challenges discussed in this document are high availability, migration and/or consolidation, and disaster recovery with Microsoft Windows environments. Traditionally these tasks would be performed with a combination of hardware provisioning and tape restore. But relying on these conventional methods can be time-consuming and prone to human error. In addition, tape restore can not provide up-to-date content, resulting in some amount of data loss and in the end making SLAs hard to meet.

The intent of this white paper is to provide a practical approach to these challenges within your Windows environments. Using a combination of EMC® RepliStor® and VMware, a single, comprehensive solution set can address all of these challenges while still adhering to even the strictest SLAs. With VMware’s virtualization technology, one physical server can host multiple virtual servers. In doing so, VMware eliminates the need for a 1 to 1 hardware requirement and provides additional cost-saving benefits while reducing complexity.

Introduction

EMC RepliStor

RepliStor delivers a simple and reliable asynchronous replication solution that geographically distributes identical sets of data instantly to one or many computers in real time on Windows platforms. This solution increases the availability of data by delivering real-time replicas of as many copies as needed to virtually any location. RepliStor enables the use of data for anything from offline backup protection, disaster recovery switchover, and file and content publication, to decision-support data warehousing and countless other applications.

The use of LANs or WANs allows RepliStor to protect more than just data; it can protect an entire site. Updates are captured to selected files on source systems and forwarded across LANs and WANs to user-specified target systems. In the event of data loss or hardware failure at the source location, an up-to-date copy of every specified file is always available on the network. RepliStor is also an ideal solution to distribute or consolidate information. Reliability and ease of use, combined with RepliStor’s ability to replicate to dissimilar systems, makes it one of the most popular choices by customers.

VMware

VMware provides the most widely deployed software suite for optimizing and managing IT environments through virtualization – from the desktop to the data center. VMware software lets you virtualize computing, storage, and networking systems and manage them all centrally. VMware products provide enterprise-class virtual machines that increase server utilization, performance, and system uptime, reducing the cost and complexity of delivering enterprise services.

VMware Infrastructure products—ESX Server with Virtual SMP and VirtualCenter with VMotion—enable companies to implement large-scale production server consolidation, business continuity, and enterprise desktop solutions with enterprise-class performance, high availability, manageability and security. VMware ESX Server is software for partitioning, consolidating, and managing servers in mission-critical environments. Ideally suited for enterprise data centers, ESX Server minimizes the total cost of ownership of computing infrastructure by increasing resource utilization and maximizing administration flexibility.
**Audience**

This document is intended for Microsoft Windows and VMware system administrators and IT professionals. It is assumed that the reader has practical experiencing installing, configuring, and administering these environments.

**Overview**

This section provides a brief description on how EMC RepliStor can be used in conjunction with VMware to provide high availability or disaster recovery for your mission-critical data or facilitate a server migration or consolidation effort. Each scenario will be discussed in detail later.

EMC RepliStor asynchronously replicates data over TCP/IP while preserving write order. Copies or mirror images of Windows 2000 and 2003 application and user data are maintained on the target server to be reused for numerous purposes. As of version 6.0, RepliStor can be configured to replicate an entire system device, capturing all data changes between the boot and shutdown sequences without any conflict that may be associated with open files. This provides the ability to create an up-to-date replica of your system device on a remote target drive while it is in use and being updated or modified. For consolidation or disaster recovery purpose, these system device replicas can be virtualized and boot as virtual machines.

VMware provides the virtualization technology and tools that allow these replicated system device images to be restarted on a virtual server. Traditionally, in order to reuse a replica of a system device would require identical hardware because of the underlying physical dependencies stored in the registry. VMware removes these dependencies when the Physical to Virtual (P2V) utility virtualizes the physical image. In addition, the user can choose the target VMware architecture of their choice.

**Theory of operations**

The following section will provide an overview of the configurations discussed so far. Each configuration is described within its respective section.

**Providing high availability with EMC RepliStor and VMware**

EMC RepliStor provides a high availability function for servers running Windows 2000 or later through a feature called Alias failover. Used in conjunction with mirroring replication, this feature enables business continuity through a simple configuration process. In an Alias configuration, at least two servers are required, a source or production server and a target or standby server. Traditionally this meant two physical servers with dedicated roles of production and standby. Much like any clustered or high-availability solution, this means another physical server that sits idly until a failure occurs. With VMware, that same idle standby server can now be configured to serve several purposes. Since VMware partitions a physical server into multiple virtual servers, that same physical machine can now serve multiple functions. With adequate hardware resources, a VMware server hosting multiple guests can provide standby instances to protect the bulk of your application servers in addition to hosting other production or test servers as depicted in Figure 1.
Configuration requirements

This section outlines the specific configuration requirements for implementing RepliStor Alias failover along with best practices for ensuring a successful deployment. In this white paper, the term *source server* refers to the production server and *target server* refers to the standby server.

