

# Microsoft SharePoint 2010 on VMware Availability and Recovery Options

© 2011 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. This product is covered by one or more patents listed at <http://www.vmware.com/download/patents.html>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.  
3401 Hillview Ave  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

## Contents

1. Introduction .....	6
2. SharePoint 2010 on VMware vSphere .....	7
3. High Availability Options .....	8
3.1 Protecting the Web and Application Server Roles .....	8
3.2 Protecting the Database Server Roles .....	9
4. Disaster Recovery Options .....	14
4.1 Warm Standby with Virtual Machine Images .....	14
4.2 SQL Server Log Shipping or Asynchronous Database Mirroring .....	14
4.3 Using VMware Site Recovery Manager (SRM) .....	15
5. Backup and Recovery Options.....	17
5.1 What to Back Up .....	17
5.2 SharePoint Native Backup and Recovery.....	17
5.3 System Center Data Protection Manager 2010 .....	19
5.4 VMware Data Recovery .....	19
6. Best Practices .....	20
6.1 Using VMware DRS Affinity and Anti-Affinity .....	20
6.2 Best practices for VMware Site Recovery Manager .....	21
6.3 SQL Server Alias for Greater Flexibility .....	21
7. Conclusion .....	23

## List of Figures

Figure 1. SharePoint 2010 Server Farm Architecture.....	7
Figure 2. Web and Application Server High Availability.....	9
Figure 3. VMware HA and SharePoint 2010.....	10
Figure 4. High Availability with Symantec ApplicationHA .....	11
Figure 5. VMware HA and Database Mirroring.....	12
Figure 6. VMware HA and Failover Clustering.....	13
Figure 7. SharePoint 2010 DR Using SRM.....	16
Figure 8. SharePoint Components.....	17
Figure 9. VMware Data Recovery.....	19



## 1. Introduction

When planning a SharePoint 2010 server farm deployment, defining measures to provide system availability and redundancy is a very important step. With the right availability architecture, critical elements of your SharePoint 2010 deployment can withstand various failure modes that might otherwise affect users accessing SharePoint services.

Traditional availability options for SharePoint using failover clustering, database mirroring, and SQL Server log shipping are complex and costly to implement and maintain. Features of the VMware vSphere® platform can enhance the overall availability of the SharePoint 2010 environment by providing options that limit both planned and unplanned downtime. For many organizations, the features provided by vSphere may satisfy the availability requirements of their business without having to follow traditional approaches. For other organizations that require a greater degree of availability, traditional approaches can be combined with the vSphere features to create an extremely flexible environment, with options for failover and recovery at both the hardware and software levels. Some of the advantages of the VMware vSphere platform include:

- VMware High Availability (HA) – If a physical server or any critical component within the server fails for any reason, VMware HA automatically reboots the virtual machine on another physical server, acting as a first line of defense against service outage.
- Virtual machine portability – A virtual machine is not bound to a particular piece of hardware. This can enhance availability in a couple of ways:
  - Design decisions are no longer permanent, that is, CPU and memory can be adjusted on a running virtual machine (VM) with VMware HotAdd as the resource demand increases.
  - More flexibility – VMware vSphere® vMotion® enables live migration of virtual machines from one physical server to another without service interruption. If a physical host requires service, vMotion can live migrate virtual machines to another host without affecting database availability.
- VMware vSphere Distributed Resource Scheduler (DRS) can balance workloads and speed recovery – VMware DRS is vMotion with intelligence. As application workloads increase, DRS can move a bottlenecked virtual machine to another host with more available resources automatically and without downtime. VMware DRS can also help to recover more quickly after server hardware failure. For example, if a physical server fails, VMware HA reboots the virtual machine on another physical server. When the failed server is replaced, DRS migrates the virtual machine back to its original location with no downtime and no interruption to the end-user.
- Symantec ApplicationHA – An agent-based high availability technology that protects against application failure. Symantec ApplicationHA is fully integrated with VMware HA and VMware vCenter Server™. Symantec ApplicationHA protects against hardware and application failures. Go to <http://go.symantec.com/applicationha/> for more information about Symantec ApplicationHA.

This document describes various options to provide SharePoint server farm availability in a virtualized environment using VMware vSphere® high availability features.

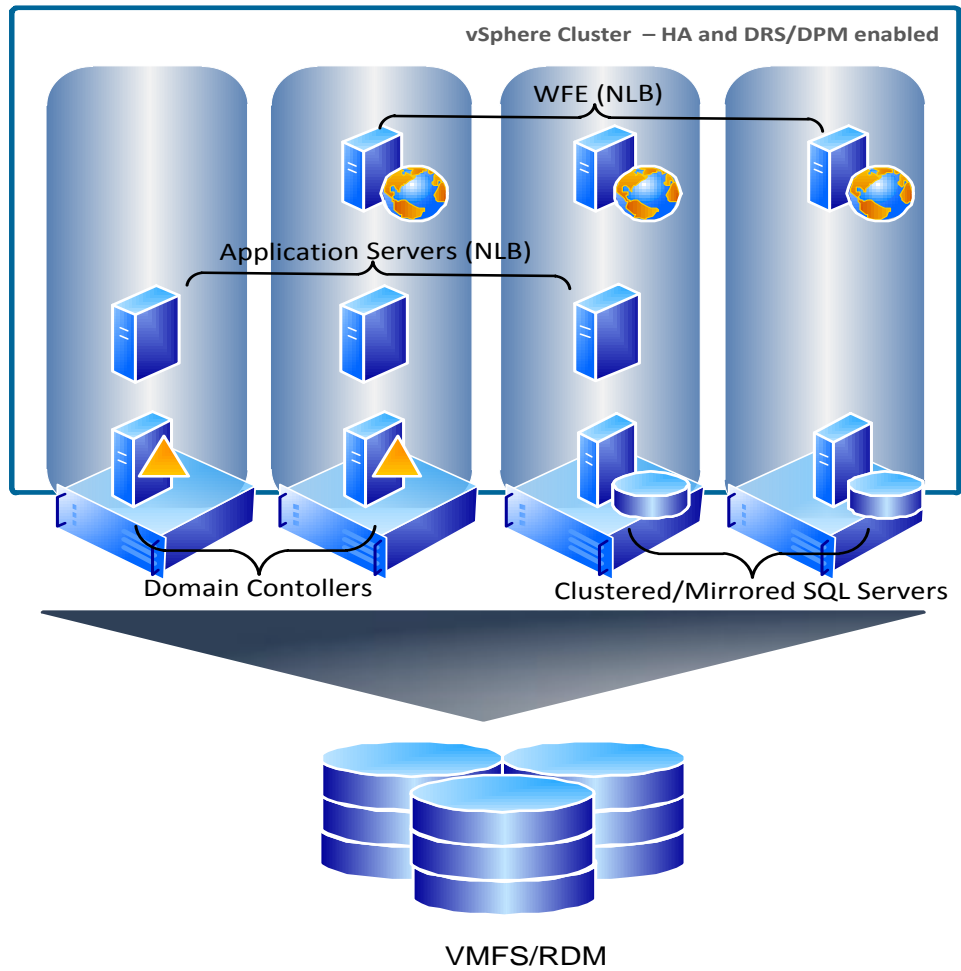
Before choosing any one option, evaluate your own business requirements to determine which solutions best meets your specific needs. To define business requirements, determine the followings for your SharePoint 2010 environment:

- Recovery point objective (RPO) describes the acceptable amount of data loss measured in time. It defines how much data an organization can afford to lose in a disaster situation.
- Recovery time objective (RTO) is the duration of time that a service level recovery requires after a disaster. It is determined by the time the business can afford for the site or service to be unavailable.
- Recovery level objective (RLO) is the objective that defines the granularity with which you must be able to recover data—whether you must be able to recover the whole server farm, Web application, site collection, site, list or library, or item.

