CLOUD COMPUTING

Disaster Recovery

Technical Considerations in a Windows Server Environment

INTRODUCTION

Cloud computing has changed the economics of disaster recovery and business continuity options. Accordingly, it is time many organizations revisit their strategies to ensure they are meeting business requirements. We have found it common for companies to have a mismatch between business continuity requirements and the strategies implemented for recovery/continuity. Why? Businesses have been reluctant to allocate funding for Disaster Recovery unless management fully understands the risks, and often they do not. Technology professionals have faced a large increase in cost and complexity in moving from basic disaster recovery to a fast and reliable applications recovery approach. That is - until the advent of cloud computing.

The focus of this paper is technology implementations using Microsoft Windows Server and optionally Microsoft SQL Server. Should other database technologies be involved, the method for handling them will be described in the section "Special Capabilities for Advanced Needs: Advanced Topic 1" below.

Cloud computing allows the company's data and applications to seamlessly reside on remotely located servers that are connected to the network. The flexibility to locate these servers and the stored data "in the network" allows functions to be performed more cost-effectively because of scale economies at the remote site. This paper describes these functions and capabilities and why the scale economies are important.

Traditional disaster recovery approaches, involving weekly and daily data backups, and the assumption that the network computing infrastructure can be quickly rebuilt following a disaster have proven inadequate time and time again. Businesses have migrated to the use of web applications for sales, customer support, supply chain management, healthcare medical records, real-time financial records and other transaction-based applications. Many of these transactions would be difficult to recover should the company have to roll back to a previous version of a database. Even when log files can be used to "catch up" a database copy with all transactions, the process depends on skilled company workers who might not be available to do the task.

Terminology

For this paper the term Disaster Recovery is used to describe processes to ensure data is moved to an alternate site and a plan for re-establishing the network computing environment exists regardless of how time consuming, but generally within days/weeks. Business Continuity will be used to describe a process where the data and applications can be quickly restored (minutes/hours), eliminating the time gap in the Disaster Recovery process; hence, the name Business Continuity. The business process requirements for Disaster Recovery and Business Continuity are generally defined on two scales:

1) Recovery Time Objective (RTO)
The goal for re-establishing a working network computing environment

2) Recovery Point Objective (RPO)
The point at which data can be recovered (e.g., to the last transaction, as of last night, as of last week, etc.)

Both scales are important considerations when assessing whether a technology strategy for Disaster Recovery or Business Continuity is meeting business process requirements, and cloud computing improves the economics of achieving various levels on both scales.
This leads to the desire to achieve a more automatic recovery that takes into account the need to recover data to the last transaction as well as a way to re-establish the network computing environment quickly with minimal need for company staff involvement. Cloud computing offers an opportunity to step up to this higher level of recovery capability at a cost that is palatable to nearly any size business.

This paper explores how cloud computing can effect this transition to a better recovery approach. Moving data and applications to the cloud might raise some questions about security, which we will address first. While many may think that cloud computing offers less security; in fact, the opposite is true as it offers a greater depth of security.

SECURITY AND THE CLOUD

People use bank safety deposit boxes instead of keeping important papers under their mattresses because of the physical security and best practice processes around which the documents can be accessed. Similarly, a cloud computing approach to maintain the safety of data can often provide a more secure environment than one that is managed in-house. Some of the features and processes cloud computing vendors utilize include:

1) Physically secure sites with 24x7 rigorous processes controlling access by people
2) Logically secure sites - up-to-date firewalls and other access control mechanisms
3) VPN (virtual private network) transfer of encrypted data over the Internet
4) Buildings with the most advanced fire suppression and other safety mechanisms

In summary, because of the importance of security to cloud computing customers, the vendors have applied best practices processes, highly skilled staff and ongoing management attention to this area. For most companies this focus by the vendors far exceeds their own in-house processes. Users have become satisfied with the safety of their information, even to the point of feeling more secure than in pre-cloud approaches.

TRADITIONAL BACKUP METHODS: HOW THEY WORK AND ASSOCIATED DOWNSIDES

Backing up data for servers located in a company datacenter has traditionally involved periodic backups to tape or other media and use of an offsite storage facility, possibly that of a service provider.

The file backup process steps include:

- directories with files to be backed up are identified.
- groups of files are identified for backup using Windows Server backup tools.
- a time to perform the backup is selected also using Windows Server tools.
- a destination location is identified.