- Source and target servers are installed and configured according to Microsoft and VMware best practices.
- Both source server and target server must have the same version of Windows installed. This includes any service packs and hotfixes.
- Applications that are being protected should be installed in the same location on both the source server and target server. The application files or binaries should not be replicated; a standard installation should be performed on each system.
- Application data file paths, such as databases or log file locations, should be configured identically on both the source and target servers.
- Active Directory domain controllers should exist in both the source and target server locations if the application is dependent on Active Directory services to ensure updates succeed and lookups can be completed in a timely manner in the case of a site failure.
- DNS servers exist in network proximity to both the source and target servers. Providing an additional DNS server ensures that updates occurring as a result of failover will succeed in the case of a site failure.
- Administrator privileged account access is needed to perform Active Directory updates and DNS updates in secure DNS configurations. It is recommended that the RepliStor Server service be started with a sufficiently privileged account.

Installing and configuring EMC RepliStor for high availability

After ensuring the configuration requirements have been met, a minimum of RepliStor 6.0 or later is installed and licensed on both the source and target servers, according to the instructions provided in the *EMC RepliStor for Microsoft Windows Installation Guide*. Following the installation, replication and Alias parameters are defined. Prior to configuring and activating the Alias, the application services must be modified to allow RepliStor to control the starting and stopping of the service during failover and failback operations. From the services applet on the source and target servers set each of the relevant services to manual startup. In addition, these services should be stopped on the target server. The steps listed below outline the tasks that must be performed.
• Modify the appropriate services for the application that is being protected. Set these services to manual startup on both the source and target server. Ensure the services are shut down on the target server prior to beginning replication and activating the Alias.

• Create specifications to define the data that will be replicated from the source to the target server. A Group specification can be used to configure all data paths as one specification.

• Configure the Alias parameters that will be used to enable the failover functionality.
  ▪ Chose a unique network name as it will be registered in DNS to allow client connectivity to the hosted application regardless if source or target are active.
  ▪ If the source and target server are in the same subnet, you may optionally define a dedicated IP address for the Alias name. This IP address will be bound to the NIC of the active server and will transfer from server to server during failover and failback operations. This is optional for same subnet or LAN configurations.
  ▪ In a WAN configuration or different subnet configurations, CNAME records are created in DNS when the alias name is registered.
  ▪ Identify the services that must be restarted during the failover operation.
  ▪ Configure the action RepliStor will take when the source server resumes activity. There are two settings that are enabled by default that configure RepliStor to reverse the direction of the data replication and enable automatic synchronization from the target back to the source server to expedite the failback process.
  ▪ Determine whether the failover operations should be automated or manually activated. By default the failover operation is automated. Failback or removing the Alias is always a manual operation allowing the administrator to control and schedule the brief interruption to services that will occur.
  ▪ Optionally configure a failover agent. The failover agent is used to prevent split-brain conditions.

• Perform the initial synchronization of data.
• Activate the Alias once the source and target servers are in synchronized state.
• Once the configuration is complete, test the failover and failback operations.

Note: RepliStor provides Microsoft Exchange and SQL Server support modules that automate the configuration tasks outlined previously for these specific applications. Please refer to the EMC RepliStor for Microsoft Windows Administrator’s Guide for more information in these modules.

Creating the RepliStor specification
The process of creating the specifications identifies the data on the source server that will be replicated, assigns the desired location on the target server, and defines additional parameters such as attribute and permission preservation. The example below illustrates the specification creation. This is an example of a SQL Server data specification created from source server (LOSBD157) to target server (LOSBD158).

1. On the Source server, attach to the source server within the RepliStor Client.

2. Select Maintenance > Add Specification > File/Directory. The specification creation wizard will be displayed as shown in Figure 2.
3. After selecting all source drives/directories, add a description for the specification. Group specifications require a description.

4. Click Next to add the target to the specification.

A site list of available targets appears (Figure 3).

