dynamic
solutions
international

Cloud-Based Storage Solutions for MCP/AS and Open Systems

By Victor A. Ludlam

Copyright

It is believed that the information contained in this document is accurate and reliable, and much care has been taken in its preparation. However, no responsibility, financial or otherwise, can be accepted for any consequence arising out of the use of this material. **THERE ARE NO WARRANTIES EXPRESS OR IMPLIED IN THIS DOCUMENT.**

Correspondence regarding this document should be addressed to:
Dynamic Solutions International, Inc.
Product Development Group
1 Inverness Drive East, Englewood, Colorado 80112
(800)641-5215 or (303)754-2000
Technical Support Hot-Line (800)332-9020
E-Mail: support@dynamicsolutions.com

Table of Contents

Overview:

Dynamic Solutions, International (DSI) has been a leading provider of storage solutions for over 35 years, serving countries around the world. DSI does extensive research on new storage solutions and methods, and brings viable solutions to the market. Cloud-based storage and storage vendors have been extensively evaluated by DSI, and this position paper is intended to provide best practices and recommendations for using cloud-based storage solutions in the Unisys MCP, MCPvm, and Open (Windows, HPUX, AIX) environments.

What is Cloud-Based Storage?

Simply put, cloud-based storage is a methodology that stores your backup data remotely. Typically, the client would hire a third-party to hold their backup data, and that data would be transmitted to the third party via a network connection, usually by Secured-Sockets-Layer (SSL) Internet connections, or by some type of private connection (dedicated fiber). The storage array holding the client data may be in the state, or could be in another country. The major difference is that cloud-based storage for backup is an alternative to using standard in-house backup methods, such as physical tape, virtual tape, D2D shadow copies, etc. The advantage of cloud-based storage solutions is that the data is not only backed up, but also fulfills the off-site storage requirements of many clients, without the perils of physical tape movement.

Cloud-based Storage has become a bit of a generic term. For instance, simply transmitting your backup data to another machine within your network could be considered a 'private cloud'. The location of the cloud is not important – the idea is that the backup data exists somewhere other than the primary host, and it got there by some type of transmission means, as opposed to cutting a physical medium and loading it on the backup server.

The Basics of Implementing Cloud-Based Storage:

Most storage providers will require some interface software to connect to the remote storage. This could be an application, or a simple Java interface to a web-based client. The client software may be loaded on a machine directly (in the case of a single-server backup), or a separate appliance is used to house the application. In the separate appliance method, backup data from various servers are sent via the internal client network to the cloud storage server, and that server controls the backup timeframes and methods to send data to the remote storage provider. The client can be charged for the amount of remote storage used, a monthly/annual fee for use of the client software, and if a dedicated appliance is used, the list price of the appliance configured to handle the data to be held until transmitted to the remote server.

Implementing Cloud-Based Storage on Unisys MCP/MCPvm Systems:

Nearly all cloud-based storage solutions are focused on byte-oriented file backups. That presents a problem for Unisys MCP/OS2200 systems, where files have a specific structure and definition, as opposed to just a stream of bytes. On Unisys MCP systems, a utility titled WRAP can be used to create a 'container' that preserves the MCP file attributes. That container file can then be transmitted via open systems Internet connections to another host, and guarantee that the file attributes can be preserved. The DSI FileManager product is cloud-aware, and has been written to create client backups using the WRAP utility, and interfacing to third-party remote storage providers to create a seamless backup solution. For more information on FileManager and interfaces to a cloud provider, contact a DSI Support Consultant.

The Different Types of Cloud Storage Solutions and Considerations:

There are a number of remote storage providers available to the client, and they range from a target marketplace of the home user to enterprise-scale solutions. The proper implementation of a remote storage solution depends upon the backup requirements of the client.

In general, there are two types of cloud storage providers – those that are centered on data archival, and those that are centered on data restoration. Archival-type providers will hold data on remote storage indefinitely until it is explicitly removed. Archival-type cloud storage providers generally charge on a 'storage-in-use' basis, and some contracts will allow for periodic automatic increases in storage leasing. Most archival-type providers are enterprise-level cloud storage providers.

Restoration-type providers are geared toward the restoration of data at a given point in time. These providers also charge on a storage consumption basis, but may include automatic controls to manage the storage use, such as automatically removing files that have not been backed up for 30 days. Since these providers are geared toward restoration, a given directory that is backed up every day may not include files that were removed from the source directory days ago. This may be unacceptable for a client backup requirement, and is not a viable mechanism to house data that requires long-term data retention, such as year-end data. Most restoration-type providers are small business and home user providers. However, some of these providers provide a 'business use' version of their software which alleviates some of these concerns, and emulates more closely the enterprise-level archival-type provider.