This approach is a holdover from the days of batch systems when at some point during a nightly processing run, the files were considered “updated” and a nightly backup performed.
Periodic backup approaches have their limitations:

1) Tape backup is prone to human error - requiring physical movement of tapes.
2) It is easy to miss required files - especially those only created at certain times of the year.
3) Tape records are sometimes unreadable, especially on old tapes.
4) The data is only current to the last backup. Increasingly, this is not sufficient as more transactions are captured via web transactions.
5) Data backup alone does not address recovery times caused by the need to rebuild the technology infrastructure following a disaster, and this gap in system availability has become unsatisfactory for many businesses since it would result in an outage affecting customers and power users.

A variation of the tape backup approach is use of FTP to move files electronically over the network to an offsite location where the files reside on disk until needed (disk to disk backup). This has the same limitations listed above except for tape handling.

For situations where SQL Server is used for data storage, the database can be treated as a whole (as a file) and backed up in the same manner as other files. Often these files can be very large, and as a result backing them up as a single large file can require a combination of a large amount of bandwidth and time to transfer the file over the network. Some users turn on the SQL Server replication feature (available in the Enterprise edition) to create redundant copies of the database in-house. That provides protection against server and disk failures but does not suffice for disaster recovery purposes as it fails to establish geo-redundancy. Only by replicating SQL databases over the network can protection be achieved, which leads to the next subject.
CLOUD COMPUTING CHANGES BACKUP AND RECOVERY

HOW IT WORKS

Data can be pushed to the cloud over the network, using VPN (virtual private network) technology to ensure security of the data. This approach works for files (a periodic backup approach) and for SQL databases (a transaction by transaction replication approach), assuming the SQL Server version used supports the replication function. This will enable RPO business objectives to be met for all but the most stringent requirements.

In addition, the cloud vendor can offer virtual computing resources capable of handling processing for the various applications to be recovered, providing a way to address RTOs. Since the data is at the cloud vendor site and the virtual network computing infrastructure is in place, recovery is as straightforward as enabling the applications and linking them to the backup data.

For many companies this provides the step-up in capability to make it possible to overlap business requirements with the implementation strategy. The following diagram shows how this is accomplished using virtual infrastructure in the cloud.

Cloud Computing and Recovery: Virtual Infrastructure

- In-house infrastructure pushes backup data over the Internet, using a VPN tunnel for security.
- The data, both periodic file copies and transaction by transaction SQL updates, is received in the virtual infrastructure (at a hosting vendor) and stored for use, and if necessary, for recovery. The SQL updates are applied to the database at the backup site, keeping the recovery SQL database synchronized with the production one. Note that file copies can and should include application programs as they change.
Virtual servers are defined and ready to operate if needed in the event of a failure of the in-house infrastructure. Applications can be pre-loaded with or without product keys, depending on how quickly recovery is required. The primary and backup virtual machines need to be kept synchronized over time, as software updates and other configuration changes are made. For example, processes are needed to ensure application software at the remote site is identical in version to that used at the primary site. This requires rigorous change control processes be established and followed, practices needed regardless of the recovery approach.

- The external users are redirected to the cloud site at time of recovery. How this is accomplished is described later in this paper.

ENSURING THAT THE RECOVERY SOLUTION WORKS

No disaster recovery solution should be counted upon to work unless it is thoroughly tested on a regular basis, and all issues identified are addressed through a process that involves retesting once the corrections have been made. There needs to be a strong linkage to a change control process to ensure the backup solution represents the way business is currently being handled at the primary location.

When testing has not been done, the issues identified when recovery is attempted both delay the recovery process and introduce the chance for serious errors, especially since the staff is working under pressure and often skilled resources may not be available. In addition, testing will uncover areas where not just technology personnel but also business operations personnel need to become involved, and will highlight what their capabilities need to be.

Testing should simulate as much as possible a real life situation; for example, the need to test recovery should be announced with no warning and without concern for the availability of all key personnel.

SPECIAL CAPABILITIES FOR ADVANCED NEEDS

The cloud computing approach described above will address the needs of many users.

For users with large files, databases or large stores of emails, they may want to explore the use of de-duplication software which both reduces the amount of data that must be stored, but in replication scenarios it reduces the amount of data that must be transmitted.

Some businesses have critical applications that push the RTOs and RPOs further, and that requires implementation strategies that can accommodate them. Three areas will be discussed:

1) Use of Storage Area Network to Eliminate Data Loss
2) Pre-Loaded Applications to Shorten Recovery Time
3) Automatic Network Failover to Shorten Recovery Time
ADVANCED TOPIC 1: USE OF STORAGE AREA NETWORK TO ELIMINATE DATA LOSS

The Issue: As covered above, SQL Server database technology Enterprise edition offers an option - that of replicating changes to the primary database on a transaction by transaction basis to the database copy. This is accomplished in near real time - with some small exposure that the replication of a transaction, or small number of transactions, may not occur immediately after an interruption due to a disaster.

