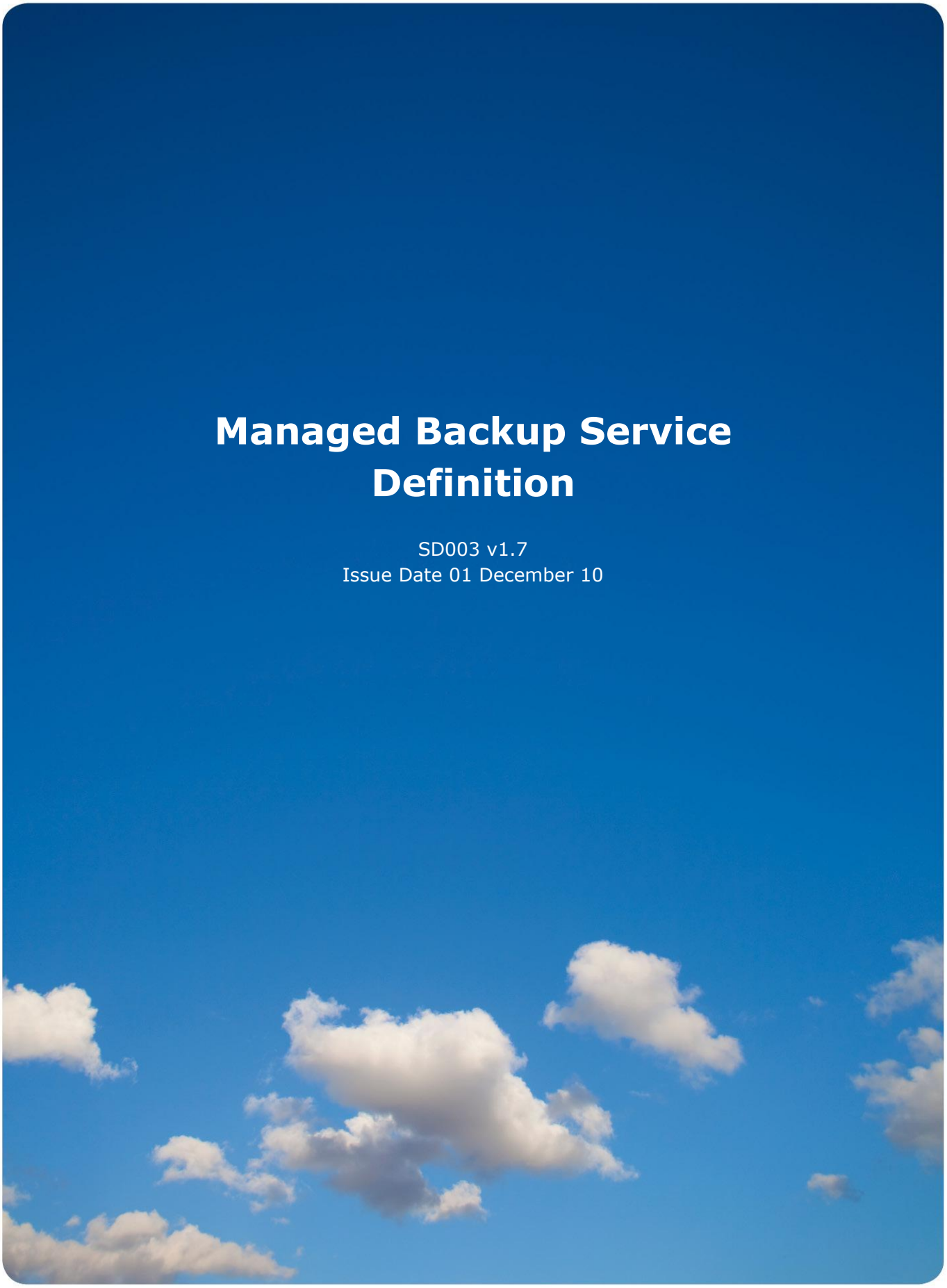
inTechnology

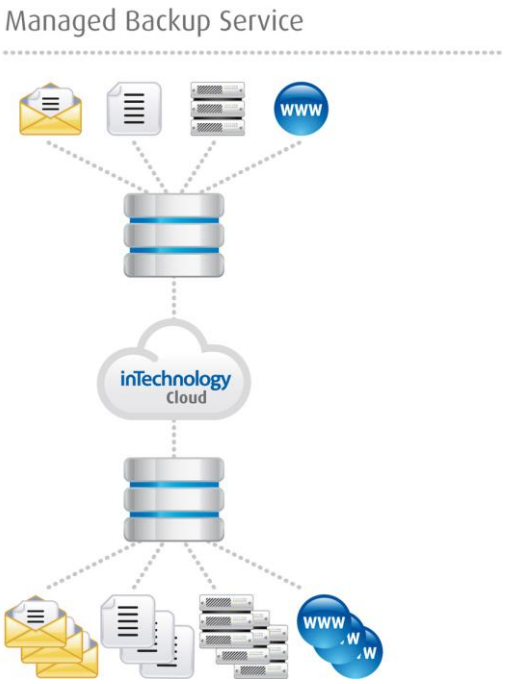
Managed Backup Service Definition

SD003 v1.7
Issue Date 01 December 10



Service Overview

- The Managed Backup Service (MBS) provides automated and remote backup & recovery for data stored on:
    - Windows file and print servers and Windows desktops / laptops
    - NetWare servers
    - UNIX, AIX and HP-UX servers
    - Linux servers
    - Microsoft Exchange servers
    - Microsoft SQL servers
    - Microsoft SharePoint servers
    - VMware servers
    - Oracle servers (both UNIX and Windows)



- Data is securely backed up and transferred offsite using MBS Agents installed on all target servers.
- Backup data is transferred offsite to one of InTechnology's secure data centres, guaranteeing availability and security.
- The Customer is enabled to encrypt all data prior to transmission offsite.
- Encrypted data is held offsite on enterprise class N+1 disk storage.
- The Service provides an easy to use interface that simplifies the backup and recovery process and provides detailed information about scheduled operations.
- Centralised control of the backup agents enables a network administrator/IT manager to specify exactly what data is to be backed up, ensuring investment is not wasted by backing up unauthorised or unnecessary information.

- A user definable number of backup versions of files are retained on disk, for immediate online restore.

- The backup vault and any networking equipment supplied is monitored 24x365 by the Customer Support Team.

- MBS backup activity logs are captured daily by the Service and are displayed in the InTechnology services portal.

- Backup data can easily be selected and restored online without the need to locate and identify backup tapes.

- Customers can perform regular online restores, allowing them to test the integrity of their data at any time.

- InTechnology's Customer Support Team is on 24x365 standby to support major data recovery by making requested backup data available to the Customer.

- InTechnology will only charge for the compressed data stored within the secure data centre and not the transferred data volumes or restorable data.

Managed Backup Service – Service Definition

