Queen Mary
University of London

TSM Backup and Restore Strategy and Overview (Draft)

Prepared by: Trevor Leigh

Version: 1.1

Document Owner:	
Name/Position	Steve Wicks, Servers & Storage Manager

Revision History			
Version	Description	Author	Date
0.1	First Draft	Jafar Albadran	21/10/2014
0.2	Added further information on strategy	Shelim Miah	27/10/2014
0.3	Comments from Steve wicks	Shelim Miah	03/11/2014
0.4	Reviewed and Edited	Jafar Albadran	03/12/2014
1.0	Rewrite as TSM Backup & Restore Strategy	Trevor Leigh	2/10/2015
1.1	Edits after initial review	Trevor Leigh	5/10/15

Note for versions 1.x

Please note that this document is not in the normal Service Design Document format. This is because it is a small revision to an existing in-production service document. Essentially there are mainly factual clarifications and general errata.

This document has been prepared so it can be tracked by our governance process which pre-dates the original versions.

Contents

Introduction

IT Services has undergone a huge transformation programme to help QMUL improve its IT infrastructure. One of the core deliverables of this programme is the QMUL Datacentres that will host all QMUL applications, servers and data.

All the data in the Datacentres are backed up using IBM Tivoli Storage Manager (TSM).

Purpose and Objective

This document is intended to describe the backup and recovery arrangements and associated service levels or targets for the information and content stored on the centrally managed QMUL infrastructure and systems. It hopes to provide clarification and guidance to all those who are involved with or affected by backups and restores.

Scope

This document is not intended to be a complete business continuity or disaster recovery plan. It is only intended to support the requirement for normal regular operational backups of files and for the restoration or recovery of files from regularly scheduled backups. Exceptions to normal operations which may from time to time occur need not be documented.

This document will cover backup and recovery of data held within the Data Centre 1 (Mile End) and Data Centre 2 (Enfield), for operational purposes in supporting the business needs and requests of IT Services customers. TSM will act as recovery for system failures and human error. Critical data from each DC is copied to the opposite DC for additional data security.

TSM Backup System

Hardware Overview

Describes the hardware used for backups and provides information about the backup server and its configuration:

The TSM Server at each datacentre is built on an IBM x3850 server with 4 x 8 core CPUs and 256GB RAM. These systems have an IBM DS3500 external disk storage array attached via SAS to provide additional storage capacity for the TSM disk storage pool. Internally each server has the following cards installed:-

- 3 x 8GB Dual Port FC HBA (for SAN connection to the IBM TS3500 Tape Library)
- 2 x 6GB SAS HBA (for connection to the IBM DS3500 external disk storage array)
- 1 x Dual Port FCoE Virtual Fabric Adapter (for LAN connection)

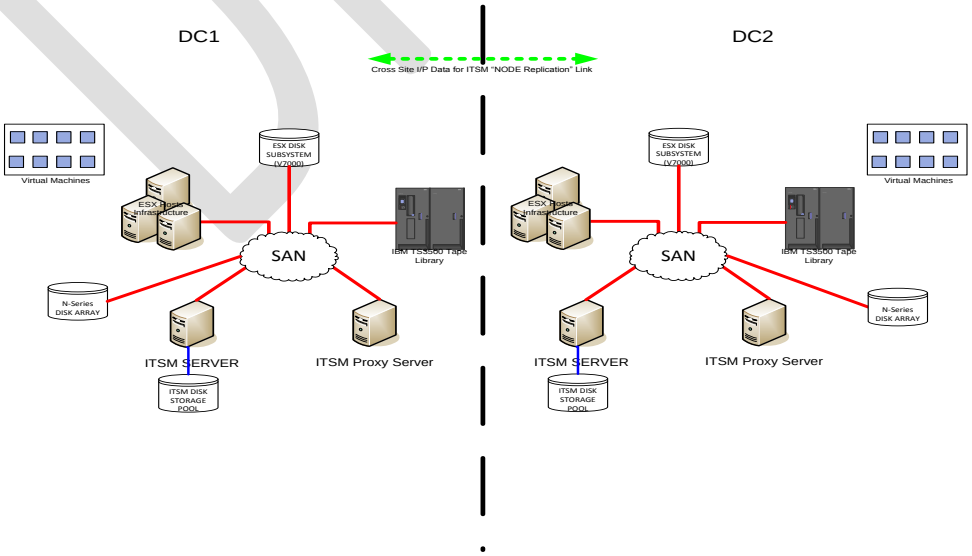
The IBM x3850 server has two FCoE ports built into the motherboard that will also be used for connection to the LAN for ITSM server functionality.