## 2. SharePoint 2010 on VMware vSphere

The following diagram shows a typical SharePoint 2010 server farm deployment on VMware vSphere.

**Figure 1. SharePoint 2010 Server Farm Architecture**



## 3. High Availability Options

Availability is the degree to which a system is accessible by users. The degree of availability is impacted by both planned and unplanned downtime. For a highly available SharePoint 2010 server farm, all server roles (Web server, application server, database server) must be protected from hardware and software failures or maintenance downtime.

### 3.1 Protecting the Web and Application Server Roles

SharePoint 2010 supports running Web server and application server roles on multiple servers. Deploying multiple Web server roles and application server roles across VMware ESX® or VMware ESXi™ host clusters is the preferred way to provide basic availability and scalability. Software or hardware load balancers are supported for load distribution and balancing.

#### 3.1.1 Using VMware HA, DRS and vMotion

VMware HA, DRS, and vMotion can improve SharePoint 2010 Web server and application server role availabilities by avoiding planned and unplanned down time.

- If the physical host on which a SharePoint 2010 Web server and/or application server virtual machines are running must be patched, serviced, or rebooted, the virtual machines can be live migrated to another host in the ESX/ESXi cluster using vMotion without interruption of service.
- In an unplanned scenario, if the physical host on which SharePoint 2010 Web server or application server virtual machines are running fails, VMware HA automatically reboots the virtual machines and brings them back online on other available ESX/ESXi hosts.
- If any Web server or application server virtual machine fails due to blue screen, VMware HA detects and reboots the virtual machine.
- When a physically host is saturated and low available resources are affecting system performance and availability, VMware DRS monitors and detects the condition and proactively balances the load by moving virtual machines to other ESX/ESXi hosts with available resources without interrupting SharePoint services.

#### 3.1.2 Native Protection in SharePoint Search

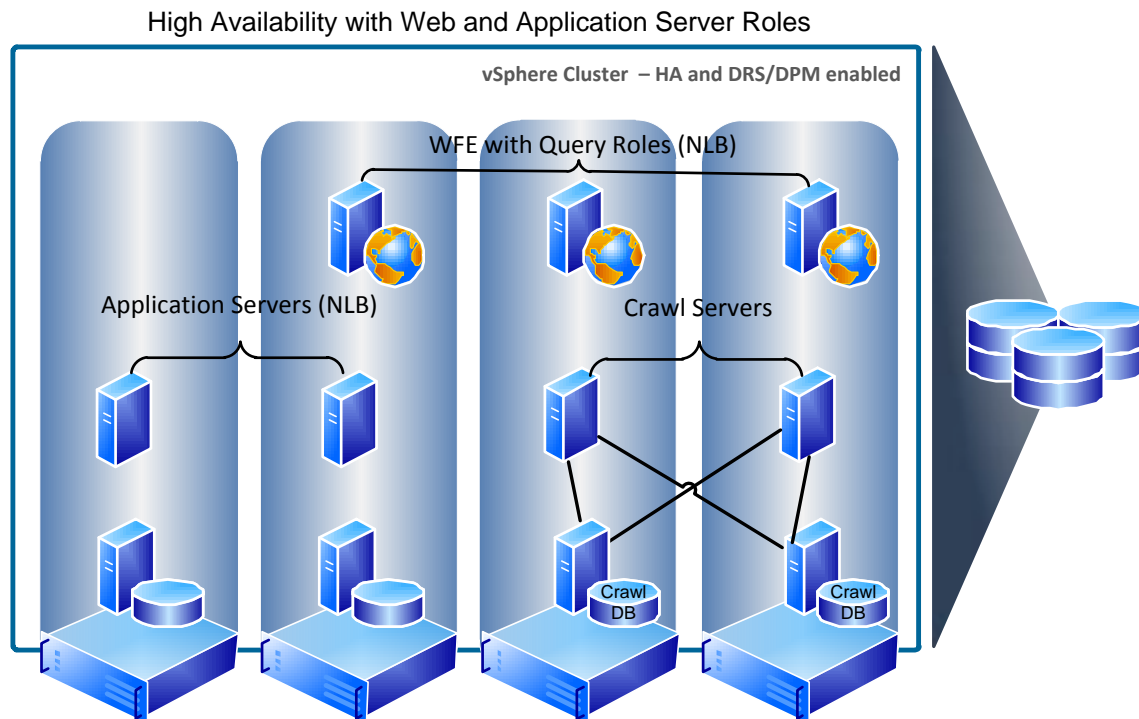
The SharePoint search service application is a special case for redundancy within a server farm. SharePoint 2010 search architecture improves availability and scalability of the crawl and query components compared with SharePoint 2007.

The Search service application consists of the following:

- Crawl servers crawl and propagate the indexes on the query server and update the property stores on the SQL server. In SharePoint 2010, the crawl server no longer stores a copy of index files. They are propagated to the query components during the crawl operation. Because of this, the crawler server is no longer a single point of failure. For redundancy, SharePoint recommends at least two crawl components.
- In SharePoint 2010, each of the query servers holds a subset of the content index files. The property store is the authoritative source for all indexed content properties and does not need to be synchronized with the crawl servers.

The query components can scale out to two or more partitions for load balancing and high availability. Each query component can hold a mirror of other index partitions for redundancy and availability consideration.

**Figure 2. Web and Application Server High Availability**



For more information on scaling and sizing search architecture for the SharePoint Server 2010 server farm, see the Microsoft article *Plan the topology for enterprise search (SharePoint Server 2010)* <http://technet.microsoft.com/en-us/library/gg502595.aspx>.

## 3.2 Protecting the Database Server Roles

SharePoint 2010 database availability requirements can be met to varying degrees by using VMware high availability features, such as VMware HA, vMotion, and DRS, or SQL Server native features, such as database mirroring or failover clustering. To get the best use of both, you can combine many of the VMware features with SQL Server native high availability features to achieve better protection and more flexibility in deployment.