The Managed Backup Service (MBS) is a unique alternative to traditional backup and restore methods, replacing conventional tape based systems with a fully automated online solution. It provides centralised and automated backups of PC's, file servers and application/database servers with secure offsite storage and immediate online restoration.

More than ever, organisations of all sizes must strategically leverage their brand as well as manage costs to foster growth and innovation. A company's information, whether it be intellectual property or in the form of historical records and files, are their competitive assets. Access, or conversely, a lack of access to that information, can render its network- and PC-tethered workforce completely ineffective.

Those employees responsible for managing information access and protecting its integrity, from the server room to the board room, face increasing pressure focused around the following issues:

- Heightened awareness of business continuity and risk assessment
- Exploding data growth and the ability to manage it
- Dispersed environment fuelled by an increase in mergers and acquisitions
- Constant OS and application changes
- Increased regulatory requirements

Enterprise-level companies, with tens of terabytes under management, combat these issues with a team of experienced, well-compensated IT professionals armed with comparatively larger budgets than small- and mid-sized organisations. Small and medium businesses also deal with the same competitive pressures, but must alleviate them despite having small or no dedicated IT staff and tight budgets.

Because of these factors, mid-sized companies requiring data protection and rapid recovery want simplified management through one vendor, cost-effectiveness, more operational control, reliability and secure and fast recovery. Where mid-tier organisations dramatically differ and where MBS has a technology advantage is by helping them overcome their smaller budgets and IT staff.

MBS is a data protection and recovery service that enables a server or a group of heterogeneous servers to backup their data to a remote storage device over common telecommunication connections. The MBS Service allows for online restores of backup data transmitted over the same or alternate telecommunication connections, as well as facilitating the migration of data to lower-cost media for long-term storage.