The exposure that a small number of transactions occurring just prior to a disaster may not be captured in the replicated database is an issue for some companies and applications. They may not have a practical manual work-around to address this small exposure. The businesses with stringent RPOs that are not satisfied with an asynchronous database replication solution can have their needs met with a synchronized approach. This requires a more sophisticated technical solution described below.

Terminology

Replication can be done synchronously or asynchronously. Synchronous replication requires the application to wait until it knows that both copies, primary and backup, have been successfully written before proceeding. Asynchronous replication allows the application to proceed without confirmation under the assumption that the infrastructure will complete making the replicated copy. There is an exposure that this asynchronous replication activity can be interrupted at time of disaster, affecting the last few transactions.

The Technology: Storage Area Network (SAN) technology is a proven approach to ensure that data exists in identical form over a wide area network, generally using fiber channel protocol over an IP WAN (Internet Protocol, Wide Area Network). Its only drawback is cost. Cloud computing helps address the cost issue through scale economies. A number of quality vendors offer this functionality.

The Solution: The implementation involves SAN technology installed at both the in-house and virtual recovery locations and manages the replication of file and database data using the most advanced techniques. It should be noted that compatible SAN technology is required at both ends.

The SAN has the intelligence to manage the replication process and to communicate with applications regarding the completion of the update to the local and replicated copy. It is this intelligence that allows for a synchronous approach to replication, eliminating the risk of lost transactions.

An additional benefit of SAN technology depending on vendor implementation is that it can accommodate selected non-Microsoft files and databases, making replication over this vehicle possible.

Alternative Solution: The primary datacenter is relocated from in-house into the cloud, operating on hosting vendor infrastructure that already has the SAN technology at its primary and secondary locations. The cost of using this approach would most likely be less than implementing a SAN in-house.
Use of Storage Area Network: Ultimate in Data Protection

Files also can be replicated on a real time basis, if needed. This is an advantage not available in the SQL Server replication approach. In addition, if there are non-SQL databases, this approach can accommodate replication of them as well. As covered before, file replication can be used to update remote copies of run time versions of application programs following changes to them - a step that can be part of the change control process and ensure that when in recovery mode, the application software is the most current version.

ADVANCED TOPIC 2: PRE-LOADED APPLICATIONS TO SHORTEN RECOVERY TIMES

The Issue: Applications need to be installed, and software product keys entered. This can take time and requires involvement of someone with knowledge of both the software and the keys. Note that software vendors are not standardized on terms for allowing backup copies of software to be used: some allow a backup copy to be installed subject to rules of use; others do not.

The Technology: The virtual servers at the cloud hosting vendor site are operationally ready when needed and can be started from a remote site as needed.

The Solution: It is possible to pre-load application files at the cloud hosting site and enable them with keys at the time of disaster. If this solution is used, the change control process needs to include steps to ensure that any changes or updates to application software get replicated to the remote site immediately.

Solution 1: Pre-load applications and product keys, essentially making the applications ready to run if transactions are presented to them.
Solution 2: Some hosting vendors offer “tenant” software-as-a-service applications, fully supported and at lower cost than licensed versions. For example, MS Exchange can be licensed in the cloud, such that it is paid for only when in use.

ADVANCED TOPIC 3: AUTOMATIC NETWORK FAILOVER TO SHORTEN RECOVERY TIME

The Issue: Stringent RTOs requiring instant recovery need to have a way to minimize failover time.

The Technology: For web transactions, the destination location is found using an IP (Internet Protocol) address or host name with the Internet Service Provider (ISP) providing the matching of the address to a physical location (“Domain Name Service” or “DNS”). ISPs have the ability to keep a list of physical locations so that if the first doesn't respond, it will try the second, and so on. Various ways available for addressing network failover will be described in the “solutions” below.

Solution: The backup site control software alerts operations personnel that the primary computer site is not responding. The network operations personnel can initiate a command that switches the network to the alternate location, i.e., initiates failover of the network. Failover along with pre-loaded and ready-to-go applications (Solution 1) and replicated data, provide an approach capable of meeting very short RTOs.

Alternative Solution: An infrastructure designed with load balancing across two physical sites, including replicated data at each site, can react to a missing location at time of disaster in a seamless manner. This approach is ideal for extremely stringent RTOs.

Use of Automatic Network Failover
CHOOSING AN APPROACH

Cloud computing provides a way to move from the center column in the table below to the right column with significantly improved recovery capabilities at minimum cost.

