

InsidePerspective

ACHIEVE THE POWER OF MEDITECH

Electronic newsletter published every 8 weeks

Virtualization: Considerations for Disaster Recovery

Jen Pixley, Core Technology Product Manager

According to Murphy's Law, whatever can go wrong, will go wrong. When talking about disaster recovery, this could range from a major power outage to a natural disaster. If an incident like this were to occur at your primary data center, how long would it take you to recover? Without a doubt, a major concern for any IT department is not only implementing a disaster recovery solution, but a manageable one.

By now we know that providing an adequate, complete, and robust disaster recovery solution for your MEDITECH HCIS requires specific backup and data replication technologies—and that's true whether your failover site is in the next room, a few miles away, or in another state. But one of the biggest challenges in recovery, and one that is sometimes overlooked, is how to fail over to servers at your disaster recovery site that look just like your production servers.

Your data may be protected through replication on storage, but how are your servers replicated? Adding virtualization into your technology mix can ease the pain of server recovery by offering flexibility and potential cost savings that you wouldn't get with non-virtualized servers.

How does VMware fit into your Disaster Recovery plan?

As you consider how virtualization fits into your overall disaster recovery plan, an important starting point is to identify your objectives and your tolerance for downtime based on each application. Determining how behind in minutes or hours your replicated copies can be from your production environment will help you map out your disaster recovery scheme for both your storage and server environment.

"Sure, I know that," you're thinking. "But do I need to incorporate virtualized servers into my disaster recovery plan and if so, how?"

Virtualizing your servers encapsulates the server into files. This means that your virtual machines can be copied, cloned, or replicated just like any other file. However, it also means that your running virtual machine behaves just like any other physical server, and therefore, must be incorporated into your backup schema.

Your backup and recovery options can range from utilizing a backup agent within the virtual machine, backing up the files from your ESX host server disk, or storing your virtual machine files on shared storage and relying on the backup procedures for your shared storage to protect your virtual environment. Choosing a backup method that replicates the virtual machine configuration files allows you to regularly duplicate the server state, image, and configuration which can be re-started at a different location rather than re-creating a server image from scratch in the event a recovery is required. Each method has advantages and disadvantages, and often a combination could be used depending on your disaster recovery goals.

Advantages of incorporating Virtualization into your Disaster Recovery plan

Virtual machines are, in most cases, hardware independent, but server platforms should still be considered

carefully for successful migration of virtual instances. In most cases, this enables the use of different hardware at your disaster recovery site than at your production site. Creating a failover site without virtualization typically requires that you build a duplicate site with the same hardware configuration. Hardware independence may allow you to re-purpose servers for disaster recovery applications and help maximize your IT investment.

When failing over from one physical server to another, recovery issues can occur if the configuration isn't exact. With virtualization, you have much more control over standardization and flexibility of virtual machine configurations. If designed properly, you can even implement a solution in which your virtual machine files are replicated and can be simply re-started in your disaster recovery environment when needed. Different levels of replication can be discussed to meet your disaster recovery goals and ensure that your replicated data is as up to date with production as needed.

Typically disaster recovery hardware sits idle until it is needed. In a virtualized environment, you can better use the equipment for testing or other non-production purposes and still ensure its integrity for disaster recovery purposes. The encapsulation of the virtual machines isolates each server instance so it does not disrupt the rest of the host environment. In the event of a disaster, any non-critical virtual machine can be quickly powered down and the server resources made available for failover virtual machines.

Additionally, using VMware consolidates the number of physical servers required which reduces the amount of power and cooling needed to sustain the disaster recovery environment, therefore reducing costs.

Know Thyself

Virtualization offers a lot of advanced functionality when implemented properly. Virtual infrastructure in conjunction with SAN and data replication technology can offer a high degree of protection within your environment. But, as we discussed in September's Virtualization article, not every server and application is a candidate for virtualization. (For a refresh of this article, see the Archives on the home page.) Before virtualizing your infrastructure, it is always recommended to perform a thorough assessment.

Since using the phrase "mission critical" doesn't seem strong enough when describing your MEDITECH HCIS, having a disaster recovery plan in place is key. Especially as Advanced Clinical application adoption moves forward, doctors and nurses rely on technology availability and even more. How will your IT staff handle an outage? How long will it take to recover? JJWild [now a Perot Systems Company] offers complete design expertise and solutions around protecting your entire MEDITECH infrastructure. If you haven't thought about disaster recovery in your environment yet, now is the time and VMware may be another technology to help you get there.

Jen Pixley is a Core Technology Product Manager for JJWild, focused on enhancements to our long-standing, integrated hardware and software products, as well as rollout of new, large-scale strategic product initiatives that impact the data center, such as virtualization. You can reach her at editor@jjwild.com.