Cloudmore Tivoli Storage Manager (CTSM)
Data Protection as a Service

1. Introduction

Cloudmore currently serves over 6000 customers across Europe with high scale, high availability cloud delivery IT solutions. Cloudmore's unique aggregation platform solves the challenges of organisations adopting multiple cloud solution by unifying the experience bringing control and predictability to the users and organisations. IBM Tivoli Storage Manager (TSM) is now available through Cloudmore and is provided as a service which means you can quickly benefit of TSM without the need for any capital investment, server or product experience.

2. The future of server backup

As IT solutions become more complex with different delivery methods, for instance public, private and hybrid cloud, what we used to refer as simply backup is now becoming known as Data Protection, Data Protection combines the all the elements of backup, snapshots, replication, archival and also include availability, business continuity and disaster recovery. Clearly the days of localised tape backup are numbered as organisations seek to meet the challenges of Data Protection in a changing and complex world of data management.

3. Tivoli Storage Manager - Data Protection as a Service

IBM Tivoli Storage Manager (TSM) is a centralised, policy-based, enterprise class, data backup and recovery solution. The software enables the user to insert objects not only via backup, but also through space management and archive tools. It also allows retrieval of the same data via similar restore, recall, and retrieve methods.

The TSM Platform as a Service provides a comprehensive solution with a focus on the key Data Protection elements of backup, archive, recovery, and disaster recovery planning.

The TSM platform, when combined with Cloudmore's automation tools provides simplified and automated Data Protection, including backup, archival and disaster recovery. Cloudmore Tivoli Storage Manager based Data Protection Service (CTSM) is extremely cost effectively, highly scalable, and very simple to deploy and manage.

4. Key Benefits of CTSM

a. Use the Cloudmore aggregation platform to manage one or many services for your organisation.

b. Reduce capital expenditure. CTSM requires zero investment in server side hardware, Save money — improve service levels and comply with data retention regulations.

c. Reduce operational expenditure - CTSM is a "set-and-forget" service with reports and alerts automatically generated, time to manage backups is substantially reduced.

d. Meet disaster recovery requirements - As your data is kept in more than one geographically separated location away from your organisation you immediately meet disaster recovery and business continuity requirements.

e. Configure one solution and surrounding processes that meets your Data Protection needs, including local backups for frequently used data, configurable backup or archive policies and optional features such as replication and bare metal machine restore.

f. Pay-as-you-go commercial model with monthly service charges, based on the storage consumption or the minimum monthly commitment.

5. Data Protection

CTSM protects data from hardware failures, errors, and unforeseen disasters by storing backup and archive copies on off-site storage managed by Cloudmore.

The CTSM platform as a Service allows you to schedule automatic routines on a per server basis, processing only incremental changes after the first backup. The file compression and de-duplicate features significantly reduce the impact on bandwidth.

The CTSM is very flexible and can protect most platforms including Windows, Linux, Solaris, HP-UX and AIX. Protected servers usually connect to the platform securely over the internet, but the service can be configured to connect to our Data Centres using other methods if required.

Basic protection requires no more than an automated installation of a storage agent on the target server, Storage agents are also available for almost any version of popular software configurations, for example, Databases: SQL and Oracle. Email, Exchange and Lotus Domino, and SharePoint. CTSM cannot back up SANs, a local installation of IBM TSM is required for this. CTSM allows business-critical applications that must run 24x7 to be protected with no interruption to their service or availability.

6. Clients

Cloudmore CTSM include local service clients for file and folder backup, SQL backup and Microsoft Exchange backup. Other types of systems files and databases can be backed up but may required additional, chargeable client customisation. Cloudmore only supports the standard Client builds. Full details of the software requirements for the CTSM Clients are available from the Cloudmore support centre.

7. Restores

As part of a highly configurable Data Protection solution, restores are managed using the local client. It is usual that only small amounts of data would need to be restored, but if the requirement is meet a much shorter recovery time than a local NAS device (see Local Storage Option)

As the administrator defines the retention policy including the number of versions you want to keep for existing and deleted data and the length of time you want to retain the inactive backups and last backup versions, full flexibility is available balancing the Data Protection Service requirement against the amount of storage used.

8. Local (NAS) Storage Option (Additional Charge)

By adding a local, Networked Attached Storage, (NAS) to CTSM you will achieve the best of both worlds, with near real-time fast restores and the security off your data being protected offsite in a secure and safe location. The service includes:

- Complete control of your local data requirements on a location by location basis
- Delivery of a faster OLA to the organisation for Data Protection
- Utilise the most cost effective hardware solution, irrespective of vendor
- Recoveries to a physical or virtual machine.

9. Data Integrity, Backup and Restore

9.1 Data Integrity

To ensure strongest possible encryption, CTSM uses 128-bit Advanced Encryption Standard (AES) data encryption as standard. Data to be protected is encrypted before it is transmitted and remains encrypted at rest and can only be decrypted by using the specific key created by the server agent. At no time does anyone have access to unencrypted stored data in the Cloudmore data centres.

9.2 Backup

CTSM is a remote and automated backup service with easy data restores over the Internet. The backup job runs at least daily incremental backups, optimising bandwidth and server resources during the backup window. All backup data is always accessible through the server agent through a restore. Most Databases and Exchange email systems are able to be backed up whilst in use.