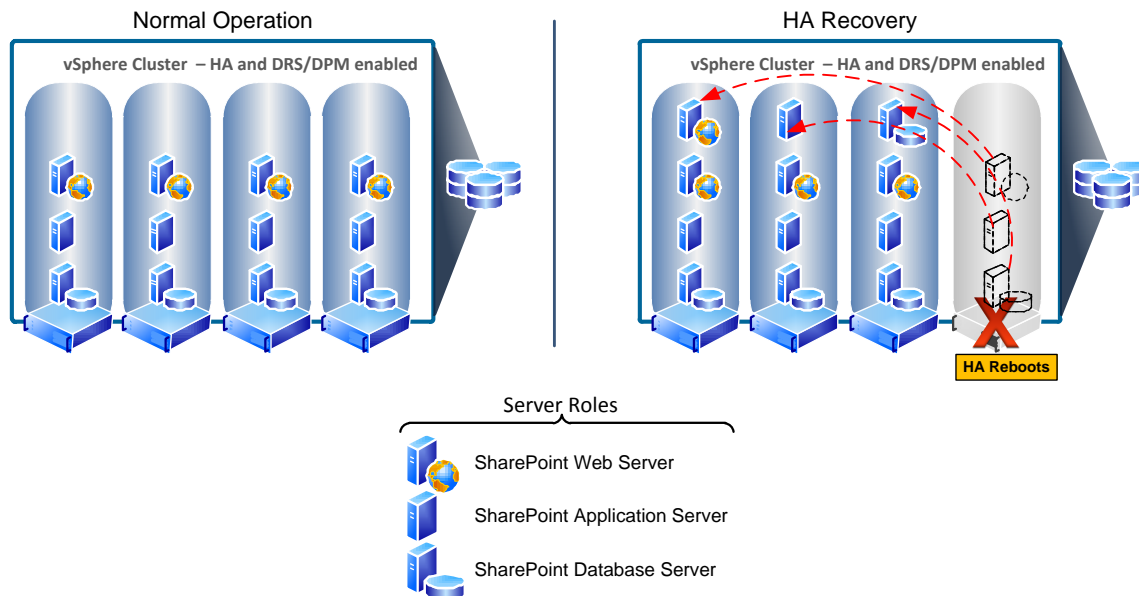
### 3.2.1 Protecting with VMware HA/vMotion/DRS

VMware vSphere with HA/vMotion/DRS provides high availability and host-level protection against hardware failure. VMware HA provides high availability for virtual machines by pooling them and the hosts they reside on into a cluster. Hosts in the cluster are monitored, and if a failure is detected, the virtual machines on a failed host are restarted on alternate hosts.

Use VMware HA when your business requirements determine that you require minimal downtime without tackling the complexities of configuring failover clustering or database mirroring. VMware HA enables you recover from host outages by restarting SharePoint 2010 SQL Server virtual machines on other running nodes in a VMware HA/DRS cluster. Crash consistency of the database is maintained during a host outage.

Using VMware HA with DRS facilitates automatic restart of virtual machines as well as intelligent load balancing of the entire HA/DRS cluster. After a host failure, the virtual machines that were running on that host are automatically restarted on another host in the cluster. During the restart of the virtual machines, DRS dynamically rebalances the cluster by intelligently relocating the virtual machines, effectively optimizing the cluster resource utilization, all while providing the required resources to the virtual machines.

Figure 3. VMware HA and SharePoint 2010



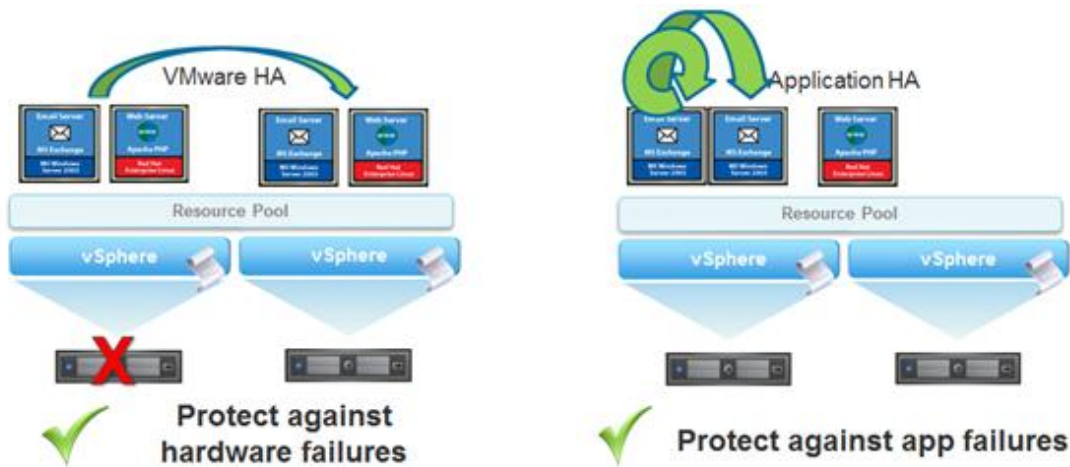
VMware vMotion leverages the complete virtualization of servers, storage, and networking to move a running virtual machine from one physical server to another. This migration is performed with no impact to running workloads or connected users. During a vMotion migration, the active memory and execution state of the virtual machine is rapidly transmitted over the network to the new physical server, all while maintaining its network identity and connections.

Note however that VMware HA/DRS does not provide application-aware monitoring and only protects against hardware failures.

### 3.2.2 Protecting with Symantec ApplicationHA

With vSphere 4.1, VMware introduced an application programming interface (API) that allows third party vendors to develop agents that can monitor the health of an application running within the guest and inform VMware HA when a problem is detected. Symantec is the first partner to develop such an agent for providing application awareness within a vSphere cluster. Symantec ApplicationHA provides monitoring capabilities for applications running inside virtual machines. Symantec ApplicationHA agent runs inside an SQL Server virtual machine to monitor the health of SQL Server resources. If a configured SQL Server instance or associated services become unavailable, the agent automatically detects it and tries to start the SQL Server services for a configurable number of attempts. If the SQL Server services fail to start, the agent considers this to be an application failure and reports the status to VMware HA. VMware HA can then restart the virtual machine. After the virtual machine restarts, the agent starts the application services and brings the configured resources online on the system.

Figure 4. High Availability with Symantec ApplicationHA



App-aware HA bridges the gap with app-level clustering

- > Automated availability for both hardware and software failures
- > 3<sup>rd</sup> party agents detect application and OS failures (eg Symantec ApplicationHA)
- > Invoke VMware HA through "Application Health Monitoring API"

Traditional solutions that protect SQL Server from hardware and software failures such as failover clustering or database mirroring require twice or more servers, storage resources, and software licenses. ApplicationHA is a great complementary solution to VMware HA. ApplicationHA monitors and protects applications from software failure, in addition to the hardware failure protection VMware HA provides, without the cost of redundant hardware/software. Symantec ApplicationHA can recover an SQL Server in as less as one minute. If your system can tolerate a limited amount of down time, ApplicationHA is a good, low-cost alternative that is easy to deploy and which is fully manageable from vCenter.