The TSM Proxy Server at each datacentre is built on an IBM x3650 server each with 2 x 4 core CPUs and 192GB RAM. Internally each server has the following cards installed:-

- 2 x 8GB Dual Port FC HBA (for SAN connection to the IBM TS3500 Tape Library)
- 1 x Dual Port FCoE Virtual Fabric Adapter (for connection to the SAN for IBM Disk Storage)

The IBM x3650 servers have two FCoE ports built into the motherboard that are also used for connection to the LAN.

The below diagram provides a high level overview of the current backup platform.



Software Overview

Describes the software application used to perform backups:

IBM Tivoli Storage Manager (TSM) is a centralized, policy-based, enterprise class, data backup and recovery package.

The table below details backup hardware used, the backup application, and details of backup accounts in place specifically for the administration of backups and restores:

Hardware Used (Type/Model/Manufacture)	**Software Used** (Vendor/Application Name/Version)	**Backup Account Details** (Account Name used to administer backups)
IBM, x3850 Server (x2)	IBM TSM 6.3.4.0	Individual administrator accounts
IBM, x3650 Server (x2)	IBMTSM4VE 6.4.0.2	
IBM, DS3500 Disk Storage Unit (x2)		
IBM, TS3500 Tape Library (x2)		
IBM, LTO5 Tape Drive (x20)		

Backup Strategy

TSM Backup Strategy Overview

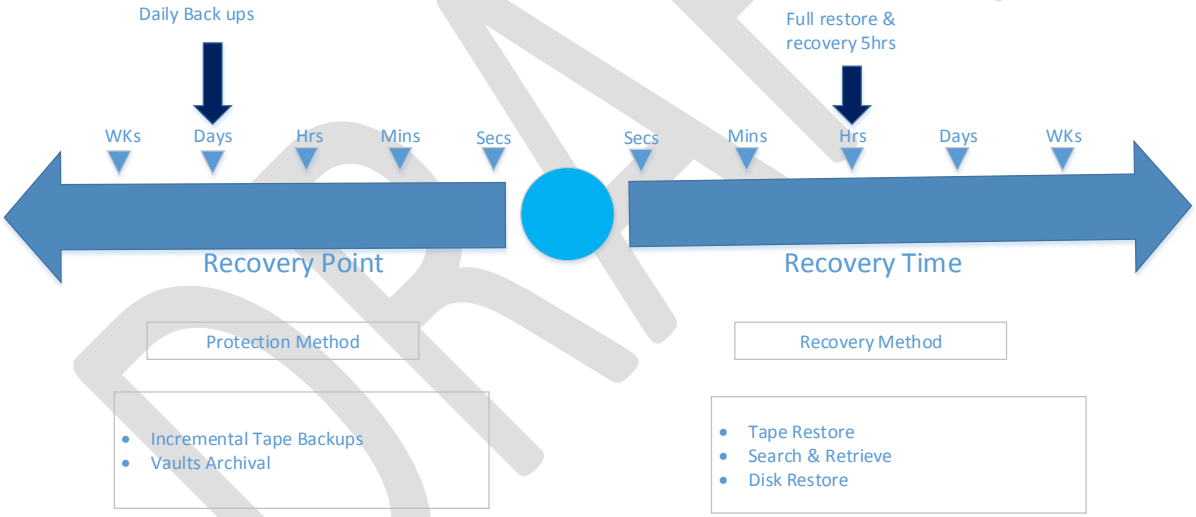
Provides an overview of the strategy in place for carrying out backups:

A backup is simply a copy of electronic data which is used as a means of recovery should the data become lost, corrupted, or compromised. This is the idea that has been kept in mind to ensure a suitable solution is in place to cater for the needs of QMUL.