InTechnology Supported Platforms

The Managed Backup Service supports the following operating systems. InTechnology will make all endeavours to support future versions of the operating systems below:

Operating Systems
Windows
Solaris
Linux
Novell NetWare

Customer Supported Platforms

The following operating systems and databases are not supported by InTechnology, but are can be backed by the customer.

Operating Systems
IBM AIX
HP-UX
Linux
Macintosh

InTechnology Supported Applications and Database Servers

The Managed Backup Service supports the following applications:

Application
MS Exchange
MS SQL Server
Oracle
VMware

The application agents for the supported applications and database servers are installed as part of the service implementation. InTechnology consultants perform installation and configuration of the application agents, in conjunction with the appropriate customer database or application administrator.

The supported application agents only backup the appropriate application data. In addition to the application agent the appropriate file system backup client must also be installed and configured to backup the remaining file system data on the customer server. There is no online archiving support for applications. Application data to be archived must be extracted using techniques such as database dumps and then archived.

How the Managed Backup Service Works

MBS relies on three components: the Director, Agent and Remote Agent Console:

- The Director program, which is managed by InTechnology, controls a Vault for data storage. It maintains the integrity of the Vault and control access to the Vault.

- The Director is used to set up access to the Vault for the Customer/organisation and, from within that organisation's name, assign specific locations, accounts and users for the Customer.

- Each computer and server to be protected will have the MBS Agent software installed on it for communications with the Customer's Remote Agent Console computer and the Director.

- Once this is done, an organisation can use the MBS Remote Agent Console program to configure and schedule backup tasks on all of their protected systems.

- The MBS Agent software on each individual computer or server will respond to its backup task (configured by MBS Agent Console) and send that system's data directly to the remote MBS Director for secure storage.

- Should a restore be required, the user or administrator using MBS Remote Agent Console, can quickly access the online data and restore a file or an entire system.

All data passed via backup or restores through the Managed Backup Service is placed in the System Independent Data Format (SIDF), which enables a single copy of the Director to manage data protection and migration across multiple operating systems. SIDF provides an independent format for representing data from many different operating systems. As such, it provides better longevity characteristics and portability than the native OS formats.

MBS Agent Console / Remote Agent Console

The Agent Console is a program residing on a Windows workstation, which configures and then manages local and/or remote backup Agents. With the Remote Agent Console, users can manage hundreds of backups from computers across local and wide area networks from a single system. The Remote Agent Console empowers the user to define the how, what, when and where for their backups.

The Remote Agent Console uses remote procedure calls (RPCs) to communicate control and status information with the backup Agents. More than one (Remote) Agent Console may exist on a network and control multiple Agents.

The Remote Agent Console has a Windows Explorer design structure. The Agents that have been defined show up in the left panel. Double-clicking on an Agent will bring up an index in the right panel of backup tasks and other control entities that may be modified or viewed remotely.

When configuring agents the Customer has the option to use the Remote Agent Console instead of the Agent Console. The Remote Agent Console uses remote procedure calls (RPCs) to communicate control and status information with Agents.

The Remote Agent Console allows Customers to have:

- Dashboard overview of all agents

- List of agents with errors and failed backups

- Ability to customise agent views

- Hierarchy of roles: admin user / execute only / view only

Agent

The backup agent is a lightweight application running on the host system. It executes backups on that system based on a set of parameters related to each backup task and monitors a defined schedule using a graphical scheduling system. Alternatively it can be scheduled from an external scheduler for example Windows scheduler or Unix cron. When a backup task is due for execution, the MBS Agent reads the backup tasks parameters and executes the backup accordingly.

The Agent takes different forms depending on the host operating system. On a Novell system, the Agent is a Netware Loadable Module (NLM); on a Windows NT Server or Workstation, the Agent is a system service. The Agent interfaces with the system console of the host system as well as with a remote Agent Console to pass status and control information regarding backups.

The Agent performs a remote backup by making a connection with the MBS Director running on a remote Vault connected via a Wide Area Network (WAN) or Virtual Private Network (VPN). Transmission Control Protocol/Internet Protocol (TCP/IP) is the base protocol used to make the connection. A proprietary protocol called Backup/Restore Transfer Protocol (BRTP) utilises RPCs to pass control information and the actual data back and forth with the MBS Director.