### 3.2.3 Protecting with VMware HA, vMotion, and Database Mirroring

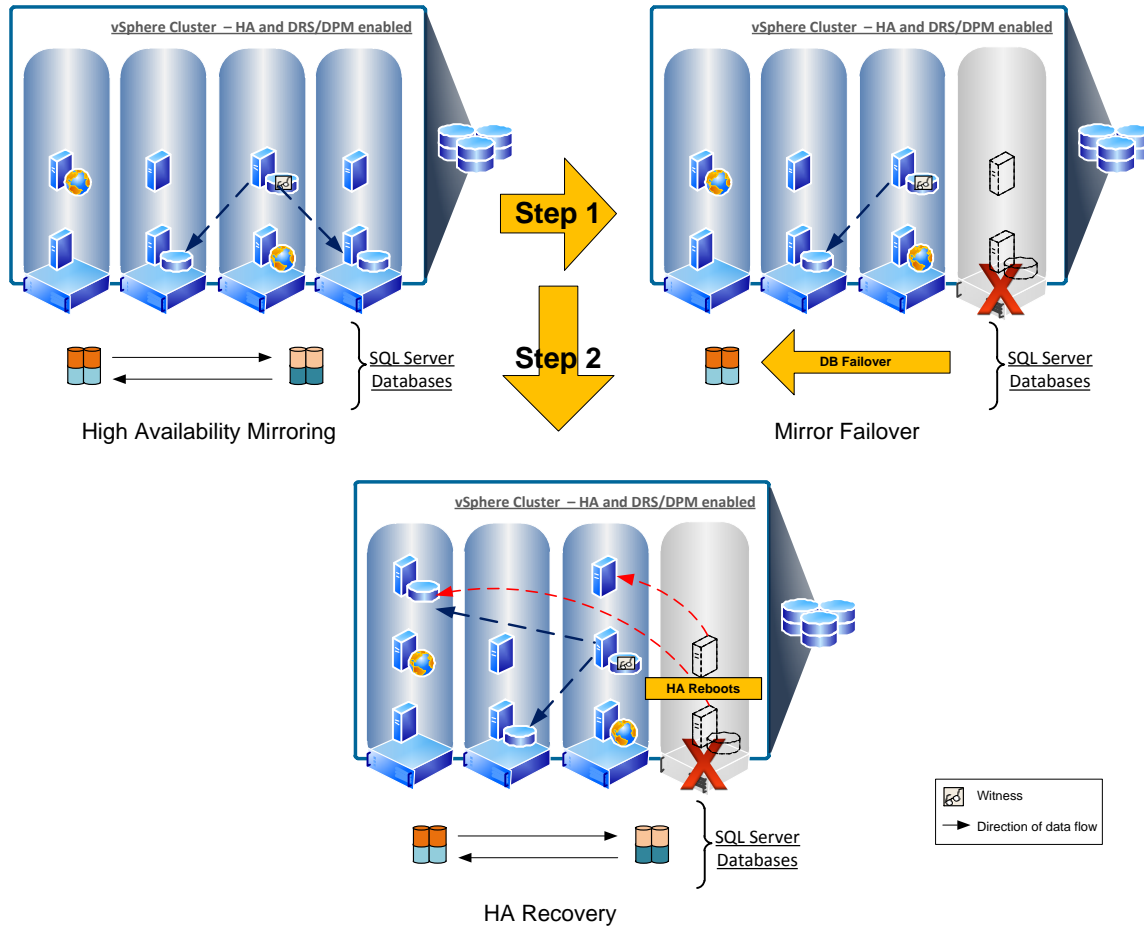
Database mirroring is an SQL Server technology that can deliver database redundancy on a per-database basis. In database mirroring, transaction log streams are sent directly from a principal database to the mirror database and applied to the mirror database. For mirroring within a SharePoint Server farm, you must use high-availability mirroring, also known as high-safety mode with automatic failover. In high availability mode, if the principal server fails, the mirror server forms a quorum with the witness server, and automatically fails over to the mirror server. Failover from the principal database to the mirror database typically takes several seconds.

A change from previous versions is that SharePoint 2010 is mirroring-aware. After you have configured a database mirror instance of SQL Server, you then use SharePoint Central Administration or Windows PowerShell cmdlets to identify the failover (mirror) database server location for a configuration database, content database, or service application database. Setting a failover database location adds a parameter to the connection string that SharePoint Server uses to connect to SQL Server. If there is an SQL Server time-out event, the following occurs:

- The witness server that is configured for SQL Server mirroring automatically swaps the roles of the primary and mirror databases.
- SharePoint Server automatically tries to contact the server that is specified as the failover database.

Within a SharePoint 2010 server farm, mirroring can provide redundancy for the content and configuration databases, and for many service databases. Even if your databases are mirrored to the same server, each database fails over individually. The following figure shows how mirroring is configured to provide availability within a SharePoint Foundation 2010 server farm.

**Figure 5. VMware HA and Database Mirroring**



For more information on configuration database mirroring for SharePoint 2010, see the Microsoft article *Configure availability by using SQL Server database mirroring (SharePoint Foundation 2010)* at <http://technet.microsoft.com/en-us/library/ff628961.aspx>.

SQL Server supports a maximum of two nodes in database mirroring. Any planned or unplanned downtime for the physical server a mirroring node runs on, for example, a BIOS upgrade, or a bad network card, can interrupt the mirroring session, and leave the database unprotected for an extensive period of time.

VMware HA and vMotion can be used as complementary technologies to increase availability of SharePoint 2010 databases that participate in a database mirroring session.

With planned maintenance, vMotion can live migrate a SQL Server virtual machine from one physical server to another without service interruption. vMotion uses the VMware cluster file system to control access to a virtual machine's storage. During a vMotion migration, the active memory and precise execution state of a virtual machine is rapidly transmitted over a high speed network from one physical server to another, and access to the virtual machine's disk storage is instantly switched to the new physical host. Because the network is also virtualized by the VMware host, the virtual machine retains its network identity and connections, resulting in a seamless migration process.

If an unexpected physical host failure occurs, VMware HA can automatically reboot virtual machines onto other running hosts; allow database mirroring session to resume without waiting for the failed physical server to be serviced.

Using vMotion reduces the need to fail over a mirroring session to service hardware. VMware HA enables continuous mirroring by reducing the time spent on recovering from a partner being down.

### 3.2.4 Protecting with VMware HA and Failover Clustering

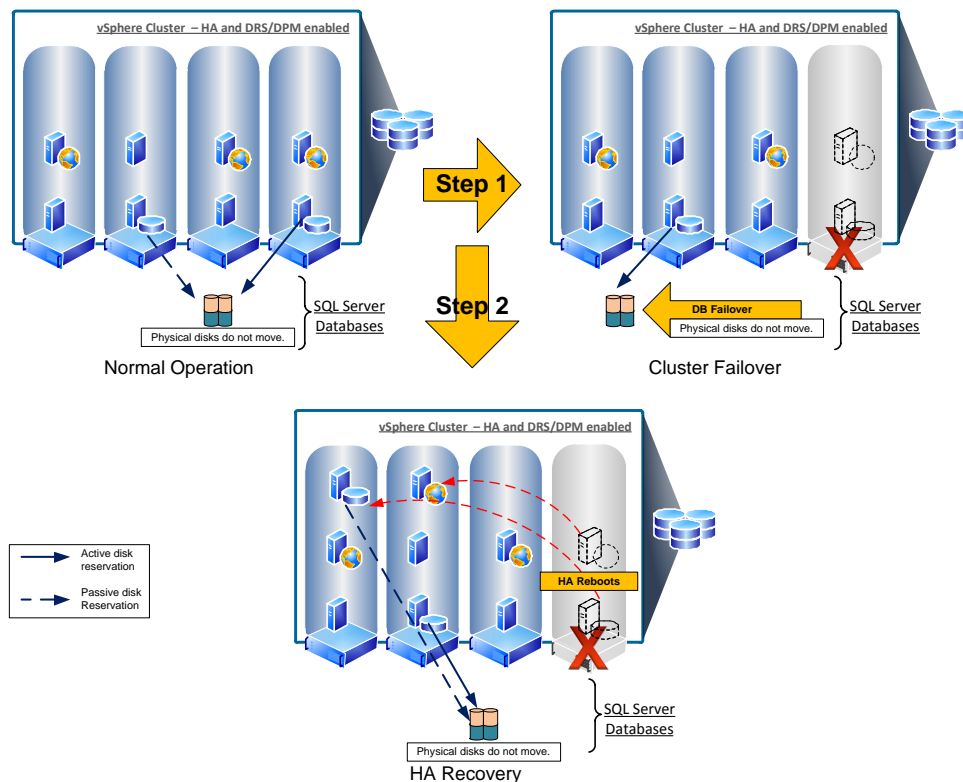
SQL Server failover clustering protects SQL Server database instance from hardware and software failure by using a cluster of servers, known as nodes, which share the same disk resources. One node is active and owns the database instance. If the node fails, another node in the cluster takes ownership of the database instance and continues to serve users. A failover cluster instance appears as a single computer, but has functionality that provides failover from one node to another if the current node becomes unavailable.

