NJ County

Disaster Recovery

Design

by

RAMe Communications

Table of Contents

Introduction

This document defines the design for the NJ County Electronic Information Systems Disaster Recovery (DR) project according to the requirements in the NJ County Disaster Recovery Report. The design includes the specifications of both physical infrastructure (facilities, networking, and user workspace) and information systems (computer hardware, operating systems, application software and peripherals). Based on the information provided in this document, NJ County will be able to make necessary facilities improvements, contract for services and purchase equipment required to implement the design.

While some sections are technical and specifically directed at Information Technology professionals, most of this document is written for anyone with a general understanding of information systems and networking.

Following the Executive Summary is a brief discussion of the design goals to provide a background to the overall functional requirements, what technologies are available to meet those requirements and how the design uses the technologies best suited to NJ County's needs.

The next section provides detailed information about the design in four areas: the physical infrastructure of buildings and equipment, network topologies, server virtualization and replication, and end-user workspace resources and configuration.

The final section provides a scenario of the disaster recovery process based on this design.

This document does not provide an implementation plan or a disaster recovery plan. The Appendix discusses these documents and the value that they have as NJ County proceeds with its disaster recovery and business continuity efforts.

Executive Summary

NJ County has invested considerable resources in information technology as part of its ongoing efforts to improve the quality and scope of services available to its constituents. In order to mitigate against a man-made or natural disaster that would disrupt the availability of those resources, NJ County has contracted to design and implement a disaster recovery site with the capacity to provide continuity of operations for critical information systems. This document provides the design for that DR site.

The original design specification document specifically addressed the needs for operational continuity of the County Electronic Document Management System in the event of a disaster. It also was based on the use of facilities at xxxxxxxxxxx, NJ as the location for the DR site.

This document applies to all production electronic information systems and is based on the use of the XXXXXXXXXX Building located at xxxxxxxxxx in Township as the DR site.

Inherent in the design are several assumptions about the level of risk which the County has deemed acceptable.

The period of time that can elapse from the onset of a disaster event until the affected information systems are made available in DR mode is no more than 24 hours. Affected systems will be restored in DR mode to a point of data consistency no more than 24 hours before the onset of the disaster event.

The fundamental concept in this design is the replication of data from the production VMware ESX server in the County Courthouse server room to another ESX server located at the disaster recovery site. This replication, or constant copying of data from one server to another, ensures that, in the event that the production server goes down, its peer will continue to provide services to key employees, and therefore provide uninterrupted access to County electronic information systems.

The DR design makes use of system virtualization technology to provide hardware independence for DR system resources, high system availability, and to facilitate and enhance the replication of the production systems to the DR site. It also plays a central role in the configuration and availability of end user laptop computers for use in DR operations.

Facilities at xxxxxxxxxxxxxxxxxxx have been identified by the county as the location for the DR site. The building is used for multiple purposes including office space for the Department 1, and the Department 2, and a meeting place for community organizations like the XXXX Club. The design specifies the DR computer room power requirements, environmental controls, fire detection and suppression equipment, security access control, and network infrastructure and equipment.

Reliable network connectivity between the County data center and the DR site is an essential element of the DR design. Current connectivity is achieved using a VPN connection via the Internet using Comcast High Speed Broadband Services. Other options that meet the design requirements are fiber optic cabling or a wireless bridge.

During a disaster event, users will need to be able to connect to and access the systems at the DR site. The design specifies the wireless networking for this purpose, the use of laptops and the configuration of those laptops for normal and DR operation.

Moving forward the county will need to create an implementation plan based on this design document and create and execute a DR test plan once the DR site implementation is complete. A short discussion of these documents is included in the Appendix.

Design Goals

According to the Cisco disaster-recovery planning document published in 2004, the leading causes of information system disruption are:

- Fire
- Storm
- Flood or other water related
- Extremely high or low temperature, humidity
- Earthquake, mudslide or other land movement
- Automobile or airplane crash

Reviewing these leading causes of disaster point out that any of these events has a probability of more then zero (0) for it to happen in the NJ County data center. One should not just view a terrorist attack or a nuclear disaster as the cause for service destruction. Fire and/or weather related storms are likely to happen anywhere. Although flood may not happen on a large scale, water damage can simply happen during a rain storm and leaking roof. Mudslides can damage computer equipment and it is enough for proximity to road construction where a pile of dirt is place in a parking lot that a microburst involving large quantities of water can wash the pile into a computer room.

Requirements

There are many different events, natural and man-made, that can be considered a disaster. The common factor in all of them is that they interfere with one or more of the four requirements for electronic information systems to be effective:

- Knowledgeable *people* to operate the systems
- Access to the *data* files
- Access to the *software* applications that create and manage the data files
- Access to *systems* configured with the proper applications & data for people to use

In order to be effective the DR design must address the following issues:

- High application availability
- Hardware independence
- Data integrity

The design presented here addresses each of these factors in the sections that follow.

Assumptions and definitions

Inherent in this design are assumptions about the level of risk the County considers acceptable. In particular, the following factors in recovery operations have been quantified.

Time to recovery: The period of time that can elapse from the onset of a disaster event until the affected information systems are made available in disaster recovery mode is no more than 24 hours.

Extent of recovery: Affected systems will be restored in disaster recovery mode to a point of data consistency no more than 24 hours before the onset of the disaster event.

Recovery duration: Operations in disaster recovery mode will last no longer than one week from the time that the affected systems are made available in disaster recovery mode until the production systems are again available for normal operations.

Extent of disaster: An event that requires a disaster recovery response will be assumed to also disrupt the work environment of users.

Resource allocation: Even though there are potential cost savings by sharing common resources, the DR computer room and equipment installed in the room are assumed to be dedicated to DR purposes.

Disaster recovery versus business continuity

Disaster recovery is a component of business continuity although often the terms are used synonymously. For the purposes of this document, disaster recovery is limited to the systems and processes needed to make the functionality of the NJ County electronic information systems available to users in the event of a disaster.