As well, the client's backup methodology should be considered when using a restoration-type provider. A methodology of using a periodic Full backup with subsequent Incremental backups could be in jeopardy if the Full backup is automatically removed due to lack of use. However, nearly all vendors do provide some recovery period for idle backups by off-loading them to tertiary storage. However, this could greatly increase recovery times when a restoration is required.

Service Level Agreements (SLAs) are also a key to the client's choice of a remote storage vendor. Some vendors might 'roll out' your data to another storage medium, and could take some time to be available for restoration. Review the individual contract information carefully to ensure that your cloud-storage backup methodology can withstand a potential delay of data being available for restoration.

Lastly, the client needs to consider where their remote data will reside. In some cases, and in some industries, data from a company or government entity may be prohibited from being transmitted to a remote storage facility in another country. Moreover, remote facility encryption in another country may not comply with United States encryption standards mandated to a particular industry.

What Solution is Best for My Enterprise?

When considering a cloud-based storage vendor for your backup requirements, consider the following items:

1) Transmission speed. A backup that occurs every 24 hours has little use when it takes 48 hours to complete. The vendor must be able to handle your data rate. Consider the best possible speed out of your site, and ensure the vendor can handle that data rate. Some vendors will 'throttle' transmission speeds during high activity periods.

2) Data volume. How much data do you need to send to a remote storage vendor? The amount of data coupled with transmission speed will dictate whether a remote storage solution is even feasible.

3) Encryption. If the vendor does not provide it, then you must encrypt all data before transmitting to the remote storage server. There are a number of third-party products that will encrypt data on a local host, and can provide some compression before transmission.

4) Control. The software from the remote storage vendor may not have an external trigger mechanism. This could leave you vulnerable if a remote storage backup starts at a specific time, and the host has not yet completed the backup due to some delay.

5) Cost. Typical costs for cloud storage consist of two parts – a monthly fee, and storage costs. Consider the amount of data you will require to be held at your remote storage vendor. This is typically the largest portion of monthly costs.

6) Retention. How long will a storage vendor keep your data? Some vendors will only retain dormant data for 30 days. Moreover, if a given file is excluded from a backup set, some vendors will immediately remove that file from the remote storage in order to preserve your storage quota. Know what your backup requirements are, and ensure that the solution fits within your long-term storage requirements.

7) Restoration. A backup has little use unless you can restore the data that has been lost, within a timeframe you can tolerate. Carefully review the SLA

(Service-Level Agreement) with your prospective cloud storage provider. Ensure that if your data has been 'archived', or 'rolled-out' of directly accessible storage, how long will it be before your data is back on-line? Ensure that your restoration commitments fit within a potential SLA commitment.

In Summary:

Cloud-based storage solutions can lower your IT costs. Tape media and peripherals can be expensive, they require manual handling by employees to move off-site, and if not encrypted, expose a vulnerability to loss of data/data breach regulations. In some industries, transmission of data storage to a foreign country is highly regulated, or in the public sector, strictly prohibited. This is not unique to United States regulation. Recently, China is working to adopt new regulations regarding personal Chinese employee information from being transmitted or stored outside of their country. Data availability will be a key to implementation. In some cases, the cloud-storage solutions available could be used as a tertiary backup solution. This can be highly valuable to clients that have a Disaster Recovery site that is relatively close to the Production site, adding a level of data protection.

While cloud-based storage solutions promise to lower IT costs, there are many factors to consider whether cloud-storage is feasible for a given client.

Appendix A of this paper provides some links to articles that may assist the reader in determining whether a cloud-storage solution is right for your enterprise. Appendix B of this document outlines the DSI recommendations for best practices for an MCP/AS environment. The remaining appendices detail the DSI testing of individual cloud-storage providers, and DSI recommendations for use of each provider.

DSI is a leading provider of data storage, regardless of the medium. If you have questions regarding a potential cloud-storage solution, DSI can help. Engage a DSI Support Consultant to help you find the right solution for your enterprise.

APPENDIX A:

Links to cloud-based Storage Discussions:

Use CTL-click to access the links below.