SharePoint Server references the cluster as a whole; therefore, failover is automatic and seamless from the perspective of SharePoint Server.

VMware supports two-node SQL Server failover clusters. If one of the nodes is down due to hardware failure or routine maintenance of hardware, the SQL Server environment is not protected until the hardware service is done and the server is back online. At this time, the SQL Server environment is vulnerable to further failure. For more information on failover cluster setup on VMware, see *Setup for Failover Clustering and Microsoft Cluster Service* at [http://www.vmware.com/pdf/vsphere4/r41/vsp\\_41\\_mscs.pdf](http://www.vmware.com/pdf/vsphere4/r41/vsp_41_mscs.pdf).

VMware HA provides protection against physical server failure. If there is a physical server failure, the affected virtual machines are automatically restarted on another physical server in the VMware cluster. Additionally, if there is an OS-related failure within a virtual machine, the failure is detected by VMware HA and the affected virtual machine is restarted on the same physical server.

Figure 6. VMware HA and Failover Clustering



## 4. Disaster Recovery Options

Disaster recovery is the ability to recover from a situation in which a data center that hosts SharePoint Server becomes unavailable. Virtualization offers inherent advantages when it comes to disaster recovery. VMware creates a layer of abstraction between the resources required by an application and operating system, and the underlying hardware that provides those resources. Decoupling the operating system and applications from the underlying hardware eliminates the need to recover the actual physical server on which an application was running. With SharePoint 2010 running on the VMware platform, there are many options to provide disaster recovery for the SharePoint server farm.

### 4.1 Warm Standby with Virtual Machine Images

Because VMware encapsulates systems into files, you can take advantage of file-based techniques, such as clones, snapshots, and replicas, to create a secondary DR site. See Backup and Recovery Options on page 17 for more information.

In a warm standby disaster recovery scenario, you can create a warm standby solution by consistently and frequently creating virtual images of the servers in your server farm that you ship to a secondary location. At the secondary location, you must have an environment available in which you can easily configure and connect the images to re-create your server farm environment.

### 4.2 SQL Server Log Shipping or Asynchronous Database Mirroring

You can configure a SharePoint 2010 DR server farm using SQL Server log shipping or asynchronous database mirroring for SharePoint databases. Log shipping and asynchronous database mirroring provide redundancy for content databases.

Log shipping enables you to configure SQL Server to continually send transaction log backups from a primary database on a primary server instance to one or more secondary databases on separate secondary server instances. The transaction log backups are applied to each secondary database individually. Continually backing up the transaction logs from a primary database, then copying and restoring them to a secondary database, keeps the secondary database almost synchronized with the primary database.

With asynchronous database mirroring (high-performance mode), as soon as the principal server sends the log for a transaction to the mirror server, the principal server sends a confirmation to the client without waiting for an acknowledgement from the mirror server. Transactions commit without waiting for the mirror server to write the log to disk. Using asynchronous mirroring, the principal server runs with minimum transaction latency. The mirror server attempts to keep up with the log records sent by the principal server, but the mirror database might lag behind the principal database. If a failure occurs, there is a possibility of data loss. Asynchronous database mirroring only allows forced failover.

SQL Server log shipping or asynchronous database mirroring cannot be used for the following databases:

- Configuration database and Central Administration content database. The configuration database and the Central Administration content database cannot be restored or moved to another location because they contain location-specific references and must be rebuilt.
- Service application databases when the Service application is running search. Search requires complete synchronization between the search databases and index. To provide up-to-date search on a failover server farm, you must run search on the secondary server farm.

For more information, see the Microsoft article *Plan for disaster recovery (SharePoint Server 2010)* at <http://technet.microsoft.com/en-us/library/ff628971.aspx>.

Disaster Recovery Method	Pros	Cons
Log shipping	Multiple secondary databases. With scheduled jobs database, corruption can be avoided.	Minimum log ship frequency is 10 seconds. More steps are required for manual failover.
Asynchronous database mirroring	Easy setup and maintenance. Fast and easy failover. Using connection strings, you can make your application mirroring aware or using SQL alias.	Database mirroring is configured per database, not per SQL server instance. No multiple secondaries.

For detailed steps to configure SharePoint 2010 DR farm using SQL Server log shipping or asynchronous database mirroring, see *Configure Disaster Recovery Farm with SharePoint 2010* <http://blogs.technet.com/b/mahesm/archive/2010/04/30/configure-disaster-recovery-farm-with-sharepoint-2010.aspx>.

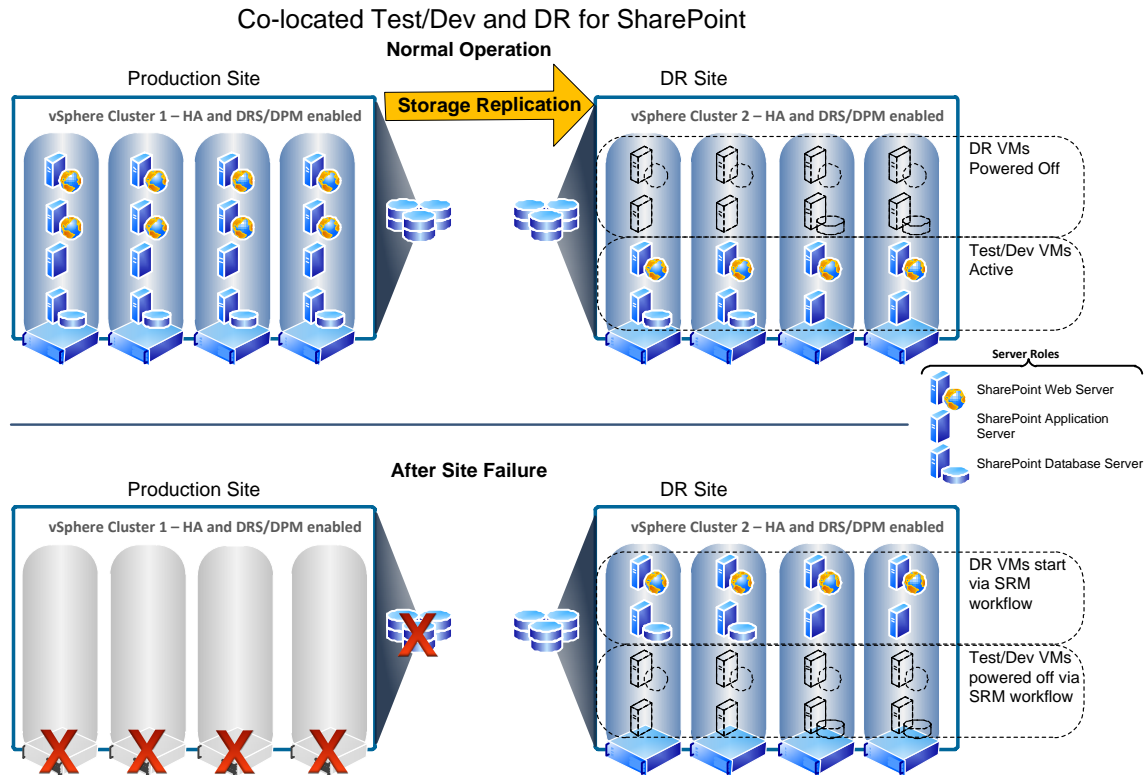
### 4.3 Using VMware Site Recovery Manager (SRM)