Virtualization

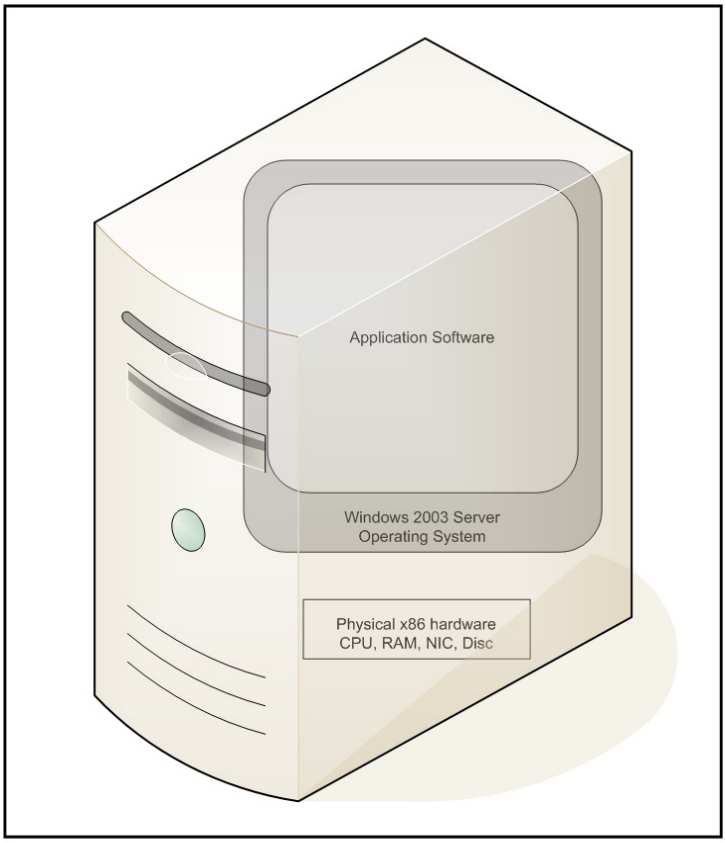
A modern datacenter is comprised of many servers running many applications providing resources to many users. This complexity introduces a number of challenges to disaster recovery design. A modern operating system (OS) such as Windows 2003 server is coupled very closely to the hardware it runs on. While a typical system implementation provides an easier environment for day to day administration because many functions can be performed automatically, it can make rebuilding or recovering a failed system very difficult. Because it is not possible to simply copy a complete system from one hardware platform to another, the traditional way to rebuild a system is to reinstall the operating system and application software on either recovered or replacement hardware and reload data from the most recent backup. Not only is this process time consuming, but without very strict configuration control and documentation the new system will not have the exact configuration of the old system.

Imaging software ("Ghost" by Symantec is perhaps the best known) has been of some value in addressing the need to create a copy of a complete system. But, because computer hardware changes frequently and two servers bought at different times (even from the same vendor) may contain entirely different hardware, an image of the first system may not be usable on the next one. In addition, imaging software can only provide a "point in time" copy of a system and can only do so when the system is off-line.

VMware virtualization technology addresses both the issue of changing hardware and the need to reduce the time required to make system resources available in DR mode. While VMware also provides additional operational benefits, this discussion will be focused on those features related to disaster recovery.

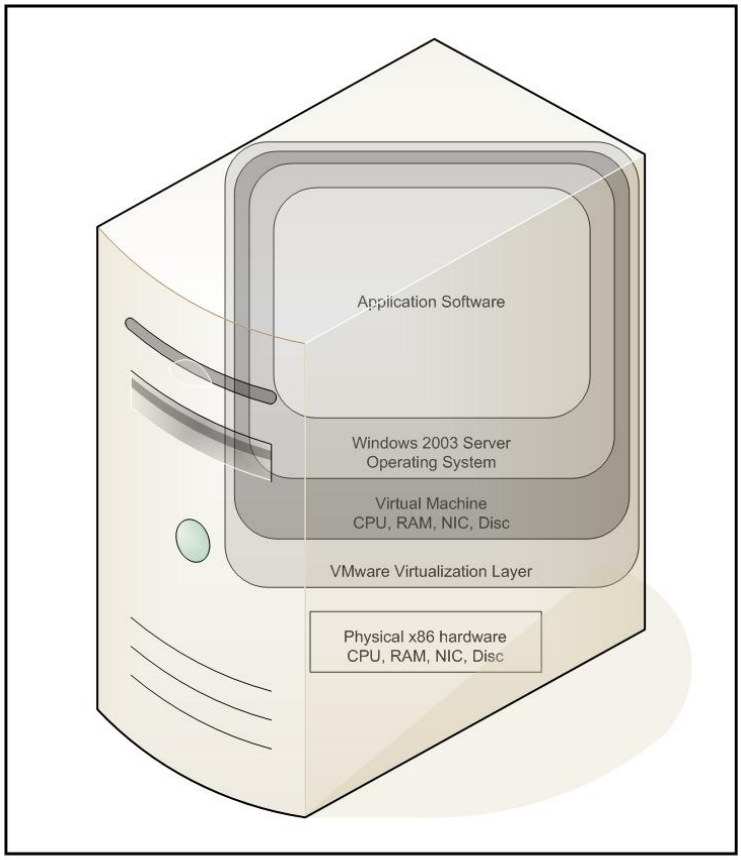
Hardware Independence

As noted above, an installation of Windows 2003 Server is tightly coupled with the physical hardware platform. Specific drivers are needed to support the motherboard resources like processors and memory, and peripheral resources like mass storage controllers and devices and network interface cards.



Typical Windows 2003 Server Implementation

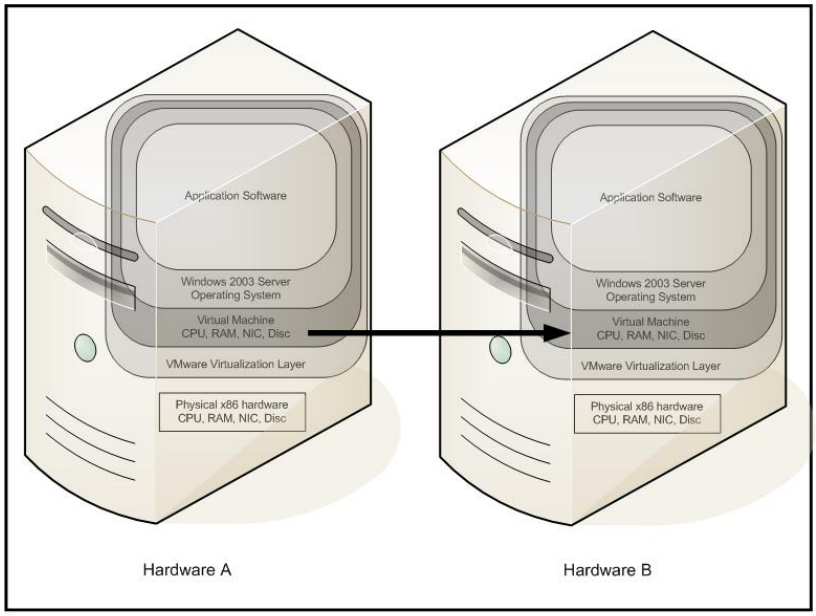
VMware's technology introduces a virtualization layer that separates the physical hardware from the operating system, presenting a standard set of hardware devices and interfaces as a virtual machines (VM) to the operating system. One or more VMs share the physical hardware resources, but each functions independently of the others. The virtualization layer is actually a highly specialized and streamlined operating system and each VM is a file structure within the virtualization layer.



Virtualized Windows 2003 Server Implementation

Each VM is based on the same standard virtual hardware devices and the virtualization layer addresses the differences from one hardware platform to another. As a result, operating system installations can be highly standardized using imaging or scripted setups.