The link below discusses the current trend of businesses looking to store data in countries with more lenient data-breach notification requirements:
Data Breach Notification Laws Influence Storage Location Decisions - Security - Security administration/management - Informationweek

The link below comes from new changes in law within the United Kingdom to protect and regulate international transfer of data:
Introduction to overseas transfers of personal data

The link below is to an article written by Michael Chertoff, previous Homeland Security Director, and now CEO of the Chertoff Group. This article shows how international law is in flux with regards to foreign storage of data, particularly with regards to the public sector:
SafeGov.org - Data Sovereignty in the Cloud: The Issues for Government

The link below indicates that China has recognized the issues of foreign storage of data, and are taking steps to regulate:
China draft rules propose that Chinese employee data cannot be stored overseas - 24 March 2011 | AustCham Beijing

The link below tracks how individual states are proceeding in providing on-line notifications of a potential data breach:
- US State Data Loss Notification and Freedom of Information Legislation | DataLossDB

The link below explains the current HR 1221 law regarding breach of data (The Data Accountability and Trust Act) in layman's terms:
Federal Data Breach Bill (H.R. 2221) Passes House | DataLossDB

Current law is in flux, and data accountability and location is a primary focus. The link below is currently offered legislation, known as the Data Accountability and Trust Act (DATA) of 2011 (HR 1841):
H.R. 1841: Data Accountability and Trust Act (DATA) of 2011 (GovTrack.us)

Nearly all financial institutions are faced with PCI (Payment Security Industry) security standards as a new regulation. The links below connect to a Frequently-Asked-Question site (FAQ) that links to other articles on PCI compliance, and the Oxford opinion of new PCI regulations:
PCI DSS FAQs
PCI compliance standards updated for cloud-based storage

APPENDIX B:

DSI Best Practice Recommendations for MCP/AS Systems:

During the DSI research and testing, we found a number of settings, options, and features in each product. The following is DSI's best practice recommendations:

1) Whenever possible, use the vendor's compression methods to limit the amount of data being transmitted. If the vendor does not have a compression method, consider a third-party compression technique prior to transmitting a backup.

2) DSI highly recommends that the client control encryption locally and no file should ever be transmitted without having been locally encrypted. Nearly all cloud-storage vendors provide encryption-on-the-wire, and will provide a local de-encryption key on one of their servers to decrypt client data. While most storage vendors provide encryption-at-rest, encryption-before-transmission ensures that the client retains control of encryption keys, and not subject to attack.

3) If a client elects to not provide local encryption before transmission, the vendor of choice *must* provide encryption during transmission, and encryption at-rest on the remote cloud storage device. This is critical to ensure that client data is protected once it has been removed from the direct control of the client. In the absence of an encryption mechanism, use a third-party software product to ensure the data is encrypted prior to transmission. By default, the data will be encrypted on the remote storage.

4) Whenever possible, use a stand-alone server to provide the interface to the cloud storage solution. That is, a dedicated server receives backup data from multiple hosts, and controlled transmissions only occur from that machine. This provides a firewall between the client data and the remote storage, ensuring that data is controlled and encrypted before transmission, and provides a machine that can be highly secured for a single function.

5) If the backup solution must reside on a server or platform that has other functions, ensure that this machine is highly secure, and only allows port traffic for backup from your remote storage provider. Your provider will be willing to assist you in ensuring that backup data only flows to their servers, and help you ensure that the backup machine cannot be compromised.

6) Most solutions provide some type of throttling mechanism to ensure that the primary function of a server is not compromised during a remote storage backup operation. A DSI support consultant can help you determine the right settings for your storage vendor in your given environment.

7) Determine the final remote storage location of your data to ensure that you are in compliance with Federal/PCI regulations (see Appendix A). The destination of your data should be included in your SLA (Service-Level-Agreement) with your remote storage provider.

8) Pay particular attention to the retention levels of data with your proposed provider. Again, some vendors are geared toward restoration of a certain directory, rather than archival of long-term data.

APPENDIX C:
Using I365 (EVAULT) for Cloud-Storage on MCP/AS Systems:

DSI tested the I365 vendor, using FileManager to interface to the I365 components. The I365 solution requires the installation of agent software on some client server that will act as the surrogate for cloud-based storage transfers. I365 is an enterprise-level (i.e., archival-type) remote storage provider. If requested, I365 provides an appliance that will act as a 'private-cloud' storage solution.

MCP/AS testing was completed using FileManager to create a WRAP file of MCP/AS data, and forwarding to the I365 server interface. DSI recommends the following settings when using the I365 product.

1) I365 provides for various settings during file transfer to the cloud-storage subsystem. DSI recommends that files are encrypted on the local server prior to transmission, but the AES256 method be selected for data transfer. The client software does provide for lower forms of encryption to accommodate foreign data transfer encryption methods. DSI used TDES in this test, and found little difference in file prepration.

2) I365 also allows for a local data-deduplication method prior to transmission. This is likely to be ineffective when transferring MCP WRAP files to the cloud, since nearly every file within the WRAP file at least changes the BACKUP date attribute. However, DSI testing did reveal that setting this option did yield some compression results, and did not adversely affect the backup times when I365 was running on a dedicated server. Enable this option by passing in the DELTA=YES option when using the Command-Line-Interface. If the server using

3) The I365 agent software does allow for a CLI (Command-Line-Interface), and the transfer to the cloud-storage array can be controlled via the MCP/AS System running FileManager. I365 work flow examples have been included in the 9.069 release of TapeManager/FileManager to assist the client in automating the sequence of backup steps.