Traditional disaster recovery has been complex and costly to implement. Attempting to restore a SharePoint server farm in an alternate location, including SQL Servers requires many steps. Testing a failover scenario is disruptive to the production environment, and requires careful planning and scheduling.

VMware vCenter Site Recovery Manager™ makes disaster recovery rapid, reliable, manageable, and affordable. SRM is a suite of tools that help to automate and test a disaster recovery plan. SRM works by integrating tightly with storage array-based replication. Most of the major storage vendors have made their products compatible with SRM.

Testing the DR plan is one of the major challenges of DR. Typically, it is not performed often enough, and sometimes not at all. SRM allows you to perform a non-disruptive failover test to your remote site and revise and fine-tune your DR plan as necessary. IP addresses of the virtual machines in the remote site can be automatically reconfigured with IP addresses that match the IP scheme of the remote DR site. The failover plan can be executed with a single click that launches user-defined scripts during the recovery process. SRM can automate a series of complex manual steps to simplify the failover process. SRM can even assist with the failback process, which can be as complicated as the original failover.

Figure 7. SharePoint 2010 DR Using SRM



For a sample solution case study of using SRM with SharePoint 2010, see the EMC whitepaper *EMC Continuous Protection for Virtualized SharePoint 2010 Farms: A Detailed Review*  
<http://www.emc.com/collateral/software/white-papers/h8139-protection-virtualized-sharepoint-wp.pdf>.

## 5. Backup and Recovery Options

There are many options to backup and recover a SharePoint 2010 environment suitable to your RPO, RTO, and RLO requirements. The feature set available when deployed in a virtual environment is no different than what is available with a physical deployment. VMware virtualization makes additional options available for backing up entire virtual machines.

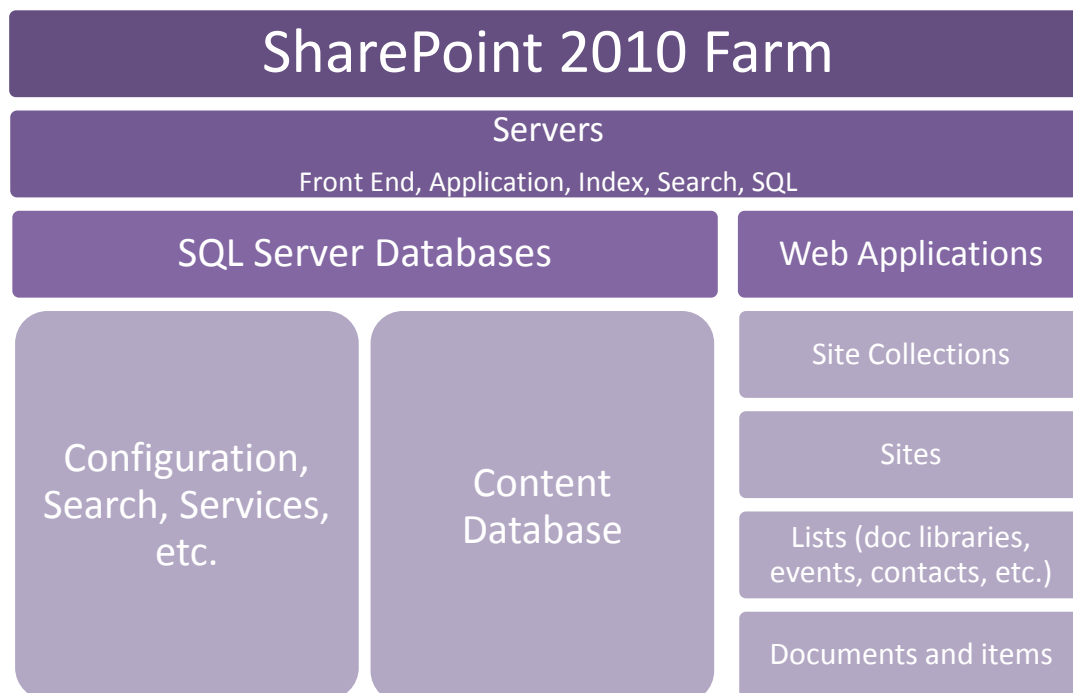
### 5.1 What to Back Up

A SharePoint 2010 environment consists of many types of components and data. Consider the following as part of a complete backup and recovery strategy:

- All databases
- Index files
- Configurations (Web applications, service applications)
- IIS settings
- Customizations

Figure 8 illustrates how data is stored in the SharePoint 2010 environment.

**Figure 8. SharePoint Components**



### 5.2 SharePoint Native Backup and Recovery

SharePoint 2010 provides an out-of-box backup and recovery tool that enables you to backup and recover a SharePoint environment at different granularity levels. You can back up all or part of the server farm, even down to single lists. You can specify whether to run a full or differential backup, and whether to back up only the configuration settings or also add the content databases. You can use the SharePoint 2010 Central Administration UI or Windows PowerShell scripts to perform the backup.

## 5.2.1 Server Farm Backup

SharePoint Server 2010 starts an SQL Server backup of content and service application databases, writes configuration content to files, and backs up the search index files and synchronizes them with the search database backups.

## 5.2.2 Granular Backup

The following table shows the different backup options. For details of performing backups at different granularity level, follow the hyperlinks to the corresponding Microsoft TechNet articles.