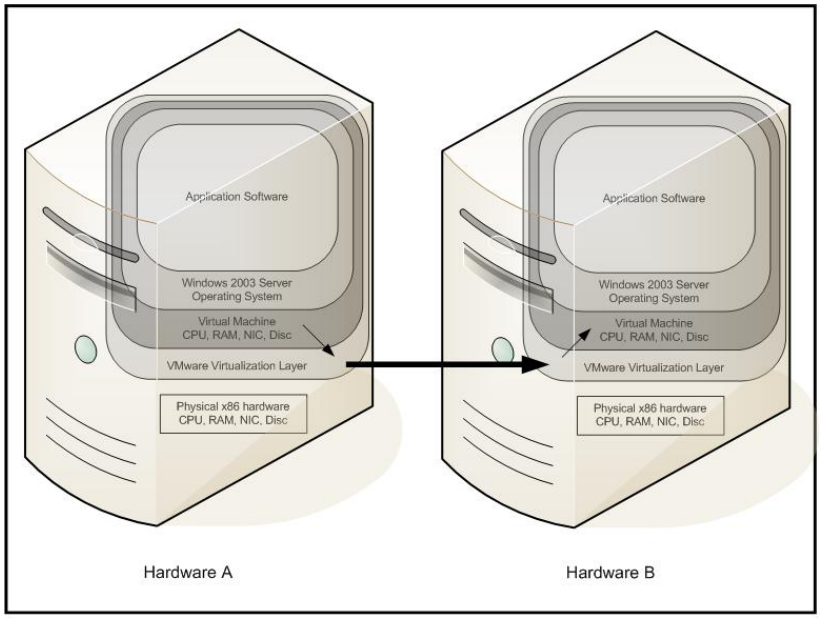
Because each VM exists as a file in the VMware virtualization layer, it can be copied from one HW platform to another even if the HW platforms have very different physical components.



Virtual Machine Copying

Replication

The VMware virtualization layer allows changes in the state of the virtual computer on Hardware A to be incrementally updated to the virtual computer on Hardware B. This process is known as replication. Replication is often used for synchronizing data, not operating systems and application software. But because the two virtual machines are actually file structures within the VMware virtualization layer, they can easily be replicated between the two HW platforms.



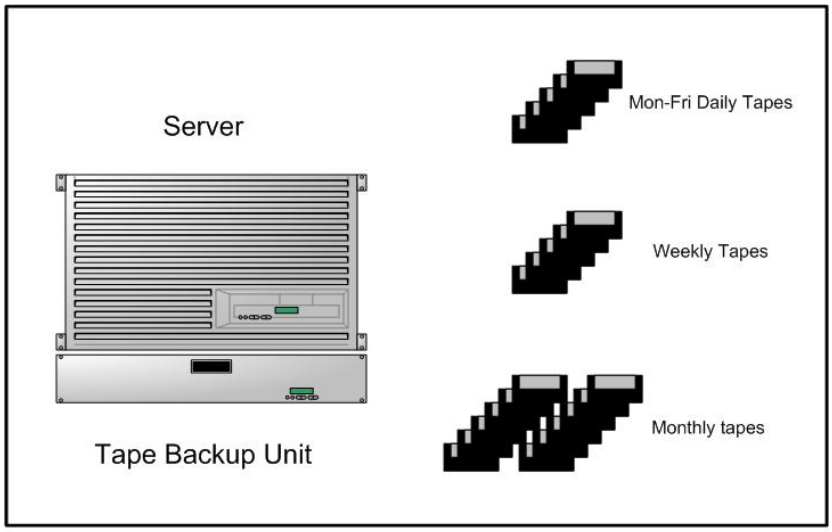
Virtual Machine Replication

Replication occurs at intervals which can be configured and tuned for the specific system and network configurations. As the interval diminishes, replication approaches real-time, continuous synchronization.

The VMware virtualization layers on the production and DR systems are in constant communication. One of the options available is automatic failover in which the DR system can immediately replace the production system if it becomes unavailable. This capability is not only valuable for DR purposes but also makes systems highly available during scheduled maintenance periods.

The Role of Backup/Restore Systems

When mainframe computers were the primary means of electronic data processing, tape-based backup and restore systems were the fundamental blocks of disaster recovery. In modern DR scenarios, tape based backup and restore still plays an important role as a way to recover from data corruption, an issue not addressed by virtualization technology.



Tape Backup History

Even when the information system hardware and software is working properly, it is possible for data to become corrupted, either due to application or user error or from a deliberate malicious action. With an appropriate tape backup rotation schedule, it is possible to go back to a version of data that has a known consistent and proceed to re-enter data from that point in time.

The sections that follow provide the specific design specifications for NJ County. Included are discussions of the physical facilities, network and connectivity requirements, DR information servers, the workspace configuration and resources for users and an example of a recovery scenario.

NJ County Disaster Recovery Facilities

This section describes the building components necessary for a robust, safe and secure facility to ensure business continuity.

Building description

The building NJ County selected for the disaster recovery (DR) site is located 6.48 miles northeast of the main campus at xxxxxxxxx, Township, NJ. Known as the Xxxxxxxxx Building, it is a cement block building supported by a steel structure. The floor is tile on poured concrete. This building was not previously used for DR purposes and special consideration must be given to the functional needs of a DR site. The following sections highlight special requirements that should be taking into consideration.

Building Occupancy

The facility is already occupied by Department 1 and Department 2. These organizations will share the VPN network connection with the DR equipment. The building has large assembly hall used for community meetings. This room will be used by County employees for work spaces during disaster recovery operations. The only other area of the building specifically allocated to DR purposes is a storage room adjacent to the assembly room that will be used as a computer equipment room.

Department 1

Department 1 will continue to occupy their suites in the building. This document does not address their needs but it is likely that the network connection between the county data center and the Xxxxxxx Building will be shared by all occupants. Therefore, when sizing the link (10Mbps, 100Mbps, 1Gbps), the county needs to consider the aggregate bandwidth requirements. This document also does not address the network infrastructure or information resource requirements of Department 1 in normal daily operation.

Department 2

This office will also continue to occupy their suites in the building. This document will not address the specific needs of the department during normal daily operation.

Disaster Recovery

The third entity in the Xxxxxxx Building is not an office or people but a function and it is the focus of all the subsequent sections. The disaster recovery design is a collection documents, testing plans, computer software and network links that together provide NJ County business continuity in case of a disaster. Since a disaster can be many things it should be define in a more narrowly term for the purpose of clarity.

> In this document, a disaster is any event that causes the county to shutdown or not use the county's datacenter and transfer data processing to alternative location for a limited but essential business functions

Power

There seems to be an adequate electricity feed into the building. However, the County must ensure that the power is clean. In addition, unless there is a significant investment for an Uninterrupted Power Supply (UPS), the County should be investigating power failure in the area.

Readiness of Electricity

During normal operation the building will be fed electricity from the utility company. However in case of emergency it is crucial to have details understanding of what the utility will be able to provide. A generator for a disaster recovery site is essential, but running a generator for a long time can be problematic. It is beyond the scope of this document to design a detailed electrical power plant. But suffice to say that a good understanding of power availability is essential. Any communication with the power company should be documented and what the county should be expecting during a disaster should be worked into a plan and understood. For example, if the power goes out in the county and the utility company restores power in order of importance, then the utility company should be made aware that the Agriculture Building is a top priority.