An Improved Recovery Approach Through Cloud Computing

<table>
<thead>
<tr>
<th>Cloud Computing Makes Business Continuity Feasible</th>
<th>Disaster Recovery – Before the Cloud</th>
<th>Business Continuity Using the Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RPO</strong> Recovery Point Objective for Data – ranging from the last periodic backup up to the last transaction</td>
<td>Data available from the last backup – e.g. last night/last Sunday</td>
<td>Data backed up to the last transaction</td>
</tr>
<tr>
<td><strong>RTO</strong> Recovery Time Objection – time to re-establish the network computing environment ranging from minutes to weeks</td>
<td>Recovery time variable due to many possible screen – generally days or weeks</td>
<td>Recovery in minutes or hours since the infrastructure is already in place</td>
</tr>
</tbody>
</table>

There is a clear difference in the ability of the various data backup approaches to meet business RPO and RTOs. Matching the business requirements with a recovery/continuity strategy should be the goal. Various approaches can be used to address cost issues as outlined below.

RPO and RTO objectives are unique to each business, but some general statements can be made:

1) Generally, accounting systems can be satisfied with nightly backups.
2) Order entry, customer service or other mission critical applications benefit from an approach involving replication of databases at the backup site.
3) Recovery times are greatly shortened and risk reduced if the remote site has an approach for quickly starting the replacement infrastructure, enabling applications and “failing over” the network to the recovery site.

The following chart summarizes the relative merits of various data backup approaches for meeting RPO and RTO (on a scale of “1” to “5” where “1” is very ineffective up to “5” which is very effective):

**Data Backup Approaches and Effectiveness for Meeting RPO and RTO**

<table>
<thead>
<tr>
<th>Approach</th>
<th>RPO</th>
<th>RTO</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN – Replication via Network</td>
<td>5</td>
<td>5</td>
<td>$$$$ - unless using hosting vendor</td>
</tr>
</tbody>
</table>
CLOUD COMPUTING
Disaster Recovery

<table>
<thead>
<tr>
<th>SQL – Replication via Network</th>
<th>4</th>
<th>5</th>
<th>$ - very good in combination with FTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP – File Copies via Network</td>
<td>3</td>
<td>3</td>
<td>$ - consider for non-critical apps</td>
</tr>
<tr>
<td>Tapes – Copies of Files Kept Off Site</td>
<td>2</td>
<td>2</td>
<td>Clumsy and error prone</td>
</tr>
<tr>
<td>Tapes – Copies of Files Kept on Site</td>
<td>1</td>
<td>1</td>
<td>High risk</td>
</tr>
</tbody>
</table>

**IMPLICATIONS OF USING A HOSTING VENDOR: PERFORMANCE AND COST**

The good news is that Cloud Computing is changing the cost structure and is making possible a higher quality recovery option at reasonable cost. Some of the considerations are highlighted in the table below:

**Data Backup Approaches and Effectiveness for Meeting RPO and RTO**

<table>
<thead>
<tr>
<th>Approach</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN</td>
<td>Hosting vendor scale economies can make SAN affordable</td>
</tr>
<tr>
<td>Multiple Datacenters</td>
<td>Multiple Hosting vendor sites are interconnected and have similar operating characteristics, ideal for both home site and backup site implementation</td>
</tr>
<tr>
<td>Network</td>
<td>Hosting vendor scale economies make network redundancy between hosting vendor sites affordable</td>
</tr>
<tr>
<td>Applications</td>
<td>Hosting vendor “tenant” software-as-a-services applications can reduce licensing costs</td>
</tr>
<tr>
<td>Tapes Kept Off Site</td>
<td>Hosting vendor retention processes likely to be more reliable than in house solutions</td>
</tr>
<tr>
<td>Skilled Labor</td>
<td>At Time of Disaster (ATOD) skills of Hosting vendor brought to bear at potential time of need</td>
</tr>
</tbody>
</table>

**SUMMARY**

Cloud computing provides an easy to implement, cost-effective approach to business continuity. It provides the alternate site needed for data replication as well as application and infrastructure recovery without the need to build, provision and operate an alternate site.

Cloud computing provides the software vehicles for controlling the environment, pushing data from the primary datacenter to a safe haven, and for bringing the data back home following rebuilding the primary datacenter.
Hosting vendors have skilled personnel managing functions that are critical to operations. At time of disaster a business may find its technical staff involved with family or addressing damage from the disaster. Having the skilled personnel familiar with the infrastructure and control software provides an additional level of assurance that recovery can be accomplished quickly.

The evolution to cloud computing has made traditional backup approaches obsolete. Previous backup methods did a poor job of protecting business processes from interruption. Cloud computing offers a superior approach that can meet the RTOs and RPOs that businesses need in a world of increasingly critical applications and dependent business processes.