Granularity	Protection
Back up a server farm	Allow restoration of data losses that might occur from problems such as hardware failure or power outages. <a href="http://technet.microsoft.com/library/ee428316(office.14).aspx">http://technet.microsoft.com/library/ee428316(office.14).aspx</a>
Back up a Web application	Make Web application-related data and configuration available for recovery. <a href="http://technet.microsoft.com/library/ee748650(office.14).aspx">http://technet.microsoft.com/library/ee748650(office.14).aspx</a>
Back up a service application	Make service application-related data and configuration available for recovery. <a href="http://technet.microsoft.com/library/ee428318(office.14).aspx">http://technet.microsoft.com/library/ee428318(office.14).aspx</a>
Back up search	Allow restoration of data losses that might occur from problems such as hardware failure or power outages. <a href="http://technet.microsoft.com/library/ee748635(office.14).aspx">http://technet.microsoft.com/library/ee748635(office.14).aspx</a>
Back up a content database	Allow restoration of data losses that might occur from problems such as hardware failure or power outages. <a href="http://technet.microsoft.com/library/ee428327(office.14).aspx">http://technet.microsoft.com/library/ee428327(office.14).aspx</a>
Back up customizations	Allow restoration of data losses that might occur from problems such as hardware failure or power outages. <a href="http://technet.microsoft.com/library/ee748642(office.14).aspx">http://technet.microsoft.com/library/ee748642(office.14).aspx</a>
Back up a site collection	Allow recovery from user error. <a href="http://technet.microsoft.com/en-us/library/ee748617.aspx">http://technet.microsoft.com/en-us/library/ee748617.aspx</a>
Export a site, list, or document library	Allow recovery from user error. <a href="http://technet.microsoft.com/en-us/library/ee428301.aspx">http://technet.microsoft.com/en-us/library/ee428301.aspx</a>
Backup logs	Provide data useful for performance analysis, troubleshooting, monitoring compliance with service level agreements, and legal, regulatory, or business reasons. <a href="http://technet.microsoft.com/en-us/library/ff621098.aspx">http://technet.microsoft.com/en-us/library/ff621098.aspx</a>

SharePoint recommends using the native backup and recovery tool for small to medium server farms only. Supported backup database size is up to 600GB. For large SharePoint server farms, System Center Data Protection Manager (DPM) is recommended. DPM 2010 supports backups up to 80TB.

### 5.3 System Center Data Protection Manager 2010

Microsoft System Center Data Protection Manager (DPM) is a backup and recovery tool that provides unified data protection to SharePoint 2010.

DPM 2010 interacts with the SharePoint and SQL Server Volume Shadow Copy Services (VSS) writers so that DPM captures consistent versions of a SharePoint deployment without interrupting client access to SharePoint content. DPM provides granular protection by combining VSS snapshot functionality with DPM block-level synchronization.

For more information on protecting SharePoint environment with DPM, see the Microsoft datasheet *DPM 2010 datasheet - How to protect Microsoft SharePoint with Microsoft System Center Data Protection Manager 2010* at

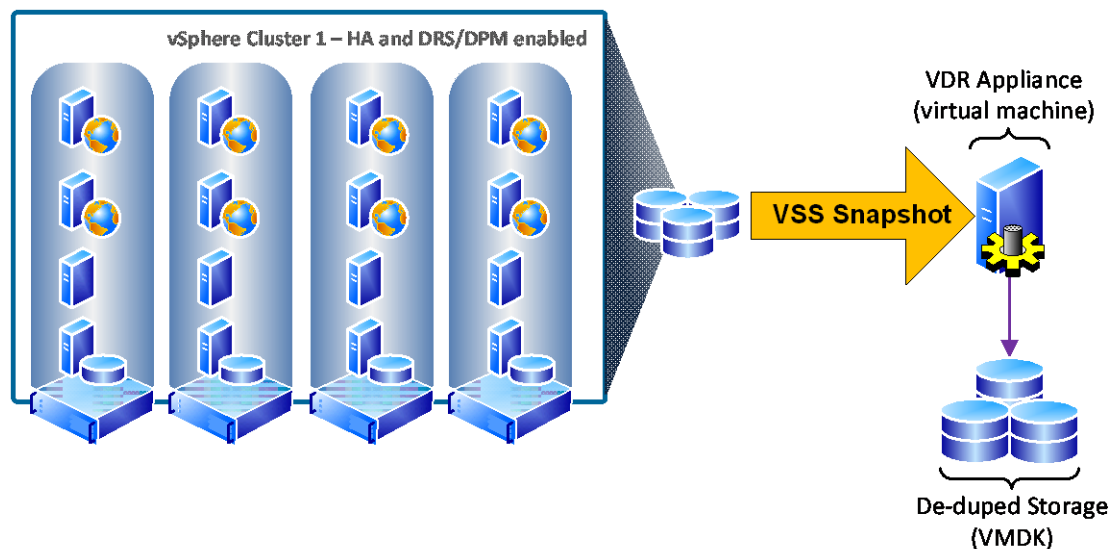
<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=D716A8F8-3864-42CC-B162-F0EE8A26643E>.

### 5.4 VMware Data Recovery

VMware® Data Recovery (VDR) protects your data at the virtual machine level, capturing application and system data as a full virtual machine image. VDR runs at the ESX/ESXi host level as a virtual appliance to provide streamlined deployment and full integration with vCenter Server. VDR stores multiple restore points for each virtual machine using *deduplication* technology to provide point-in-time restore capabilities, and to use available disk space efficiently.

VDR is based on VMware snapshots, which are not currently supported by Microsoft for SQL, but can be used for SharePoint Web and application servers.

Figure 9. VMware Data Recovery



## 6. Best Practices

The following are best practices for running a SharePoint 2010 Server farm on VMware vSphere.

### 6.1 Using VMware DRS Affinity and Anti-Affinity

DRS provides the ability to define anti-affinity and affinity rules. You can specify groups of virtual machines that should never reside on the same host (anti-affinity) or that should always run together on the same host. DRS also enables grouping of virtual machines by common name and restricting their execution to a specific subset of hosts.

DRS affinity/anti-affinity rules can be used to spread SharePoint Web server roles and application server roles across hosts in the ESX cluster. DRS affinity/anti-affinity rules should also be defined to avoid clustered or mirrored SQL Server virtual machines from running on the same host.

#### To set up affinity or anti-affinity rules

1. In the vSphere Client, right-click the cluster in the inventory and select **Edit Settings**.
2. In the left pane of the **Cluster Settings** dialog box, under **VMware DRS**, select **Rules**.
3. Click **Add**.
4. In the **Rule** dialog box, type a name for the rule.
5. From the **Type** dropdown menu, select a rule.
6. For a cluster of virtual machines on one physical host, select **Keep Virtual Machines Together**. For a cluster of virtual machines across physical hosts, select **Separate Virtual Machines**.
7. Click **Add**.
8. Select the two virtual machines to which the rule applies and click **OK**.
9. Click **OK**.

#### 6.1.1 Enable Strict Enforcement of Affinity Rules

To strictly apply affinity and anti-affinity rules, set an advanced option for VMware DRS. Setting the advanced option `ForceAffinePoweron` to 1 enables strict enforcement of the affinity and anti-affinity rules that you created.

#### To set the ForceAffinePoweron option

1. In the vSphere Client, right-click the cluster in the inventory and select **Edit Settings**.
2. In the left pane of the **Cluster Settings** dialog box, select **VMware DRS**.
3. Click **Advanced Options**.
4. In the **Option** column, type `ForceAffinePoweron`.
5. In the **Value** column, type 1.
6. Click **OK**.

#### 6.1.2 Set Automation Level for DRS

You must set the automation level of all virtual machines in an MSCS cluster to **Partially Automated**. vCenter Server then performs initial placement of virtual machines when they are powered on and provides migration recommendations for them.

For more information, see *vSphere Resource Management Guide* at [http://www.vmware.com/pdf/vsphere4/r41/vsp\\_41\\_resource\\_mgmt.pdf](http://www.vmware.com/pdf/vsphere4/r41/vsp_41_resource_mgmt.pdf).