Backup Generator

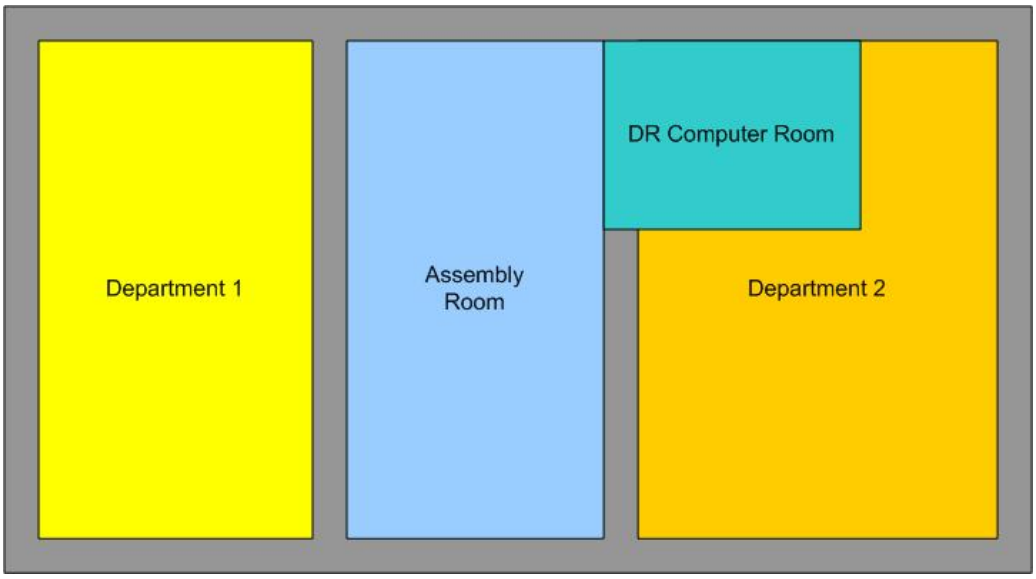
In a national survey done by the Business Continuity Planners Association, nearly all companies which suffered disaster (81%) have taken actions as a result o the disaster to reduce business interruption in the future. The most common changes made were adding alternate power sources. The problem with a good reliable electric generator and provide enough power to a computer room is the cost. A good electric generator is expensive and is used rarely. Specifying which generator the county should buy is not in the scope of this document. However, a common mistake is specifying a generator that can produce enough power for a short time. The recommendation we would like to make is buy an electric generator that is built to run for a few days, not a few hours even if it means buying a larger generator.

Fuel Testing

Most generators rely on diesel fuel which is susceptible to bacteria, water absorption and contamination. Typically a generator is operated only few times a year and only for testing. This presents a potential problem during a real disaster. During an extended power outage, the generator diesel engine will empty the fuel tank. If the unused fuel from the bottom half of the tank is contaminated, it can lead to an engine malfunction during an extended period of operation. The generator needs to be designed to run reliably for at least two-three days of continuous operation and the fuel needs to be replaced or consumed on regular basis. The generator should be tested for a long running period at least once a year.

Environmental controls

The building will have four distinct climate zones requiring separate environmental controls: office space for Department 1, office space for Department 2, the public assembly room, and the computer room for the DR site. In each area both temperature will need to be monitored and controlled separately as well as humidity monitoring and control in the computer room. The following sections specifically address the needs of the computer room.



Temperature requirements

Maintaining an ambient temperature range of 68° to 75°F is optimal for system reliability. This temperature range provides a safe buffer for equipment to operate in the event of air conditioning or HVAC equipment failure while making it easier to maintain a safe relative humidity level. Under no circumstances should computer equipment be operated in conditions where the ambient temperature exceeds 85°F. Monitoring equipment should generate early warning alerts at 60° and 80°F, with critical alerts at 50° and 85°F.

Humidity requirements

Relative humidity (RH) is defined as the amount of moisture in the air at a given temperature in relation to the maximum amount of moisture the air could hold at the same temperature. The DR computer room needs to maintain ambient relative humidity levels between 45% and 55% for optimal performance and reliability.

When relative humidity levels are too high, water condensation can occur which results in hardware corrosion and early system and component failure. If the relative humidity is too low, computer equipment becomes susceptible to electrostatic discharge which can cause damage to sensitive components. Monitoring equipment should generate

early warning alerts at 40% and 60% RH, with critical alerts at 30% and 70% RH. It is important to remember that the RH is directly related to the current temperature, so monitoring temperature and humidity together is critical.

Fire detection/suppression

A water sprinkler with air charged pipes is now recommended for office spaces and the archives area. The air in the pipe prevents water leaks and gives a time delay to stop the system if a false alarm is triggered. In most cases the damage from fire damage outweighs the damage from water. Fire extinguishers should also be placed throughout all areas. Smoke detection devices need to be present in all areas. They should trigger a signaling system that is monitored continuously by a person or company that can dispatch the appropriate responders.

The DR computer room should be equipped with a gas based fire suppression system that uses one of the many Halon alternatives (FM-200, Inergen, Argonite, etc.). These systems are safe for both equipment and people. Because the room is relatively small it should not be necessary to have a secondary dry pipe sprinkler system as a backup.

Security

A limited number of county employees will need access to the DR computer room and controlling and monitoring access to the room is an essential element to ensuring system availability and reliability. The entrance door should be equipped with an electronically controlled lock that requires a key card or other authenticator in addition to a PIN or pass code. All attempts to access the computer room must be logged and identify who and when the access was made. Repeated access failures must generate an alert to notify county IT and public safety personnel.

Cable installation and management

The reliability of the DR site is highly dependent on the quality of the cable installation used to connect the resources in the DR computer room to the county data center and to the users. All data cabling including fiber optic and unshielded twisted pair (UTP) must be installed following EIA/TIA-568-B.2, EIA/TIA-568-B.3, EIA/TIA-569-A, EIA/TIA-607, ISO/IEC 11801 and ISO/IEC 14763 standards. These standards are copyrighted publications of the issuing organizations and can be purchased from IHS Global Engineering Documents (http://global.ihs.com). Additionally, cable installation must conform to local building codes and ordinances.

In general, structured data cabling requires professional installation by knowledgeable and experienced vendors. Cable ladders are used for stress relief and organization; punch-down patch panels provide proper termination; conduit protects

cabling on runs through walls and floors; fire stop materials seal core penetrations, protecting against the spread of fire. All installations need to be thoroughly tested to verify performance and reliability.

Racks

All information servers and network equipment in the DR computer room will be designed for mounting in IEEE standard 19” racks. Generally, two types of rack systems are available: ladder (open) and enclosures.

Enclosures provide additional security and protection for computer equipment and are well suited for installation on a raised floor with cooling and ventilation from below. A single, 42U (1 U = 1.75”) cabinet will provide sufficient space for the DR ESX server, disk array enclosure, UPS, management console, network equipment and cable management. An important part of installation is to properly ground the enclosure.

Network Specifications

The network infrastructure for the DR computer room includes two basic components: connectivity to the County data center and a local area network for users to connect to the DR ESX server.