Figure 2. Select replication directories

Figure 3. Available targets list
5. Select the target from the list of available systems. Select **Same As Source** in the list box. Selecting **Same As Source** implies that the application data paths match from source to target server and that the target locations (drives) exist.

6. Click **Next** to select the replication options for the target site (Figure 4).

![Figure 4. Options](image)

7. Ensure the following options are selected in the **Options** dialog box (Figure 4):
   - In the **Mirroring Options** section, select:
     - **Protect Target Files** to set the files to read only on the target server
   - In the **Propagate** section, select:
     - **Attributes** to maintain file attributes from source to target
     - **From Shares** to replicate the additions and deletions of shares to the path
   - In the **Permissions as** section, select:
     - **Sids** to preserve Sids

8. Click **Next** to display the **Synchronization** dialog box (Figure 5).

9. **Incremental** and **Delete Orphans** are selected by default. Although **Incremental** is selected, a full synchronization will occur as it is the initial synchronization. **Delete Orphans** configures RepliStor to remove any files on the target server that do not exist on the source server.

10. Select **Yes** in **Synchronize Target** to start synchronization. Allow the specification to become fully synchronized before creating and activating the Alias.
Creating the RepliStor Alias
This section provides an example of creating an Alias to enable failover.

1. On the source server launch the RepliStor client. From the **Maintenance** menu select **Alias**. The screen in Figure 6 displays. Click **Add**.

![Figure 6. Alias Maintenance](image)
2. Enter a unique name in the **Alias** field and select the target from the **Target** list box (Figure 7). If manual failover is desired, select **Manual Activation on Target**. In addition, any scripts that may be required to perform actions prior to failover or failback can be specified in the **Commands:** **Adding Alias** and **Commands:** **Removing Alias** boxes.

![Figure 7. Add Computer Alias (Alias tab)](image)

3. Click the **IP Addresses** tab (Figure 8). Enter an IP address if the source and target servers are on the same subnet and then click **Add**. If this is a WAN configuration, leave this blank. For both LAN and WAN configurations, select **Add to DNS Servers** to register the IP or CNAME record in DNS for the Alias.

![Figure 8. Add Computer Alias (IP Addresses tab)](image)
4. Click the **Services** tab (Figure 9). Click **Add** to display a list of services that are available. Select the appropriate services to be restarted as part of the failover/failback operation.

![Figure 9. Add Computer Alias (Services tab)](image)

5. Select the **Target** tab (Figure 10). By default the **Transfer Specifications to Target** and **Auto-Synchronize** options are selected. These options facilitate failback by automatically reversing specification from target back to source and specifying that reverse synchronization starts once the source server is available on the network. In addition, notifications can be configured here. Click **OK**.

![Figure 10. Add Computer Alias (Target tab)](image)
6. The **Alias Maintenance** screen (Figure 11) displays again. Select **Activate Aliases** if you are ready to enable the Alias and click **OK**. If deferred activation is required, leave as is, click **OK**, and activate the Alias at a later time.

Figure 11. Alias Maintenance

7. Once the Alias has been activated, scheduled testing should be performed. This can be done by selecting the Alias and performing a **Manual Fail** as shown in Figure 12.

Figure 12. Manual Fail

8. Client applications should be modified to reflect the Alias name to ensure connectivity. For example, update the SQL client utility or Outlook profiles with the Alias name.
**Migrating or consolidating a physical server to VMware virtual servers**

This section provides details on how EMC RepliStor can be used to capture and replicate an entire server to a target location that can then be virtualized with VMware’s P2V utility. Once the virtualization has completed the devices can be presented to a VMware server and used to re-create the server as a virtual system. Figure 13 illustrates the configuration and data flow. In this example, ESX Server is used as the VMware target.

**Figure 13. Moving to a VMware server**

**Configuration requirements**

The section outlines some prerequisite requirements that enable operating system replication.