4) Once the MCP/AS system has completed the transfer of the FileManager WRAP file, it is recommended that the MCP/AS system start the transfer to the remote storage site. This can be accomplished through the I365 CLI interface, as follows:

   ```
   vv.exe backup DSIBkupFTP /DELTA=YES /COMPRESSION=MAXIMUM
   ```
   where DSIBkupFTP is the backup name that has been defined in the I365 GUI Interface.

The COMPESSION setting is the DSI recommended setting for a dedicated third-party server. DSI found little difference in wall-clock time for cloud- storage backups, and the MAXIMUM setting may provide a bit shorter transmission time. Shared servers may require CPU to handle other functions, and may elect for a smaller compression setting.

See the FileManager documentation for the 9.069 release, and the EXAMPLE/WFL code examples for more information on how to implement the I365 methodology.

APPENDIX D:

Using MOZY.COM for Cloud-Storage on MCP/AS Systems:

MOZY.COM is a cloud-based storage vendor that is a restoration-type provider. The system uses a java-based interface that resides on a Windows-based server. Implementation of MCP-based backup was tested using FileManager to create a WRAP File, and transfer that WRAP file to the MOZY server for transfer to the remote cloud storage.

DSI recommendations/observations of the MOZY.com provider are as follows:

1) There is no compression mechanism, and there is a single standard encryption which ensures encryption during transmission, and encryption at-rest on the remote storage device. Again, DSI recommends that encryption remain under control of the client, and any data transmitted be encrypted using client-based encryption software prior to transmission outside the client environment. The MOZY interface is quite simple, but limits the selection of specific options.

2) MOZY does allow for the definition of backup criteria. DSI would recommend that the client create a directory specifically dedicated to MCP WRAP files.

3) MOZY advanced settings do allow for throttle control. That is, backups can be delayed based on current CPU Usage, time of day, etc., which makes this solution a good candidate for clients that cannot dedicate a server to cloud-storage backup.

4) Created backup scenarios can be started by time, or via a CLI interface. In order to start the cloud-storage backup as soon as the MCP WRAP file has been delivered to the MOZY server. Use the following syntax to start a MOZY transfer remotely:

   ```
   mozyprobackup.exe /backup
   ```

   Note that this syntax will start all defined backups under the MOZY interface.

5) MOZY is a restoration-type provider. Remember that these vendors lean toward data restoration, not archival. Files that are archived could be automatically removed after 30 days. As well, this method may not backup everything. Example, if File A and File B exist in a directory DATA, and the DATA directory is backed up on day 1, and File B is removed – Tomorrow's backup of the DATA directory will exclude File B, and the backup of that directory will only include File A.

6) When looking at this solution, look at the MozyPro version for business solutions.

APPENDIX E:
Using CARBONITE.COM for Cloud-Storage on MCP/AS Systems:

Carbonite was tested using an MCP WRAP file generated via FileManager, and investigating the results.

The Carbonite solution is very generic, and more geared toward home PC users. However, it does have a few advantages. DSI recommendations follow:

1) Carbonite is employed by downloading their agent software to a server. This server would be the interface to the remote storage. Carbonite offers a free 30-day trial.

2) The interface is quite simplistic, with very few options. DSI does recommend that any backup configured use the 'Reduce Carbonite's Internet Usage' option. This is a compression technique that may reduce transmission times.

3) When configuring Carbonite, select a directory that will hold the incoming MCP wrap files. Note that Carbonite, by default, does not back up Windows code files or applications.

4) Carbonite is a restoration-type provider, and may not be appropriate for long-term data storage, such as year-end data retention.

5) When considering this solution, use the Carbonite Business solution for the 30-day trial. At the end of the trial, Carbonite will provide an estimated cost based on your storage usage.

6) One large advantage to Carbonite is that an MCP/AS system does not have to trigger a backup after transfer of an MCP/WRAP file to the server hosting Carbonite. Carbonite continuously looks for changed in the directories selected, and as soon as a new file (or file change) is detected, Carbonite automatically begins a cloud-storage backup.

7) Carbonite does provide for encryption-during-transmission, and client data is encrypted at-rest on the remote storage facilities. Currently, Carbonite generates a specific key for your data, and holds that key on a Carbonite server for your use during restoration. Some clients may find this acceptable, but DSI strongly recommends that ANY data moved to any cloud-storage provider be encrypted on a local server prior to transmission, ensuring that the client maintains control of the encryption/decryption process.