The parameters that define a backup are referred to as a task. One or more backup tasks may be created to implement the backup necessary to protect a single system. Each time a backup is executed a log file is created and a catalogue is created. The log file is an audit trail for the backup and displays the start time, connection information, statistics and summary information regarding the backup. The catalogue is an index for all the files that are contained in the backup. The catalogue contains file attribute information, dates, full directory information, and sizes. The catalogue information is used to search for files, summarise statistics regarding a series of backups via the *analyse* function, as well as browse, and initiate restores. At the remote server, a safeset that actually contains all the data represents each backup.

The Agent executes restores in a similar manner to backups. A restore definition file is created containing the parameters necessary to complete a restore of all or a subset of files in a specific backup. The Agent makes a connection to the Director. The Director locates the safeset (based on the catalogue), finds the requested file(s), and the Agent receives the file data from the server.

Director

The Director application, managed by InTechnology provides backup and restore functionality to any number of remote Agents. In addition to online transaction processing with clients, the Director's key function is to manage the storage and migration of backup data. Based on the parameters defined by the Agent (via the Remote Agent Console) each backup has a life span and may be migrated from online storage to archive or deleted depending on policy.

The Director resides on a LAN with one or several network connections. The network interfaces will support the variety of communication types requested by the clients connecting to the Director. There could be a mix of:

- Frame Relay routers - supporting links to Frame Relay clouds
- High-speed routers - to support fast (DSL on up) Internet connections or directly to client networks

Each Director site has a web page accessible on a HTTP server for downloading the latest version of the Agents and to support automatic registration of demonstration accounts.

Managed Backup Service Setup

Depending on the service options chose, these activities will either be performed by InTechnology or the Customer:

1. The first step is installing the Remote Agent Console and the Agents on all the servers and client machines that will be backed up. The MBS requires a minimum 100MB free space for Agents on installed hosts and an additional 1% of the raw data backup size for processing the changed data information.

2. Using the Remote Agent Console the Customer will next select the files and/or directories to be backed up.

3. The Customer then schedules the frequency of backups, encryption methodology, Vault passwords and type of backup for each machine. After the first full backup, subsequent backups will most likely be incremental, to reduce time and bandwidth for future backups.

4. After the Customer has completed step 3 all backups will then be performed automatically per the schedule set and sent offsite to the MBS Vault.

5. Restoring a single file from the MBS Vault is usually performed within a few minutes. There is simply no better solution to data protection available.

Using the Remote Agent Console, the MBS administrator software, a single LAN administrator can setup backups on behalf of other users. The managed system has to be running the Agent in the background, and the manager station running Remote Agent Console connects to the managed system to configure the backup tasks and schedules them remotely.

There are two major security features in the MBS. The first is an encrypted authorisation feature for every user that connects to the MBS Vault. This protects the data from unauthorised access. An additional option is to encrypt the data before transmission to the MBS Vault. This protects the data both during transmission over the network and while the data is stored on the remote storage server. Because MBS is based on TCP/IP, the underlying physical communication method is immaterial. Thus, a local LAN connection, leased line and ADSL are all valid methods for connection between an Agent and the MBS Vault.

Delta Processing

Within MBS, a combination of data compression and delta processing technologies reduce the amount of data required to reconstruct a file being transmitted from an Agent to the Director for backup purposes. In the case of compression, standard high compression techniques are utilised on a per-packet basis as the data is being transmitted to the server.

The MBS delta-processing algorithm is an industry-leading example of block-level delta processing. The block size can vary from 1K to 32K in size based on software settings. Block-level delta processing (for 1K blocks) determines changes on the 1024-byte sector level of a file. The blocks in the file are created by treating the file as a stream of 1 to N bytes. Changes are detected in the blocks by comparing the current block with the previous block in the same position as the image representation from the previous backup. Changed blocks are addressed, compressed, optionally encrypted, and transmitted in order from the first through to the last block in the file. MBS delta-processing is particularly beneficial for binary files, databases that are updated in a random manner, and file systems whose basic input-output units tend to be sector based.

Delta file re-creation support: the Agent has the ability to re-create a missing delta file, with additional information within the backup (on the Vault). This will not work on a corrupted delta file. In that case the file must be manually deleted prior to running the synchronize command. If the delta information was only partially recovered, some data may be reseeded during the backup. Additional information will show in the log file if a delta file has been re-created.