County Data Center to DR Site Connectivity

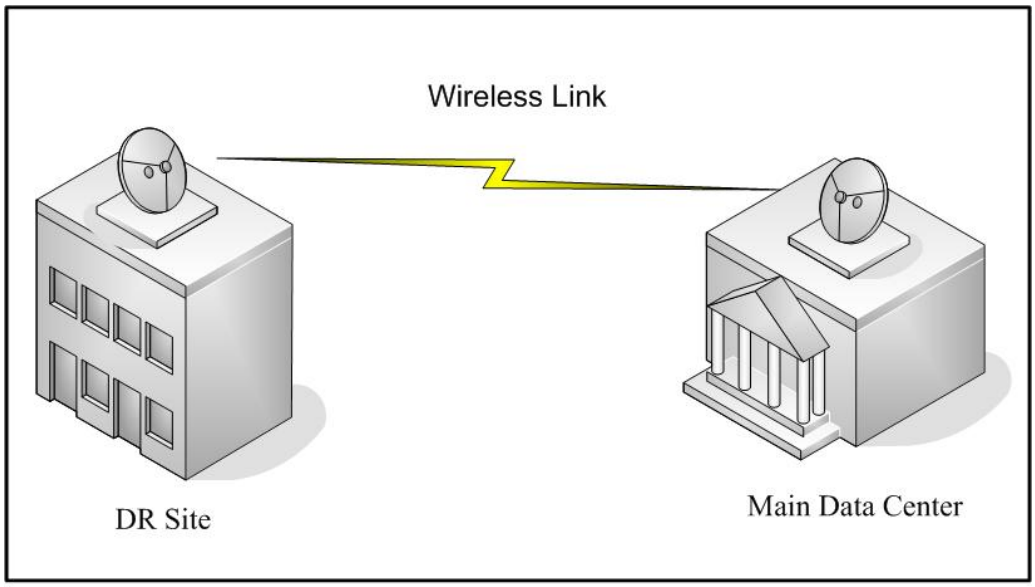
The DR building needs a full time network connection to NJ County datacenter. The three options are presented in the following sections in order of preference: fiber optic, wireless, and Internet VPN. This connection is essential for the automatic DR replication, remote access to DR machines, and in general connectivity with the County computer room. In addition, network access will provide the County with the option to connect to other municipalities.

Fiber Optic

While ideal in terms of reliability and maximum bandwidth, it may be cost prohibitive to extend the County's fiber optic infrastructure to the Xxxxxxx Building. However, the County should investigate the feasibility of the project within the scope of other connectivity projects.

Wireless

Using 6, 11, 18, 23, or 38Ghz (licensed) wireless link, the County can have from 50 to 900Mbps connectivity between the two locations. This technology requires a line of site between the two buildings and operates at distances up to 30 miles.

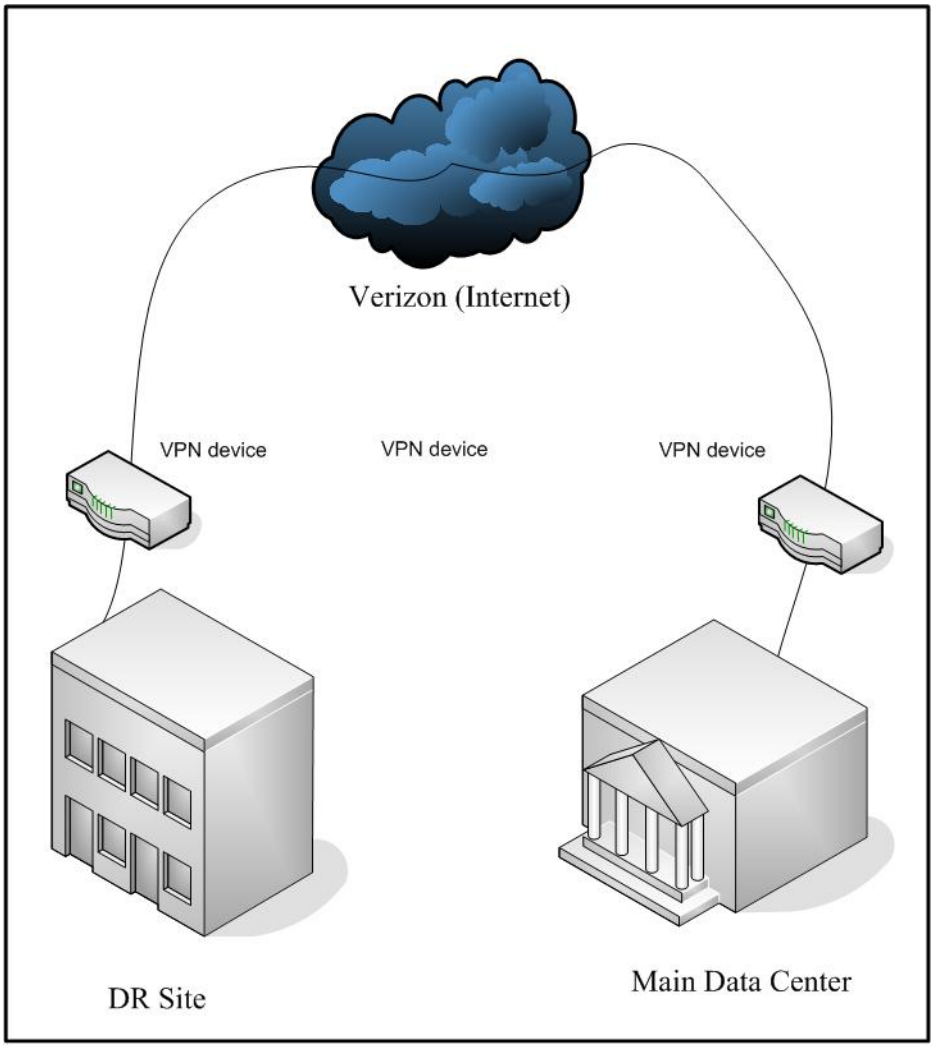


Wireless Connection

The advantage of a wireless link is that the County will avoid ongoing service expenses. Once the link is installed, there are no additional costs other than routine maintenance. The equipment is designed for extended use in exposed conditions. Ceragon's FibeAir family of products provides a number of options for high reliability solutions. However, the county should consider an extended warranty and service agreement with the wireless equipment vendor to protect against outages due to hardware failure.

VPN via the Internet

The county currently uses Comcast High Speed Internet Service to communicate between the data center and the Xxxxxxxxxx Building with a Virtual Private Network configuration to protect the privacy and the security of the County's data. The Internet connection must be upgraded to at least T1 bandwidth to support replication.



VPN Connection

Verizon can provide Internet connectivity to the DR site.

Bandwidth

For DR operations alone, a 10Mbps connection between the County data center and the DR site should be sufficient. But it is likely that the connection used for DR purposes will also be used to connect Department 1 and Department 2 offices to the NJ network. The bandwidth requirement for those departments is not known and it is possible that a 10Mbps connection will require a bandwidth management device to ensure that DR replication can be prioritized. A 100Mbps connection (or higher) is preferred and will provide enough bandwidth for the DR computer room to become a secondary datacenter for the county in addition to fulfilling the minimum requirements for DR and normal business operations.

Internet Access

Access to the Internet is important to disaster recovery site. The Internet in the DR site will be used for County personnel to connect to the systems that are running at the DR site over the Internet.

Comcast is currently providing Internet connectivity to the Xxxxxxxxx Building.

Local Area Network in the Agriculture Building

During a disaster, at least 40 people will have to be connected locally to the DR computer room. In essence, during a disaster, the DR site will become the computer room. The DR site should support a 100Mbps local area network independent of outside networks. This means that the IP addresses should be unique to the DR site and a router will be used between the main datacenter and the DR network.

Server Virtualization

Minimally, the production and DR hardware platforms will be running VMware ESX server with the production server replicated to the DR server. While not necessary for the DR design, it may also be useful to run DR site infrastructure servers (domain controllers, file servers, print servers) as virtual machines on the DR hardware platform.