This strategy looks at the data source, the back-up method for copying the data across and the frequency of back-ups.

The strategic backup and recovery solution chosen by QMUL is IBM Tivoli Storage Manager (TSM). TSM employs an "incremental forever" policy for file backups where an initial full backup is taken and that is followed by an incremental backup of changed files only. The backups are performed daily from 18:00. The data is stored locally on LTO5 tapes and a second copy is created in the opposite datacentre, also stored on LTO5 tapes. The data copies are synchronised on a daily basis.

Datacentre Virtual Machines and some Physical Servers are backed up by TSM.



TSM Backup Principals at QMUL

The key principles to the approach at QMUL are:

Automatic block-level backup of Virtual Machines in the DC1 and DC2 datacentres: TSM is configured to carry out automatic backup of any VM hosted in either of the two QMUL Datacentres. Any server not within DC1 or DC2 will not be backed up by TSM unless a TSM BA Client is installed and configured (file-level backup).

File-level backups are carried out by request. Some VMs are also configured for file-level backups for operational reasons. Physical servers can only be backed up file-level.

Full data duplication from the datacentres to TSM, updated on a daily basis

Backups are scheduled out of business hours from 18:00 as it is the usual backup window when the production systems are at their lowest activity.

There is no additional backup or increased frequency for critical applications or data. These should be handled by other means by the application designers.

At QMUL all backups are via central schedules configured at the TSM server at each site.

TSM employs an "incremental forever" policy for file backups where an initial full backup is taken and that is followed by an incremental backup of changed files only.

At DC1 VMs are backed up incrementally every night. At DC2 the VMs are backed up incrementally for the first four days of the week followed by a FULL back up on Friday. TSM is understood to work perfectly correctly running in this incrementally forever mode in DC1. The decision to move to incrementally forever in DC1 was tactical.

File-level backups are incremental forever.

Scope of TSM Backups

Describes what is backed up and how:

TSM servers and TSM proxies are located at DC1 (Mile End) and at DC2 (Enfield) and are configured for the following main types of backups:

VM backups (block-level):

For Virtual Machines, the backup utilises the TSM4VE client which is installed on a TSM proxy server. The VM backup is at block-level and is done by taking a snapshot of the VM and data is sent to the TSM server using LAN-free technology where data is moved directly from the disks where the VMs are located to tapes without using the LAN. The backups are scheduled and initiated from the TSM server. New VMs are backed up at block-level automatically by TSM4VE and do not need a TSM client installed.

Physical servers:

Physical servers are backed up file-level via a TSM Backup Archive client installed onto the host. The backups are scheduled and initiated from the TSM server.

Database servers:

SQL or Oracle databases are backed up locally by their DBAs, using their own internal tools, to export files located on an agreed drive and these local backup files are then picked up by the TSM backups. Most database servers (VMs) are backed up file-level in the same way as physical servers.

Linux VMs:

Linux VMs also utilise a BA Client for file-level backups.

N-Series (NetApp) filers:

For N-Series filers, the CIFS file systems are mapped onto the TSM server and backed up as a local drive. The TSM schedule executes a script which calls snapdiff, leveraging NetApp snapshot technology to increase backup performance.

DFS file shares:

Backed up file-level via BA Clients installed on the cluster nodes but configured to address individual file server 'roles'

GPFS:

Uses the IBM mmbackup utility which generates and uses a shadow database to track changed files quickly

TSM Backup Procedure Overview

Describes the initiation of a new TSM backup:

The following is a brief description of how backups are undertaken with TSM at QMUL:

1. A User requests a server to be created via LANDesk.
2. This is created in the appropriate datacentre by the Servers & Storage Team.
3. Block-level backups of VMs are made automatically unless excluded by an administrator.
4. If a file-level back up is needed a request must be made to Servers & Storage via LANDesk, specifying which areas of the server need to be backed up at file-level.
5. File-level backups are set up by installing a TSM client onto the host which performs the required checks and sends data to TSM.
6. Backup operations are scheduled on the hosts by local scheduler services that contact the TSM server to determine the next time for backup.
7. The time of backup is set on the TSM server. The TSM client initiates a backup at the agreed time.
8. A member of the Servers & Storage team checks for unsuccessful backups the following morning.
9. If successful no further action is required. Recurring backup failures are investigated as incidents.