Data Format and Representation

One of the primary goals of the Managed Backup Service is its ability to backup a variety of system architectures. To achieve this, the technology adheres to a standard method developed to store and represent data in a format that could be restored on another system with all security, alternate data streams, and file system attributes intact. MBS adopted the SIDF standard and serves as the primary method to store data from a variety of operating systems utilising a single Director. For more information on the SIDF standard, consult: http://www.cs.wisc.edu/~jgast/sidf/

The MBS delta-processing algorithm provides the equivalent of traditional full backups, despite the fact that only changed blocks are sent.

Target Backup Destination

Unlike a local disk or tape device the Managed Backup Service provides a remote MBS Vault application using the Agent to send the backup data to the MBS Vault typically over a wide area network connection.

Backup Source Types

There are multiple source types that can be selected for backup. The options are:

- **Local Drive** – data from any locally connected disk
- **UNC Backup** – data from Network Attach Storage (NAS) devices where there is no possibility of installing the Agent.
- **MS Exchange Server (Database**) – this allows you to back up the entire Exchange database for disaster recovery purposes
- **MS Exchange Server (Mailboxes and Public Folders)** – this allows you to backup any combination of mailboxes and folders
- **MS SharePoint Server** – this allows you to back up and restore of MS SharePoint Server Portal 2003 and MS Office SharePoint Server 2007
- **MS SQL Server (Database)** – this allows you to back up the entire SQL database for disaster recovery purposes
- **Oracle (Database)** – this allows you to back up the entire Oracle database for disaster recovery purposes

VMware Server – the VMware offering consists of the ESX Server Agent and the VMware Console Plug-In:

- **ESX Server Agent** provides file level protection of ESX Servers
- **VMware Console Plug-In** provides "hot" DR protection of the entire virtual machine including all guest systems and applications

Initial Backup

The MBS compression algorithm provides highly effective compression ratios that enable large data volumes to be backed up over relatively low speed lines such as ADSL lines. However, the initial backup needs to be a full backup that serves as a baseline from which to conduct incremental backups. To satisfy this situation, especially if bandwidth is limited, the Customer may send the first backup data to a USB or NAS device. This USB or NAS device may be loaded at the MBS Server and the data becomes the initial "seed" backup. Subsequent backups may be performed over the communication line.

Deferred Backup

If using a NAS device is not practical, an additional seeding option is a deferred backup. In these cases, the backup task can be set up to have a maximum elapsed time. If the backup window available is six hours for example, then setting the defer backup after six hours will cause the Agent to backup as much data as possible in the six-hour period of each backup. The variable length of time is based how often and how much the data changes and the effective compression ratio achieved by the data compression algorithm.

Retention Scheduling

The MBS Director always keeps the first generation of any backup on a RAID array. Second and subsequent online generations are maintained online or archived offline for long term storage. Archive generations are copied from online storage to offline storage based on Customer-specified parameters.

The server will always maintain at least one generation of a backup online regardless of the retention settings of the MBS Agent. The Customer must call the operator of the MBS server system to request purging of outdated or unused backup safesets.

Filters

It is important that the user has the option to include or exclude files in a backup task definition based on a number of different methods. The first and most obvious is to physically select files via the graphical interface. The second method, which complements the first method, is to narrow the files included in a backup task by specifying include or exclude filters. The filters allow you to exclude files based on a file specification mask, or only include files in certain directories, or exclude specific file types.

Encryption

There are five primary encryption algorithms with differing key strengths to choose from:

- 56 bit Blowfish
- 56 bit DES
- 112 bit Triple DES
- 128 bit AES
- 128 bit Blowfish
- 256 bit AES

As with any encryption method, a modest performance penalty is paid for all forms of encryption. It is also very important to note that the sole owner of the key is the client. If they lose the password for whatever reason, the entirety of their encrypted backup data is no longer readable.

Maintaining System Attributes

Operating systems and their associated filing systems maintain various attributes including, but not limited to, defining security access and alternate data streams. MBS storage management protocols accommodate these various attributes.