9.3 Archive

Data archiving is intended to preserve a copy of a related set of files as they stood at a point in time for legal or compliance purposes. An archive is not the same as Backup, which typically involves copying an unrelated set of changed files to tape and to retain them for a relatively short time. Also, a backup does not affect the source data, whereas an archive can delete the source data. Archive is about retaining data at a point in time

CTSM Archive service enables data to be protected for legal or historical purposes. With Archive, you choose the retention time on each set of data and can complete a full incremental backup of potentially very large data volumes.

10. Bare Metal Recovery (CTSM BMR) (Additional Charge)

CTSM Bare metal Recovery provides the functionality to automatically or semi automatically recover an entire machine including the operating system, configuration and applications. Servers can be recovered, depending on Bandwidth, very quickly and multiple servers can be restored simultaneously, and restores can be from any point in time that is available. This solution can also be used to create clones for testing and migration purposes. Advantages of CTSM BMR are:

- No additional backup is required, as the recovery is from normal backups
- Recoveries can usually be completed as little as 10 minutes
- Multiple machines may be recovered simultaneously
- Recoveries can be to the original or to dissimilar hardware or to a virtual machine
- The recovery process can be fully automated
- Recovery Simulator add-on
- The recovered machine is an identical copy of the original (which is not the case when software is re-installed)

11. Active Directory

During normal day-to-day operations, you can use the Active Directory individual object recovery and item-level restore to recover from accidental corruption or deletion of Active Directory objects. You can chose to restore one or more individual Active Directory objects. This feature does not require you to shut down or restart the Active Directory server.

12. Datacentre

The datacentre is ISO 27001 certified for information security management systems. The datacentre is manned 24x7 with on-site security personnel, regularly patrolling the datacentre parameter and managing the video surveillance internally. The generators located in the Interxion, Stockholm site, are built using an n+1 redundancy principle. This redundancy principle stipulates that for every generator needed to power the datacentre, in case of a grid outage, there is an extra generator available.

13. Storage

You can create your own service policies for different applications. for instance; files will have one policy and SQL and Exchange have different policies

14. System Requirements

CTSM supports data backup on most systems. The service requires a minimum of Microsoft Windows Server 2008 (64 bit only for 2008) and does not support Linux x86. All other systems are supported.

15. Localization

CTSM is delivered in English; however, other languages are available upon request.

16. Data Ownership

All data created or stored by the users within CTSM are the users' property. Cloudmore shall allow access to such data to authorised personnel only. Upon CTSM termination, Cloudmore will not retain any data including, but not limited to, user data, Active Directory, log files and backup copies.

17. Access

CTSM is provisioned and managed through the Cloudmore Control Panel configuration of policies is done through the control panel and the server agent. Once the Node name and password have been entered you will be logged on the system.

18. Cloudmore Control Panel

The Cloudmore Control Panel is an intuitive system to use, you can:

- Purchase and provision CTSM using a unique wizard system.
- Manage multiple customers within one place.
- White label and delegate Cloud Service control to your customers or manage on their behalf.
- Add, amend or remove Service Plans and Service add-ons to customer subscription(s).
- Manage users subscriptions and storage.
- Access to backup status reports and storage usage.

19. Cloudmore Support

This service is technically supported 24x7, with phone and email support from the Cloudmore Support Centre for all incident severities.

- Severity 1 incidents, as defined by the Service Level Agreement, will be processed 24x7.
- Severity 2, 3 and 4 incidents will be processed during core hours of business.

20. SLA

CTSM has a Service Level Target of 99.9% Service Availability for the service.

Cloudmore shall use reasonable care and skill when providing services, but does not guarantee that the services shall be continually available to the customer. There may be occasions when services are disrupted through an error or act of the customer or another third party, or circumstances outside the reasonable control of Cloudmore (“Service Disruption”). In the event of unavailability of services to the customer, other than in the case of Service Disruption, Cloudmore shall reimburse the partner or customer (“Service Credit”) as stated in the CTSM Service Level Agreement.

In addition to the SLA, the CTSM is designed with availability in mind:

- The protected data is synchronised between two different storage systems through node replication. Node replication is the process of incrementally copying, or replicating, data that belongs to backup-archive client nodes. Data is replicated between CTSM servers. If a disaster occurs and the source replication server is temporarily unavailable, server nodes can recover their data from the target replication server. Synchronisation between the servers occurs on daily basis. (RPO).
- If the for any reason the primary backup window is not able to be accessed or there is a problem with the protected server then the system will automatically resume their backup service during the next primary backup window after service disruption. This means that there may be a longer period between backups/archive jobs. (RTO)

The following conditions apply to service continuity management:

- The Primary backup window is 6pm – 9pm CET every night.
- Client access after recovery from a service disruption typically does not require reconfiguration.

The RPO and RTO and SLA shall not apply where the unavailability of the service is due to:

- Network unavailability: Service unavailability resulting from network unavailability will not be included in the Service Availability calculation. Network unavailability is defined as problems on the end users' portion of the network and DNS issues outside the direct control of Cloudmore.
- Acts and Omissions:
  Acts or omissions including, without limitation, any negligence, wilful misconduct, or use of the Service in breach of Cloudmore's Acceptable Use Policy, AUP, and terms and conditions regarding the use of the software.