TSM Backup Scheduling

Describes the principles of the approach used to schedule backups.

Backups take place out of main business hours from 18:00. VM block-level backups commence at 18:00 and file-level backups are staggered throughout the night.

At DC1 VMs are backed up incrementally every night. At DC2 the VMs are backed up incrementally for the first four days of the week followed by a FULL back up on Friday.

File-level backups are incremental forever.

Backup Retention

Describes how long backup data is retained:

TSM backups do not follow the classic model of tape retention. Instead, TSM uses storage pools where data is stored on multiple tapes. When data is expired on certain tapes and these tapes become less utilised, TSM consolidates the remaining amount of data onto other tapes and returns

the empty tapes into the scratch pool for future use. There are no monthly, quarterly and yearly backup sets done using TSM.

The retention period set for TSM is 90 days, for any files that have been modified.

There is no long term data archiving solution available as part of our backup solution. Applications that require this must design this in at the application layer.

TSM Backup storage and security

Backup Storage

Locations

The location of the backup media is as per the security point below.

All backup data that is for disaster recovery purposes is stored offsite, whilst daily back-ups for human error or corrupt data are stored locally at each datacentre.

Tape rotation

TSM does not follow the classic model of media rotation; instead it moves data between tapes when they become less used and returns the empty tapes into circulation.

At QMUL, large tape libraries are deployed which have the media capacity to store our entire backup data requirements. Tapes are not routinely removed from these libraries or moved between sites, unlike in some other backup solutions. Data is copied between sites to provide an off-site copy.

Security

How access is gained to the locations where backup media is stored:

The backup data is contained on tapes that reside within the automated tape libraries (ATLs). These libraries are physically located in secure locations that are controlled using the usual methods of card, key and combination access. The DC1 tape library is located outside of the DC1 datacentre in the Mile End library building and access to the room is secured via card, key and combination. The DC2 library is located within a secure third-party data centre in Enfield and access to its location is controlled by the usual security procedures applied by the third-party data centre management.

Vendor Services

QMUL does not employ any third part storage services for storing their backup media. Instead, backups are copied online to the opposite site and tapes are stored in tape libraries on these sites.

QMUL does have support contracts with IBM, covering both software and hardware.

QMUL also leverages the expertise of a contracted third-party TSM expert (i-Stor Ltd) via a contractual arrangement.

Data Quality

Backup Checks

The success and failure of backups are manually checked every morning by Servers and Storage staff via logs on the TSM servers and by utilising the Tivoli Integrated Portal (TIP) reporting tool. There is limited reporting functionality on VM backups only.

Backup Failure Response

Failed backups are identified by the backup team using regular morning checks. These failures are then investigated as incidents and corrected as necessary.

A brief summary of backup status is then emailed to the other Servers and Storage team members.

The TSM administrator investigates major backup failures and persistent backup failures. Incidents may be followed up under our IBM support contracts if necessary.

Backup Media testing

There is no direct media testing as such, but TSM marks media that are experiencing any read and write errors and prevents them from being used. Data that exists on these tapes will then be moved to another tape using TSM commands.

Restoration testing

There are no planned schedules for testing. Operational restore testing occurs regularly as a normal element of BAU.

Backup Records

All backup records are kept within the TSM database. These records are accessed via TSM commands and through external tools such as TSMManager. The TSM database is backed up daily to ensure availability in case of a TSM server failure.

Data Recovery

Restore requests

User requested restores:

Restores are requested via a LANDesk ticket to Servers and Storage.

Restore SLAs

A Restore Time Objective (RTO) of 5 days and a Restore Point Objective (RPO) of 24 hours is applied. TSM is used to recover services which require manual intervention from the technical teams, service availability hours are therefore aligned with the standard support hours of the teams.

Restores - Documented Procedures

The operational procedures are kept here:

J(IT Services):\Infrastructure\Servers and Storage\Backup Systems\TSM\TSM Restores

Restoration Records

Restores are tracked by TSM and kept in the TSM database, as are the backup records.