Restoration

File restoration may be done on an entire safeset level or on a file-by-file basis. The graphical user interface of the Remote Agent Console lets users select individual files or directories for restore. There is also a search utility that allows users to scan an entire catalogue using a file specification mask that may include wild cards. The catalogue is the index that allows users to browse the contents of an instance of a backup task (i.e. safeset).

In the situation where all of the data is lost, the Customer needs to re-install the Agent and Remote Agent Console. Once installed, the Customer can connect to the remote MBS Director that can recreate the local catalogues. Once the catalogues are recreated from the MBS Director, administrators can proceed to initiate restores. Restores can be performed online or the Customer can request that the backup safeset is placed on a USB or NAS device and physically sent to the Customer's location (or alternate location if recovering from a major disaster).

Communications Options

Since the Managed Backup Service operates using the BRTP protocol that resides on top of the TCP/IP protocol, MBS may utilise any network connection that supports TCP/IP. Thus, multiple users at a site may share a single communication line that is routed to the MBS Director site.

Open File Handling

There are a number of techniques available to handle open files depending on the applications involved and the operational constraints (i.e. uptime, maintenance window):

Databases (other than MS Exchange, MS SQL Server or Oracle, which are backed up using MBS Agent Plug-ins)

- Shut down application and then backup
- Readlock, checkpoint, backup, enable
- Backup online dump
- Application Program Interface (API) - MS Exchange, MS SQL Server and Oracle

General File Server

- Enable Backup Open Files option during task definition
- Open File Manager (OFM)

MS Exchange Plug-In – an add-on option that uses the standard Microsoft API (MAPI) to perform backups and restores while Exchange is running. There are two components to the plug-in:

- DR: Disaster Recovery – backs up and restores the entire Information store
- MAPI: Brick Level – backs up individual mailboxes and folders and can restore down to the individual email message while online

MS SQL Agent Plug-In – an add-on option that uses the standard Microsoft API (MAPI) to perform backups and restores while SQL Server is running.

Oracle Agent Plug-In – an add-on option that uses the standard RMAN interface to perform backups and restores while Oracle is running.

MS SharePoint Agent Plug-in – support for SharePoint Plug-In for backup and restores of MS SharePoint Server Portal 2003 and MS Office SharePoint Server 2007.

VMware Plug-in – the VMware plug-in provides centralised backup solution for VMware by protecting any VM hosted on an ESX server. This approach allows the Customer with a number of ESX servers to spread the resource consumption/backup load and to effectively reduce the backup window. In case of failure of an ESX host, the VMware plug-in makes it easy and fast to restore VMs between ESX servers within the same or to another VMware Infrastructure.