## 6.2 Best practices for VMware Site Recovery Manager

For best SRM performance, follow these recommendations:

- Grouping virtual machines under fewer protection groups enables faster test and real recoveries, provided those virtual machines have no constraints preventing them from being grouped under similar protection groups.
- Enable VMware DRS at the recovery site. This optimizes performance and recovery time as VMware DRS load balances the recovered virtual machines across the hosts.
- Because it impacts test and real recovery time, chart out the dependencies between, and priorities for, virtual machines to be recovered so that only a certain number of required virtual machines can be assigned as high priority. Similarly, suspending virtual machines on the recovery site also impacts recovery time.
- Install VMware Tools in all protected virtual machines to accurately acquire their heartbeats and network change notification.
- Confirm that any internal script or call out prompt does not block recovery indefinitely.

For more information, see *VMware vCenter Site Recovery Manager Performance and Best Practices for Performance* at

[http://www.vmware.com/pdf/Perf\\_SiteRecoveryManager10\\_Best-Practices.pdf](http://www.vmware.com/pdf/Perf_SiteRecoveryManager10_Best-Practices.pdf).

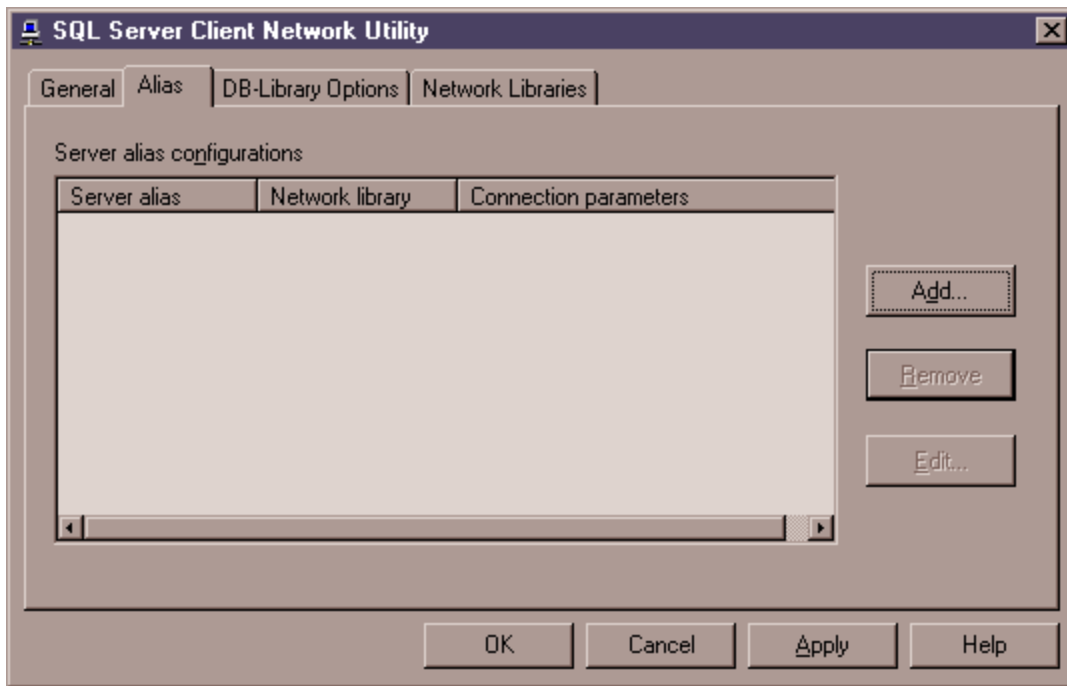
## 6.3 SQL Server Alias for Greater Flexibility

A connection alias is an alternate name that can be used to make a connection to an SQL Server instance. In the case of SharePoint products and technologies, you can create an SQL Server alias that is used by all servers (including the front-end Web servers) to connect to the SQL Server instance. Configure an SQL Server alias for SharePoint. This enables you to re-home your SharePoint client to use a different SQL Server (possibly a different instance) when necessary.

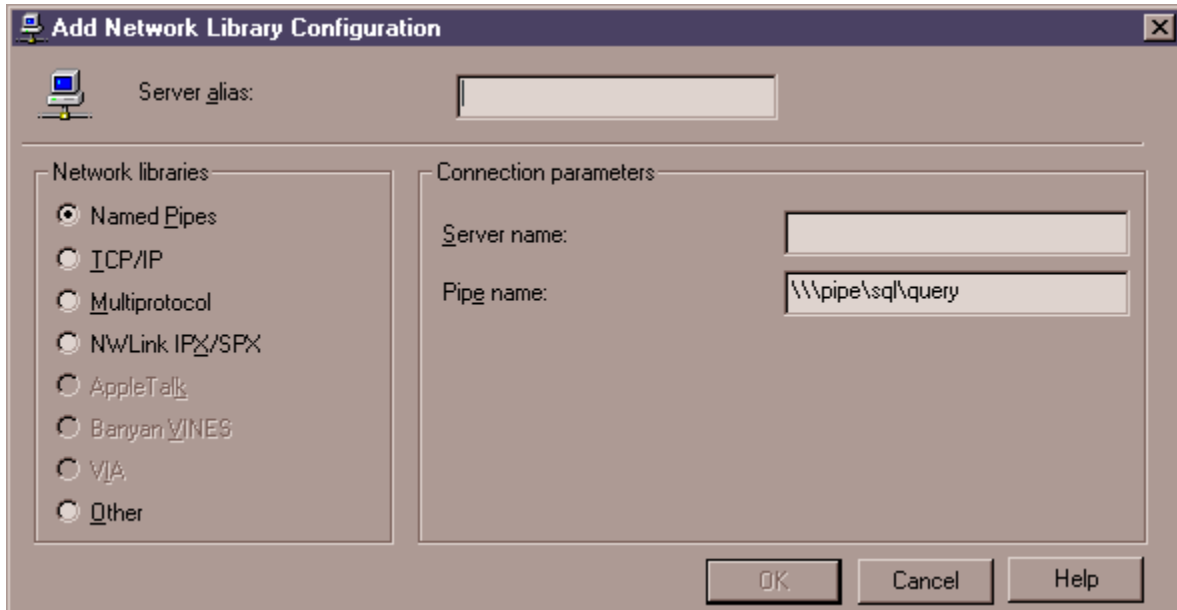
If you plan to use an SQL Server alias, set up the alias before installing SharePoint. Complete the following steps on every front-end Web server, and on every server that connects to SQL Server.

**To create an alias**

1. Start the **SQL Server Native Client Network Utility** by running %SYSTEM%\cliconfg.exe from the command prompt.



2. Click the **Alias** tab, and then click **Add**.



3. Select **TCP/IP** type an alias, type the server name to associate with the alias, and then click **OK**.

**Note** If you are setting up aliasing for an existing server farm, use an alias with the same name as the principal server so that you do not have to change the front-end Web servers to start using the alias.

## 7. Conclusion

This document described options to provide SharePoint 2010 server farm availability in a virtualized environment using VMware vSphere features, such as VMware HA/DRS, vMotion, and SRM, in combination with SharePoint 2010 and SQL Server native availability features. Various high availability options, disaster recovery options, backup and recovery options for the different server roles, and protection levels were described.

Before choosing any one availability option to implement in your environment, evaluate the business requirements to determine which scenario best meets your specific needs. The options you choose can also take into account complexity and cost, available equipment, and network resources.

Go to <http://www.vmware.com/solutions/business-critical-apps/> for more information.