- RepliStor is installed on the source server to be migrated. It has been configured to enable loading the RepliStor driver early in the boot sequence.
- A target server has been identified, and RepliStor is installed. This system will be referred to as an Image Collector.
- Target devices for source server OS devices are formatted to contain boot sectors. This is required to enable the boot process and discussed in detail later.
- A third server is used to run P2V. This is known as the P2V helper machine. An additional server is needed because P2V has a limitation that allows only the first four LUNs to be seen by the P2V utility. Since the Image Collector will likely contain more than four LUNs, it cannot be used as the P2V helper.
- Target devices are easily provisioned to the Image Collector, P2V helper, and VMware server. A SAN environment is ideal for this configuration. Target devices should be easily presented to both servers via zoning and masking/unmasking.
- Optional: Create clones of the target disks to enable preserving of the real-time replica. If a clone is created, it can be presented to the P2V helper as shown in Figure 14.
Preparing target devices with boot sectors

RepliStor is capable of replicating only the data from the source server’s system device. The boot sectors are not replicated to the target devices. In order for the target device to be bootable it must contain pre-created boot sectors. There are several methods that can be used to create boot sectors on a disk. The user decides which method is most convenient. The list below offers some suggested methods:

- In a SAN environment where booting from SAN is already configured and hardware cloning capabilities are available, an existing boot device can be cloned to create boot sectors on other devices. This clone device would then be repeatedly cloned to create a sufficient amount of target devices. It would be a good idea to keep one extra device for future considerations. These cloned devices are then zoned to the Image Collector to be used for OS target disks only.

- If booting from SAN is not already in use, booting a server from the SAN to create a base installation of Windows will provide the necessary boot sectors. As above, this device can then be cloned with the hardware to produce multiple OS target devices. Refer to your HBA and array manufacturer’s documentation for information on booting Windows systems from a SAN.

- Use VMware to create a temporary virtual machine on a SAN LUN. When creating the temporary VM and selecting the virtual disk, select **System LUN/Disk** as shown in Figure 14 and Figure 15 to create the OS device on a physical disk. Select the appropriate device and set to physical compatibility mode.

- Use any third-party imaging product that can create boot sectors on a target device.

![Figure 14. Selecting Virtual Disk](image.png)
Presenting target devices to the Image Collector

Once the sufficient amount of devices containing boot sectors has been created, they should be zoned to the Image Collector and mounted. **Do not format these devices!** Formatting the disks will remove the boot sectors. Simply assign them a drive letter and descriptive label such as `servername_sysdisk`. These devices can now be used as RepliStor target devices for source server system disks.

Installing and configuring EMC RepliStor

Install and license EMC RepliStor on the source server and Image Collector following the instructions in the *EMC RepliStor for Microsoft Windows Installation Guide*. Once the installation completes configure RepliStor to enable boot load of the driver and create specifications for the data to be replicated.

**Enabling RepliStor boot load and configuring replication**

On the source server launch the RepliStor client to enable the boot loading of the RepliStor driver.

1. From the **Maintenance** menu select **Options** and click the **Advanced** tab. Select **Boot Load Driver** as shown in Figure 16. Click **OK**.
2. Reboot the system. Rebooting the system will guarantee that all data is being captured from boot to shut down in the event that the specification is set up for a long period of time before the actual migration occurs.

3. Create a specification for the system device. Select the entire C: drive (system device) as the source. Select the corresponding target device that was created following the directions in “Preparing target devices with boot sectors.” Select the appropriate mirror options for the device. Refer to the *EMC RepliStor for Microsoft Windows Administrator’s Guide* or online help for a complete description of each mirror option.

4. Create additional specification for the rest of the data drives. The target devices for these do not need to contain boot sectors.

Converting the physical OS replica to a virtual machine

This section addresses the tasks that must be performed to convert the replica of the source server’s system device into a virtual machine. To ensure that the replica is up to date, a planned outage should be scheduled to perform this task and complete the migration to the virtual server. Before proceeding ensure that all specifications are completely synchronized.

- Shut down the source server.
- On the target server (Image Collector), unmount the target drives that will be presented to the virtual machine by removing their drive letters via the disk management applet.
- If you elected to create clones of your replicas, split or facture them.
- Via zoning or masking, remove access to the replicated devices for the system that is being migrated.
- Via zoning or masking, add access to the device (or clone) that contains the source server’s OS replica to the P2V helper.
- On the P2V server reboot or rescan disks from the disk management applet to see the newly presented disk. Note: P2V has a limitation where it can access only the first four physical disks. Ensure that your disk is presented in the first four addresses.
- Launch P2V.
- Via zoning or masking present the virtualized device and the additional data devices from the source server to the ESX Server.
- Rescan disks on the ESX Server.
- Create the new virtual machine on the ESX Server.

Running P2V on the helper machine
This section provides some examples of the P2V process. Please refer VMware’s P2V Assistant User’s Manual for more information on using P2V.

