

## Re: Fault Tolerance on SBS2003 Prem.

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-05/5393.html>

---

**From:** root (postmaster\_at\_buchanangc.com)

**Date:** 05/17/04

Date: Mon, 17 May 2004 14:17:35 -0700

"Jeff Middleton [SBS-MVP]" <jeff@cfisolutions.com> wrote in message news:elfzLmBPEHA.2960@TK2MSFTNGP10.phx.gbl...

> *Too often this topic is approached without defining any scale or costs. It leads to some interesting debate, but not nearly as much useful strategic information for a practical decision. Fault Tolerance and Disaster*

*Recovery*

> *are important topics, no doubt, but they are topics that need to be mapped on a scale of cost management, business priorities, and technical resource realities.*

>

> *The thing I noticed in your post, Chris, before I started, you are an MS partner, therefore you are not likely asking this question for your own consumption, rather for a strategic policy or plan for your own customers, right?*

>

> *There are no absolute answers when it comes to spending other people's money, or managing other people's risks if you don't bother to find out what*

> *THEY think about it. Therefore, I would recommend a really practical set of*

> *questions you should ask your customers in order for you to design an FT and*

> *DR plan that suits their needs. The key point that is so often missed is that most really small businesses are not actually going to prefer to pay a*

> *contractor \$12000 a year to avoid 1 lost day of work for the business.*

Precisely or even two.

> *I'm*

> *not saying that it's never going to be the case, I'm offering that for most*

> *small businesses, spending money on low probability risk protections isn't*

> *necessarily better than accepting the possibility of an unforeseen "snow day" in which the network is down due to a failure.*

>

- > *Of course, prevent any preventable condition that is easily cost justified,*
- > *but going to the extremes of labor intensive preventative steps isn't the*
- > *best answer. There is always a compromise involved in any business*
- > *decision, and it's the IT consultants job to include the owner of the*
- > *business in arriving at a suitable answer.*

Precisely and further it's the business of a good consultant to filter and foresee what the business needs really are as many small business owners aren't able to actually fully contemplate such decisions.

- > *So, let's take a look a list of questions you could ask the customer:*
- >
- > *1. Hypothetically, if a technical failure were likely to occur once in each*
- > *year that caused the total loss of function for your business for a period*
- > *of 4 hrs, how much would you be willing to spend in costs paid out monthly*
- > *to make that time be reduced to 1 hr?*
- > *\$200/mo?*
- > *\$500/mo?*
- > *\$1000/mo?*
- > *2. Same question, but what if the cost were a one-time expense when you*
- > *bought your new server, essentially something that you could spend on the*
- > *server equipment that improved the recovery time from an annual event from*
- > *4hrs to 1hr?*
- > *\$200/mo?*
- > *\$500/mo?*
- > *\$1000/mo?*
- > *3. Same question as the first one, but this time, what if the risk was a*
- > *failure that would cause you to lose an entire day of work, and the*
- > *improvement was only reducing the downtime from the full day to a 4hr*
- > *downtime?*
- > *\$200/mo?*
- > *\$500/mo?*
- > *\$1000/mo?*
- >
- > *Next set of questions, this time on data loss and loss of operations:*
- >
- > *1. If your company suffered an unpreventable incident that cause your*
- > *server*
- > *to crash at some point during the day, and a recovery of the system*
- > *required*
- > *a choice between longer downtime to recover data changes that day, how*
- > *would*
- > *you prioritize the following:*
- >
- > *4 hrs into the day's work, the crash occurs and in order to recover the*
- > *first 4hrs of data changes, you must keep the server down for 4 hrs., or*
- > *forfeit that technical data recovery process by returning to the start of*
- > *day condition within an hour and having your staff reconstruct the data by*
- > *re-entry? Would you prefer to miss the rest of the day's work, or give up*