Implementation considerations for the EDMS server

The EDMS application software is licensed in the form of a USB key. Currently, the server has the key plugged into it so the vendor can dial in and perform maintenance. The key is only necessary to run the EDMS program. All other maintenance can be done as with any another Windows 2003 server. A more robust approach will be for the vendor to access a workstation that has the USB key to provide support services.

Fax boards on the production EDMS server are proprietary and VMware will require direct HW access to them.

Initial Production Server Migration

It will be necessary to convert the production servers to VMware "in place," a process supported by VMWare ESX. This conversion will be lengthy and should be scheduled during a time when systems can be generally unavailable to users.

Each VM is a file in the VMware ESX server and includes the installation "footprint" of the operating system and application software. Data will be stored on a separate virtual disk system that can be shared by multiple VMs. A minimum of 12GB needs to be allocated for each VM on the DR server. Additional disk space will be required for the DR data.

If the County uses a VPN connection via the Internet to connect the County data center and the Xxxxxxxx Building, the initial replication of the production and DR servers will need to be done at the County data center. Alternatively, the replication can be done using the 4TB portable disc array.

DR ESX server specification

The following is the recommended minimum system configuration for the DR server. It will run VMware ESX Server and the DR servers will run as VMs on that platform. The system has sufficient resources to meet the requirements of an Active Directory domain controller and the VMware ACE server running as VMs on the same hardware platform.

Component	Specification	Qty
CPU	3.2 Ghz Intel Xeon processor	2
RAM	4GB SDRAM	16
Video	integrated SVGA or better	1
Disc	Hot swap147 GB Ultra 320 SCSI	15
Disc	72 GB Ultra 320 SCSI	2
NIC	10/100/1000 Mbps	1
HDD controller	Ultra 320 SCSI RAID 1 and 5	2
Power supply	Hot swap 730W	2
TBU	Tandberg Data 160/320GB Super DLT	1
Case	Rack mount, 3 fixed drive bays, 4 hot swap drive bays	1
Optical drive	DVD/CD-RW	1
Monitor	17" rank mount flat panel	1
Input device	rack mount keyboard and mouse	1
OS	VMware ESX Server	1
OS	Windows 2003 Server (12 CAL)	3
Software	Backup Exec	1
Software	OnBase EDMS	1
Software	MS SQL Server 2005 (2 CPU)	1
UPS	rack mount 2200VA	1

Infrastructure Servers

At least one Active Directory domain controller will be required at the Xxxxxxxxx Building for both normal and DR operations. A server running the VMware ACE application software is also required to manage the VM used for the user laptops.

Continuous data replication

From a disaster recovery point of view, the VM servers consist of two kinds of data: system data and user data. System data, which includes the Windows 2003 operating system, SQL Server software, and the software applications are fairly static and only change when software is updated or reconfigured. User data may change daily, hourly or even by the minute. VMware ESX on the production server will replicate these changes to the DR server on an ongoing basis using the link between the Xxxxxxxxx Building and the County data center.

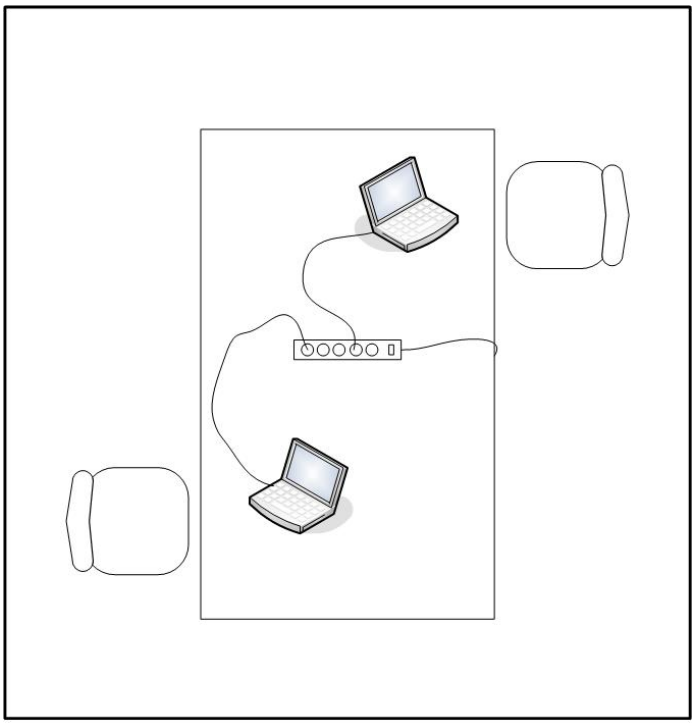
User workspace

As many as 40 users will need to be able to access the DR ESX server during a disaster event. Not only will they need a place to work, they will need computers to work on and the means to communicate with other County employees and County residents.

The County will use the Assembly room area of the Xxxxxxxxx Building for DR user work space. Tables and chairs are stored within the computer room closet area when they are not being used.

Physical space

Each user will require a desk or table to work at, a chair and at least one power outlet. Folding tables can be used with 2 users sharing a 5’ or 6’ table.



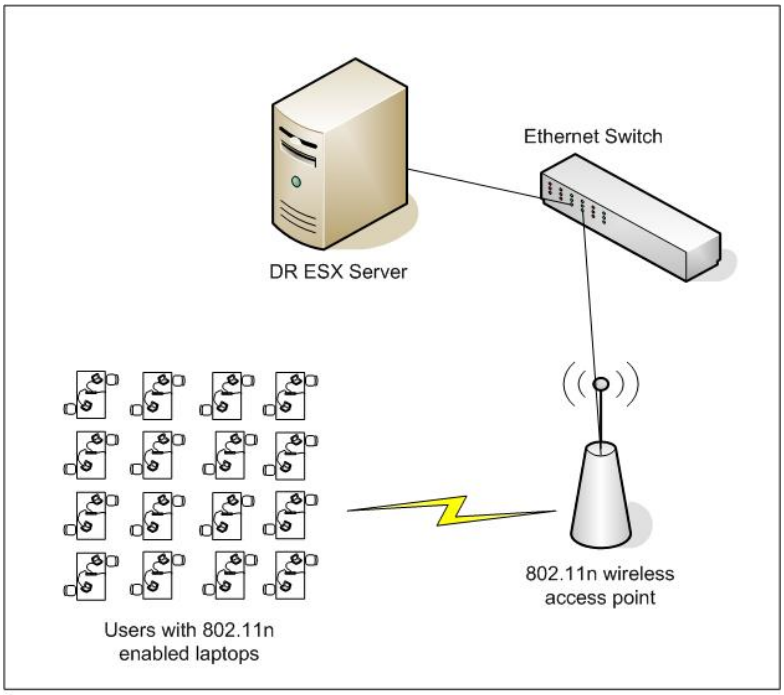
User Workspace

Chairs should be stackable for easier storage. Folding chairs are not recommended.

At least one 110 VAC power outlet is needed for each user. A surge/power strip on each table will be sufficient.

Network

In order to minimize the need for cabling to each user workspace, 802.11n wireless networking is recommended. 802.11n is a new multi-streaming modulation technique that has recently been developed; the standard is still under draft development, although products designed based on proprietary pre-draft versions of the standard are being sold. No only does this technology provide substantially higher bandwidth (up to 200Mbps), it resolves many of the issues with roaming and access point association.