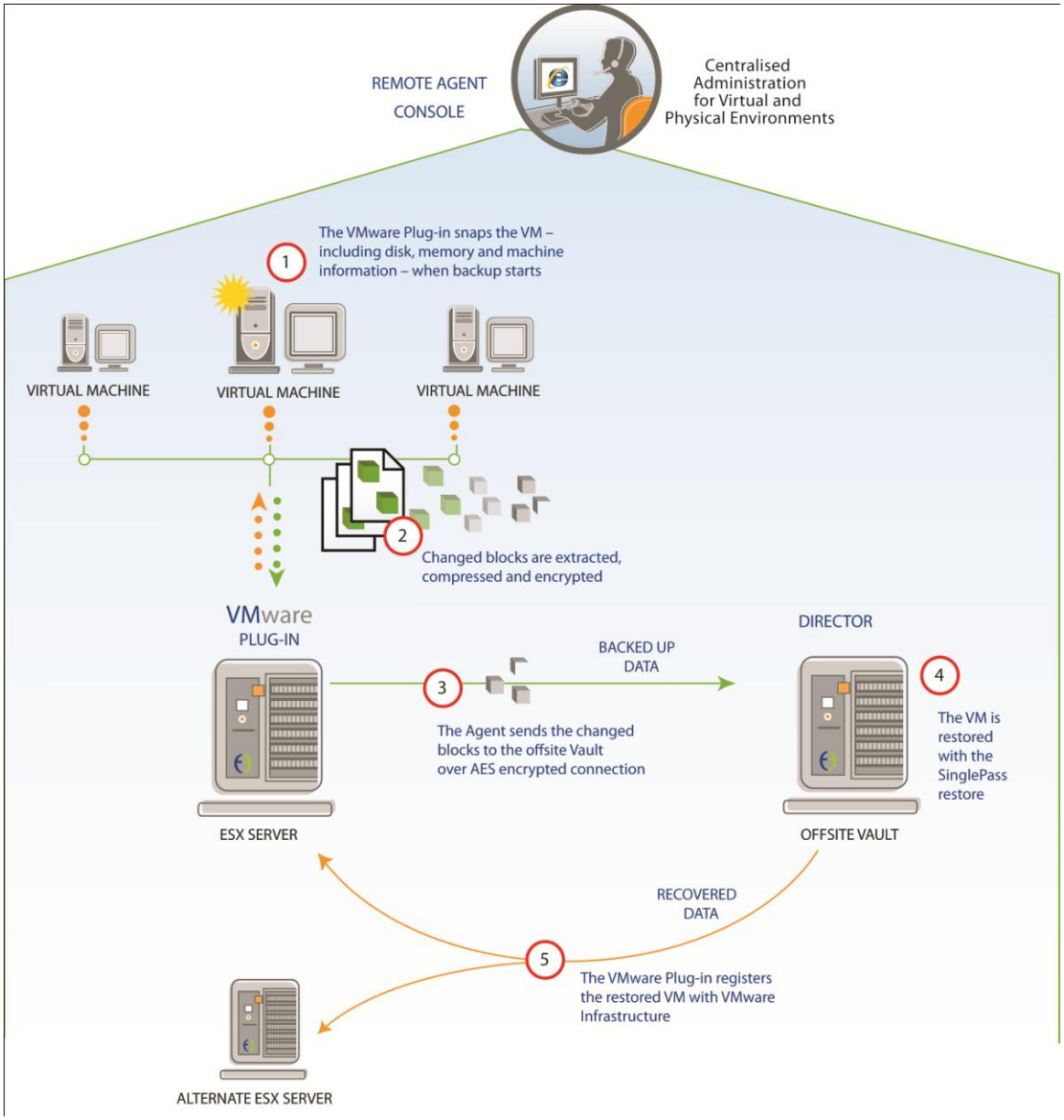
The VMware offering consists of the ESX server agent and the VMware console plug-in:

- **ESX Server Agent** provides file level protection of ESX servers
- **VMware Console Plug-In** provides "hot" DR protection of the entire virtual machine including all guest systems and applications

The ESX server agent and VMware console plug-in are both installed on each ESX server:

- The VMware Plug-in integrates with VMware's backup infrastructure and the MBS hot VM backups feature user controlled multi-level snapshotting. This capability significantly reduces the impact of a backup on production virtual machines, particularly for the most active systems.
- The VMware Plug-in supports backups from VMware vCenter with VMotion support. This allows backup of virtual machines spread across a VMware HA/DRS/VMotion enabled cluster.
- InTechnology's solution for VMware integrates into the MBS framework allowing users to centrally manage data protection of both virtual and physical environments across multiple sites.
- InTechnology's Remote Agent Console makes it possible to securely manage and monitor the solution from anywhere in the world simply using a web browser.
- InTechnology's VMware plug-in provides the fastest way to provide a bare-metal restore of virtual environments running any OS or application supported by VMware.
- With the *Single Pass* restore, the MBS VMware plug-in takes all recovery steps and minimizes the need for any scripts or manual adjustments. All the user needs to do is power the VM to resume operations.
- The VMware Plug-in integrates with VMware snap shots and Windows VSS, where installed with VMware tools ESX3.5 update 4 onwards, to provide application consistent backups and restore of VSS supported applications.
- The VMware Plug-in cannot be installed on VMware ESXi hosts. However virtual machines hosted on VMware ESXi hosts can be backed up providing the agent is installed on a VMware ESX host within the same VMware vCenter cluster.
- Raw Disk Mapping is not supported. Therefore Virtual Machines with RDM will register as an incomplete backup. RDMs can be backed up using a MBS agent installed within the guest environment at a file or application level.