1. Ensure that the device is visible on the P2V helper machine and that it appears in the first four disks. Launch P2V (Figure 17). Select **Perform a System Reconfiguration…** and click **Next**.

   ![Figure 17. Select a task](image)

   **Figure 17. Select a task**

   2. The **Select a Target Disk** screen appears as shown in Figure 18. Click **Select**.

      ![Figure 18. Select a target disk](image)

      **Figure 18. Select a target disk**
3. Select the appropriate target device from the list presented (Figure 19).

![Figure 19. Disk Device Selector](image)

4. Note that the disk now appears in Selected disk number (Figure 20). Click Next.

![Figure 20. Selected disk number](image)

5. The volume that you selected displays (Figure 21) along with the operating system information. Click Next.
6. Choose the VMware host version and number of CPUs (Figure 22). Click Next.

![Figure 22. Select the target VMware product](image)

7. Confirm that you want to continue with the conversion (Figure 23) and click Next.

![Figure 23. Commit the operation](image)
8. The summary screen appears (Figure 24). Click **Finish** to exit.

![Summary screen](image)

**Figure 24. Summary screen**

**Creating the virtual machine**

Now that the source server OS device has been virtualized, it can be presented to the ESX Server and a virtual machine (VM) can be created. Follow the steps below to add the new VM:

- Via zoning, remove access to the virtual OS device from the P2V helper.
- Via zoning, add access to all the disks needed to re-create the VM to the ESX Server. This includes the new virtualized OS device and all data devices.
- From the ESX console under Storage Management, rescan the storage to add the new devices. Note the new device numbers.
- Create a new VM using the System LUN/Disk option to use a physical device and set compatibility to physical mode.
- Modify the newly created VM to add the additional data disks as physical devices. Note that the devices will need to be modified to have the same drive letters they had on the physical machine. This will not happen automatically.
- Power on the VM.
- Plug and Play will detect new hardware and require a reboot. Reboot the VM.
- Install the VMware tools as documented in the *VMware ESX Server 2.5 Administration Guide* and reboot the VM.
- Configure the network with the proper IP address. Note: IP configuration information is bound to the original NIC card’s MAC address and is not automatically enabled. In fact, the current server’s NIC cards will appear to be in addition to the original server’s configuration and will not appear as “local area connection 1”. A warning message about duplicate IPs will appear. These can be ignored.
- Reassign drive letters to their original settings.
**Disaster recovery options**

Using the same configuration as the migration/consolidation solution can provide an alternative to disaster recovery. When an outage occurs, the physical server’s image is virtualized and a VM is created to replace the original physical server. Recovering back to the original server requires a mechanism to convert Virtual to Physical. VMware does not provide a tool that can perform this with a single operation like P2V. However, they have published processes that can be used to revert a virtual server to a physical server. In addition, there are third-party products available to perform the same operation. For more information on Virtual to Physical conversion refer to VMware’s *Virtual Machine to Physical Machine Migration* tech note or contact VMware Professional Services.

**Conclusion**

IT organizations are responsible for maintaining server uptime and sustaining user productivity. These tasks can be challenging given that most solutions that can provide high availability are complex and costly. EMC RepliStor in conjunction with VMware offers a simple solution that eliminates costly hardware requirements. By leveraging VMware’s virtualization technology, one server can be provisioned to protect multiple physical servers in a high availability or disaster recovery configuration.

Migrating or consolidating legacy servers to a VMware platform to centralize operations or reduce costs is becoming a common practice. Traditional methods that involve tape backups can not provide up-to-the-minute data coverage. Other solutions such as array-to-array replication can be costly and are useless where there is internal disk. EMC RepliStor is hardware-agnostic and can replicate data regardless of the source data’s underlying storage. By capturing the data continuously, the target location will always have an update copy of the data unlike tape backups. With proper planning and coordination, a minimal amount of downtime is required to complete the migration process.

**References**

- EMC RepliStor for Microsoft Windows Administrator’s Guide
- EMC RepliStor for Microsoft Windows Installation Guide
- EMC RepliStor for Microsoft Windows Release Notes
- VMware P2V Assistant 2.1.1 User’s Manual
- VMware ESX Server 2.5 Administration Guide
- VMware ESX Server 2.5 Installation Guide
- VMware ESX Server 2.5 Release Note
- VMware Guest Operating System Installation Guide
- VMware ESX Server SAN Configuration Guide