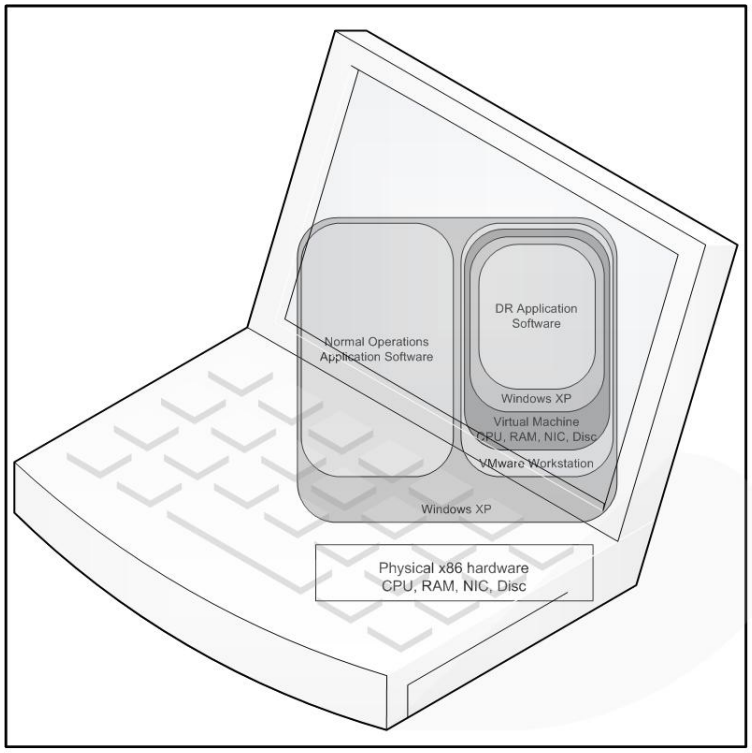


802.11n Wireless Network

User workstations

Users will use laptops as their primary computer platform. The minimum laptop configuration should be a 1.6Ghz Intel CPU, 1GB RAM, and a 40GB hard disk. Each laptop will also require an 802.11n wireless PC CARD and a headphone/microphone and USB video camera. In DR mode, Skype software will be used to allow voice and video communication.

VMware Workstation will be loaded on each laptop and configured to retrieve VM images from the VMware ACE server running on the DR ESX platform.



Virtualized Windows XP Implementation

NJ County Disaster Recovery Scenario

This section describes how the DR design provides continuity of operations for NJ County electronic information systems in the event that the main data center is no longer functioning. It is an example of the general process by which operations are restored.

Initiate Response to Disaster Event

A disaster can occur at any time, but that does not necessarily mean that it is either discovered immediately or that the county immediately responds to it. The county has to define its disaster response policy and provide the resources to meet that policy. If the goal is immediate 24 hour response, consideration must be given to who is available on that basis and how they will communicate during non-working hours.

Identify scope of disaster

The County will need to determine to what extent the production ESX server is affected. The goal is to make an estimate regarding how many people are affected, in what ways they are affected and for how long they will be affected.

Vendors associated with the electronic information systems need to be contacted and apprised of the situation. If needed, replacement equipment should be ordered as soon as possible.

The county insurer needs to be contacted and apprised as soon as possible so damage can be assessed and funds can be made available.

Notify affected users

Users need to be informed of the scope of the disaster, who it affects, in what ways they are affected and for how long they will be affected.

Prepare user DR workspace

The Assembly room in the Xxxxxxxx Building designated for DR user work space needs to be prepared. The tables have to be set up with chairs and power outlets.

Activate DR systems

The DR virtual machines need to be activated and made available on the network.

Perform data and system integrity checks

Once systems are available, they need to be checked to determine that data and system integrity has been maintained during the replication from the production server. It is important to determine the point at which replication was interrupted so that data can be re-entered if necessary after production systems are recovered.

Change to DR system access procedure

The VMware workstation VM on user laptops will need to be activated and used while in DR mode.

Notify users of DR system availability

Once the standby systems are available and accessible, the users of those systems need to be informed how to access those systems and who should do so.

Recover production systems

When business operations are restored in disaster recovery mode, attention must be directed at restoring the disrupted production systems. Depending on the severity and scope of the disaster, this could involve building projects (electrical, construction, wiring etc.) and purchasing replacement hardware. Once the physical plant and required equipment is available, the new production system can be built by replication from the DR ESX server.

Data and system integrity checks

The same data consistency procedures used to bring up the DR systems are now used on the restored production systems.

Notify users of production system availability

When the production servers is ready and available, the users need to be notified that they can resume normal operations. The VMware workstation VM on the laptops is shut down, users can return to their normal work spaces and connect to the production systems.

Appendix - Next steps

The DR design provides the foundation for the County to make decisions about the DR implementation including the selection of vendors for computer hardware and software, network equipment, data cabling, and a service provider for Internet connectivity. Before proceeding with actual renovations or installation of equipment, the County should first create planning documents to help ensure a successful outcome.

Implementation plan

Once the DR design is accepted and approved, the County needs a detailed implementation project plan that includes the specific tasks required to:

- identify and purchase equipment, supplies and services
- equip the DR computer room
- install and configure the VMware ESX servers
- install and configure user laptops
- install and configure routers, switches and wireless network devices

As with any project plan, accurate resource utilization and budgeting will be essential to the success of the project.

DR test plan

Testing the DR implementation is an essential step in DR preparedness. Not only does testing determine if the County can successfully recover from a disaster, it also provides everyone involved in the project with a clear and specific understanding of their role in that recovery. The goal is to have the recovery process well known and practiced so that it is not necessary to determine during the chaos of a disaster what action to take.

It cannot be stressed strongly enough how important it is to routinely test the disaster recovery plan. During the first year of implementation, the plan will need to be tested repeatedly to determine that it meets the county's needs. Afterward it must be tested at least annually to make sure that it is still accurate and results in a successful recovery. If testing of the plan fails, the plan needs to be modified and retested until the test is successful.

The Virtualization Concept In Depth

According to Forester research report called "Pragmatic Approaches to Server Virtualization" conducted in June 2006, adaptation of server virstualization has continued at a rapid pace. 40% of 56 datacenter administrators working for companies 500 employees or more reported engaging in some form of virtualization of the computer in the datacenter. This high percentage amount to a tremendous pressure on software vendors to make their offering compatible with the logical server concept.

Forester research indicated that most companies use virtualization to provide file and print servers, Web servers, custom applications and infrastructure servers. Most companies ran three to six logical servers on one physical machine but some ran up to 15.

Surprisingly, the Forester research report found out that on the surface flexibility, and not cost savings, was the primary factor to server virtualization. Flexibility is also the key factor in our approach to disaster recovery design. However once all factors such as quick upgrade cycle, ease of use, manageability and reduce environmental components such as power and hit, virtualization does show significant cost savings.

The Forester report also found that 23% of respondents were using server virtualization for disaster recovery and that VMware continues to lead as the prefer vendors. This should assure NJ county that the our recommended approach is not on the bleeding edge and the product we recommend is well established. In fact VMware is a wholly own company of EMC, one of the largest companies in the tech industry.