- > *the data changes recovery?*
- >
- > *Same scenario, but what if the crash implied loss of 1 week of data, but*
- > *required 1 day of technical work?*
- >
- > *What is the maximum number of hours or days of work you would feel*
- > *comfortable in your company's ability for reconstructing if a technical*
- > *recovery was cost prohibitive or simply unavailable?*
- >
- > *2. List the types of information that you business maintains as data you*
- > *expect to keep stored on your server, and assign a value on a scale of 1 –*
- 5
- > *(5 is critical) what your priority would be in recovering information if*
- the
- > *cost was excessively high, but unavoidable:*
- >
- > *Email*
- > *Electronic Faxes*
- > *Word, Excel, Powerpoint files*
- > *Accounting/Line of business application based data*
- > *Technical or creative business records (Autocad files, scanned documents,*
- > *graphic design)*
- > *Contact lists, electronic calendar schedules*
- > *Legal documents*
- > *Records with Federal/State/Local requirements to maintain*
- > *Files and Data you possess which represent your own customer's*
- > *investment/expense to create*
- > *Photographs, Digital Video*
- >
- > *3. If it were possible to keep your business operating in some partial*
- sense
- > *for a day, 2 days, 3 days or a week, identify from the list you created*
- just
- > *above, how long your business could operate without the ability to update*
- or
- > *use each of those items, but assuming that you would regain use without*
- loss
- > *of the historical information, just the time delay?*
- >
- >
- > *From these questions, and others like them, you should be able to develop*
- a
- > *profile of the customer's needs that helps you to understand what costs*
- and
- > *tradeoffs for downtime they are willing to choose....if they have the*
- option
- > *to make the choice.*
- >
- > *Many small businesses will prefer to take a chance on missing a day of*
- work
- > *if it saves them \$5000 per year simply because many small businesses*

operate

> *on a basis where a delay of a day in work isn't that expensive to them.*

Not

> *many businesses would prefer to miss a day or a week of work, but that's*

not

> *the question here. The question for the owner is if you must pay in*

> *advance...forever losing that money invested for a risk with only a low*

> *probability of impact...would you simply pay or would you take your chances?*

>

> *At some point, this translates back to risk aversion and return on*

> *investment information that helps decide the budgets and expectations this*

> *owner has.*

>

> *The IT consultant's job is to then translate the options back to available*

> *technology and strategic planning initiatives.*

And to make a determination of what those needs/decisions are and should be.

Often the owner/bill payer doesn't know the exact answer to all the questions you pose. A good consultant will figure out what the business really does and what their vulnerabilities and risks are such that many of the questions you pose can be constructed around actual details of who is doing what and the risks/costs of interruption or loss.

> *Clearly, most IT consultants should make some basic decisions going in that*

> *are just part of a baseline assumption if at all possible:*

> *- a UPS on the server*

> *- a regular system and data backup*

> *- hardware that can be maintained by a vendor who will be around in a year*

> *or more*

> *- a reasonably standard installation that can be recreated and repaired*

>

> *But when it comes to the FT and DR issues, most of the issues are going to be measured as*

> *- downtime for maintenance*

> *- invested cost of equipment which provides no added value, only FT/DR*

> *functionality*

> *- routine fee costs of preventative maintenance*

>

> *...that vs.*

> *- cost of critical response*

> *- response time for a loss of operations event*

> *- downtime for recovery*

> *- data loss tradeoffs for technical recovery*

> *- unavoidable data loss due to a "window of time" during which there is no*

> *data protection in-place*

> *- emergency expedite cost for equipment replacement vs. stocking spare*

> *parts.*

> *- unforeseen downtime that an FT/DR plan doesn't address*

>

- > *When you present all this information, if the FT/DR plan calls for taking a*
- > *customer from a \$3000 server up to needing another \$3000 server, plus*
- > *another \$3000 worth of other hardware and software, plus \$12,000/yr in*
- > *preventative labor....you might find the owner just doesn't see this as a*
- > *great idea to invest in so that you have a "nothing can go wrong plan"*
- > *which*
- > *in fact, isn't really a fact anyway. You know, if the power goes off, even*
- > *if you have that backup generator in the yard to run the server, if you*
- > *can't run the workstations, telephones and air*
- > *conditioning/heat....chances*
- > *are the owner is sending the staff home anyway.*
- >
- > *If the DR plan calls for rebuilding a server in 1hr by spending \$15000/yr*
- > *in*
- > *prep work for that event, could just be the owner would rather take a day*
- > *to*
- > *go golfing and let the staff go home while you do a \$2000 repair day on*
- > *the*
- > *server. The owner might even forfeit the previous day's work rather than*
- > *paying \$3000 for more stuff or services. You don't know if you don't ask.*
- >
- > *And in the final level of details, the ones that other's posted thoughts*
- > *on*
- > *this thread with, there are very many good practical steps you can take to*
- > *improve FT/DR that include better hardware to begin with, reliable backup*
- > *operations, and strategic DR snapshots with drive images.*
- >
- > *As a rule of thumb, sort of arbitrary, but I start with getting a*
- > *validation*
- > *from the owner that most of my customers are able to survive a 4hr*
- > *downtime,*
- > *unless they identify why that's not the case in fact. A single server*
- > *environment with a contractor as IT support should generally be able to*
- > *address a four hour recovery in most situations, and the server should be*
- > *designed with that thought in mind. However, if you look at the nightly*
- > *back, you may well realize that if it takes 6 hrs to restore from tape, a*
- > *4*
- > *hr recovery may be hard to hit, right?*
- >
- > *In this case, having a second server and splitting the roles of the*
- > *servers*
- > *is probably the most likely way to cut the risks in half, or at least,*
- > *split*
- > *the risk by improving survival of some more critical operations. I rarely*
- > *find that having a duplicate server sitting cold at a customer office is*
- > *more valuable than having that second server operating in a valuable role,*
- > *but that's not an absolute situation. In offices where I have 4 or more*
- > *servers, I usually do have a strategic plan for switching roles of*
- > *servers,*
- > *or bringing in a suitable alternate package of hardware as needed.*