The potential challenges to converting physical server to logical servers (virtualization) involved Learning the technology, the technology itself and support with other vendors. First the visturalization concept has been around for many years, but until recently the implementation took a performance toll. For example to virtualize a Windows 2003 server one had to run a Windows 2003 (virtualized) on top Windows 2003 (the base OS). Today with VMware ESX server the base operating is based on Linux and is much faster with almost no overhead. This high performance configuration and improved ease of use have addressed most of the concerns voiced at the Forested report from Jun 2006.

The Forester report recommendation are as follow:

- Gain Experience with non-critical applications
- Temporarily avoid organizational issues
- Sidestep licensing challenges
- Chose VMware for most deployments
- Develop a backup/snapshot plan
- Develop a management and ata center automation plan
- Build a long-term plan for metering shared services

Building DR solutions using VMWare and Replications

The goal of a virtualized datacenter and disaster recovery system is to protect business-critical production servers. The technique accomplish that by providing a proven protection for multiple production application servers by leveraging real-time data replication and virtualization technologies to create cost-effective, simplified disaster recovery architectures. Simply put, virtual machines enable to replicate application data from multiple production servers to a single disaster recovery target and failover to the disaster recovery target in the event of an outage. This section describes how virtualization software can be used with replication to provide solutions for challenging high availability and disaster recovery problems.

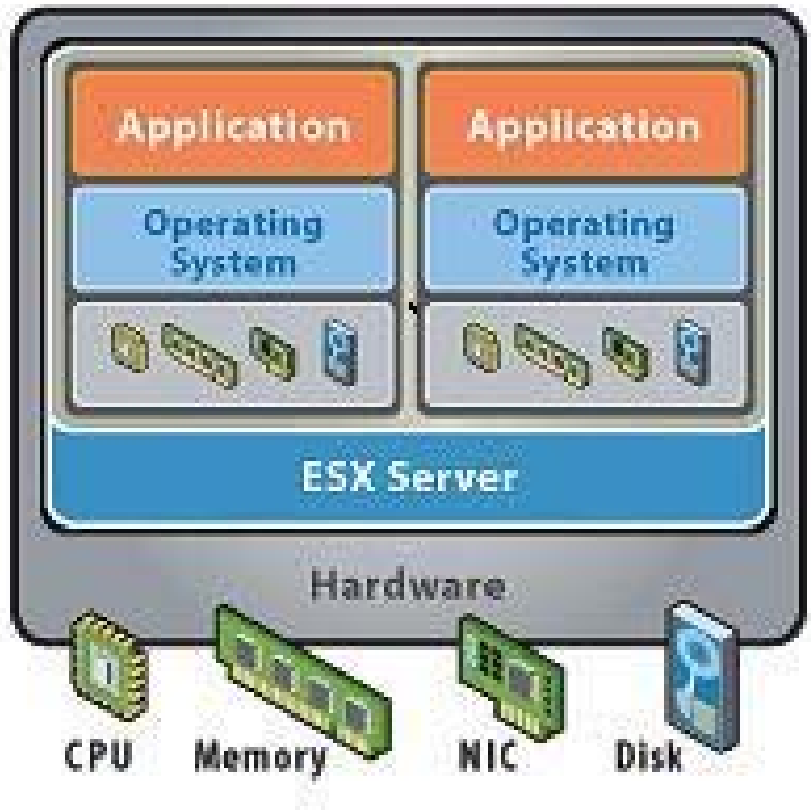
What is VMware Infrastructure?
VMware Infrastructure is the most widely deployed software suite for optimizing and managing industry standard IT environments through virtualization the data center. The production-ready virtualization software suite VMware Infrastructure delivers results in a variety of environments and applications at more than 20,000 customers of all sizes.

The suite is fully optimized, rigorously tested and certified for the widest range of hardware, operating systems and software applications. VMware Infrastructure provides built-in management, resource optimization, application availability and operational automation capabilities – delivering transformative cost savings and increased operational efficiency, flexibility and service levels.

VMware ESX Server is datacenter-class virtual infrastructure software for partitioning, consolidating and managing systems. ESX Server, included in Virtual Infrastructure, provides a highly scalable virtual machine platform with advanced resource management capabilities that can be managed by VMware VirtualCenter. ESX Server runs directly on x86 hardware, providing high performance and complete hardware resource control.

VMware VirtualCenter delivers centralized management, operational automation, resource optimization and high availability to IT environments. Virtualization-based distributed services equip the data center with unprecedented levels of responsiveness, serviceability, efficiency and reliability. VirtualCenter delivers the highest levels of simplicity, efficiency, security and reliability required to manage virtualized IT environments of any size.

A Primer on Server Virtualization Technology
In a national survey done by the Business Continuity Planners Association, nearly all companies which suffered disaster (81%) have taken actions as a result of the disaster to reduce business interruption in the future. The second most common change was to obtaining a back-up server (21%). Server virtualization technology, pioneered by VMware, allows one physical platform to run multiple virtual machines simultaneously. Adding an additional servers in this environment is relatively easy. Each virtual machine has its own processor(s), memory, disks and network interfaces. VMware ESX server provides a highly efficient virtualization platform that runs on the hardware platform and does not need any *host* operating system. In other words, it is a bare metal virtualization server. Functionally, each virtual machine is autonomous and unaware that the hardware is being shared. This allows multiple servers (even of different operating systems or versions) to run on one hardware platform.



VMware Server Architecture

One solution that this enables, for example, is for a single physical machine to support three different virtual machines:

- Microsoft Windows Server® 2003 running EDMS software
- A domain controller
- File and Print services

The domain controller virtual machine in the example above, a virtualized domain controller (DC), is useful for distributed branch offices that require a local DC but do not want to pay for the physical asset. In general applications that mandates separate hardware to avoid incompatibility issues and to maximize performance can be now share a physical hardware vi the virtualization mechanism. The key to these solutions is in the complete autonomy between virtual machines and their respective operating systems and applications.

"Many-to-One" Failover for Physical to Virtual Protection

One of the most interesting uses of virtualization technology in relation to disaster recovery is the use of virtual machines as disaster recovery targets. In NJ County there are about 10 production servers and recreating these servers at the disaster recovery site is a burden, expensive and may not be practical for from an acquisition as well as a

maintenance perspective. Consolidating multiple production applications to a single OS at the disaster recovery site is sometimes possible but is often complex, difficult and practically impossible to support.

By leveraging virtual machines as disaster recovery targets, NJ County can achieve a "many-to-one" failover scenario for their physical servers and reduce both the operating costs and complexity associated with their disaster recovery architecture. An example of this scenario (outlined below) illustrates four source production servers replicating and failing over to one physical target:

- Microsoft Exchange Server running Windows Server 2003
- EDMS software running Windows Server 2003
- Microsoft SQL Database server running Windows 2003 Server
- Microsoft Domain Controller

While each of these applications may run fine as the only application on each server, compatibility issues may arise by having three four applications installed and running on the same target server. Using VMware virtualization, and replication mechanism can provide for failover for all of these servers to one physical machine. The target server (running VMware ESX Server) would be configured with four virtual machines – each running the Windows 2003 Server OS tuned specifically to the application that runs on it.

During normal operation, the applications would be in a "down" state, allowing thre replication software to replicate changes to the protected data to these virtual machines in real-time. At failover time, the appropriate application services would be started within a corresponding virtual machine and and users will be redirected from the original production server to the standby server running within a virtual machine at the DR site. This would allow the target to provide high-availability for each of the protected servers.