- >
- > *In the long run, the single most valuable skill an IT person can have in a*
- > *DR role is experience in rebuilding an installation on different hardware,*
- > *and the experience to know how long that will take them given a specific*
- set
- > *of tools. Identify what those tools are for your experience and technical*
- > *level, then practice with them. Quote your customer based upon this*
- > *experience and set of tools. For instance, it's my baseline preference to*
- > *have the following available to me at every customer server site:*
- >
- > – *FT drives, preferably RAID5 because a drive failure still isn't an*
- > *emergency if there's a hot spare, and a mirror is likely to cause a boot*
- > *failure even if the system/data is still preserved*
- > – *nightly backups to removeable media such as tapes*
- > – *UPS on the server*
- > – *Server is not used as a workstation or by local logons*
- > – *A system partition drive image has been prepared at some point in the*
- last
- > *yr., or during the last lift of major Service Pack update level.*
- > – *The server is running AV on the local system*
- > – *The server is running a backup program that provide job by job logging*
- > *history, not just last job*
- > – *I have either at my office or at the customer's location, another*
- computer
- > *which is reasonably suitable to load that disk image as needed.*
- > – *I have either at my office or at the customer's location, another drive*
- > *suitable to boot that drive image.*
- >
- > *The last two items in the list deserve a little more detail.*
- >
- > *Many people do not know or have the technical skill to reliably or*
- > *consistently implement a server recovery on different server hardware, or*
- > *even from a different set of boot drive hardware. For instance, I prepare*
- > *all my servers to boot from a drive image either on the native production*
- > *boot controller (typically a SCSI RAID) or in addition, from the onboard*
- > *EIDE controller. It's pretty simple to make this happen. Once you finish*
- > *installing the server OS, or at any time in the future, if you simply plug*
- > *in an EIDE drive and then perform a complete boot cycle and shutdown, you*
- > *will probably now be able to install a drive image of the RAID as a*
- restore
- > *onto EIDE drive in that same computer and boot from the EIDE with not*
- > *additional steps. (This assumes that the SCSI subsystem drives are not*
- > *attached at the time, otherwise you do need to indicate boot preference*
- for
- > *one of the two bootable subsystems)*
- >
- > *Furthermore, booting a drive image on different server hardware (different*
- > *motherboard) isn't really that complicated either. In fact, I think it's a*
- > *good idea for an IT consultant to be aware of what similar and dissimilar*
- > *server hardware they handle that is compatible to transfer and boot from.*
- As

- > a general rule, if you have the same boot controller (SCSI card or PCI EIDE
- > or SATA card), you probably can boot most any dual processor based
- > motherboard with the same Windows install provided the motherboard is recent
- > within the last 4 yrs and therefore ACPI compliant. Similar comment for
- > single CPU P4 is going to boot from a Windows Dual CPU install. Note that if
- > the motherboard is dual CPU socket, it's not relevant that you have only a
- > single CPU, it's a Dual CPU motherboard.
- >
- > The point at which you realize that most of the over-zealous FT/DR plans are
- > just overkill is when you see the look on a customer's face when you find
- > any means to get them back up and running quickly, using whatever resources
- > you have available.....and they are not paying a fortune for those
- > resources. Most customers really don't care if you use a PIII workstation
- > running on EIDE as a temporary workaround to having their production Dual
- > Xeon server with RAID5 go down by a lightning strike, or burst waterpipe, or
- > fire in the server closet. All that matters is that you can get them back up
- > and running on something.
- >
- > Building a technical nerve center that involves multiple servers adding to
- > the upgrade costs, the maintenance costs, and the purchase costs isn't
- > really the right answer for most businesses. The right answer is letting
- > them have a way to contribute to determining the costs to run their
- > business, to participate in the risk analysis, and to have an IT contractor
- > who is both competent technically, and has a sense of business reality as
- > well.