The following diagram illustrates the integration and backup process for VMWare:



Miscellaneous Features

- Activity Logs: extensive logging is included with selectable levels of detail and automatic version management
- Backup Resumption: network backup reliability is enhanced with automatic task retry and resumption in the event of a connectivity failure
- Catalogue: index of a safeset
- Log: a file created with statistics for each backup and restore
- Notifications: email notification on task success,failure or error, which can all be sent to any number of addresses
- Online Reporting: complete Customer backup history is available via the MBS Portal
- Retentions: any number of user definable retention policies can be set to meet the most complex corporate requirements for online storage and long term, offline archival
- Safeset: a set of backup data in SIDF format
- Scheduler: a flexible general-purpose scheduler is included for complete, automated operation
- Task: parameters that makeup a backup

The Customer is responsible for storing their original encryption keys in a secure location. Loss of the keys will prevent recovery of the Customer's backup data. InTechnology has no knowledge of the Customer's encryption keys and cannot recover / reproduce these under any circumstance.

Managed Backup Service Day-to-Day Operations

All MBS operations are performed using the Remote Agent Console interface. Authority to perform MBS operations can be controlled by defining access to authorised users or groups of users, thus preventing backup and restoration of data by unauthorised personnel.

Backups

MBS backups are based on backup sets that define the scope of the backup operation to be performed. Backup sets are executed to perform the specified backup operation and can be executed manually or scheduled automatically.

Backup Sets

A backup set defines the files or databases that are to be backed up. They can include or exclude files or databases by directories, or by filtering the file type. This allows the Customer’s administrator to define backup sets that meet precisely the Customer's requirements, thus eliminating the backup of unnecessary data.

In addition, these sets define the number of retained generations, or versions, of files and databases backed up. This enables the Customer to selectively restore any of the previous versions of files that have been backed up. The default is set at five generations.

Multiple backup sets can be defined for the same Customer system. This feature enables the Customer to define separate backups of different types of data on the same system. Multiple backup sets for the same system can also be actioned independently.

A backup set can only include data from a single Customer system; one or more backup sets must be defined for each system to be backed up.

Backup sets are defined in a similar manner for Microsoft Windows and Novell NetWare file systems and for backups of Microsoft Exchange and SQL Server. This single interface enables efficient administration of the MBS Service. Authorised administrators can manually execute ad-hoc backups, however, the normal method will be to schedule automatic execution of the backup sets.

Open file backup

By default, MBS will attempt to backup files that are opened, but not locked, by other applications on the Customer’s system. The Customer’s system administrator can further configure this functionality, either globally or by individual backup set, to define the method for handling open files and the number of backup re-tries to perform. The Customer’s Agent Console interface provides comprehensive online help information for defining these options.

Files that are completely locked by another application, such as Microsoft Outlook PST files, will not be backed up.

All open files that fail to backup are reported in the activity log on the Customer’s Remote Agent Console interface.

Backup Schedules

MBS has an extensive calendar based scheduler for automatically executing backup sets. Schedules can be defined to execute backups daily, weekly, monthly, or on a more defined frequency, such as the last day of the month.

Multiple schedules can be defined, and multiple backup sets can be associated with a schedule. Where multiple backup sets are associated to a schedule, the Customer's system administrator can define the number of concurrent backup sets to be executed and the priority in which they should be executed.

The Customer's Remote Agent Console interface provides a graphical view of the backup schedules. This allows the Customer's system administrator to quickly view the status of the backups and identify any conflicting or overlapping schedules. Agents can also be scheduled externally, allowing ultimate flexibility.

Monitoring Backups

The Customer's Remote Agent Console interface provides extensive monitoring and reporting capabilities for Customer administrators. This includes detailed logs of backup activity, details of all files backed up, error reports and audit trails for all backup and restore activity. Additionally failed backup e-mail notifications can be sent from the Agent to a system administrator.

Initial Data Collection

The primary method of backup is over the internet or service connection between the Agents on the Customer's site and the MBS Vault at InTechnology's Data Centre. However, in situations where the initial backup volume is such that a network transfer is impractical, InTechnology will collect and transport it to the data centre (depending on the service option chosen, this option will be charged for).

Where it is appropriate for InTechnology to manually transport the initial backup data, the process will involve installing a local drive / portable MBS Vault on the Customer's premises. Initial backups are performed to this temporary MBS Vault until an agreed time when the MBS Vault is disconnected and transported back to the data centre.

Once re-installed at the data centre the MBS Vault is re-configured and connected via the Service Connection. The Agents and the MBS Vault are then re-synchronised and normal service activity resumes.

Restoration

The Customer's Remote Agent Console interface allows the authorised Customer network administrator to quickly and easily select and restore data. Data can be restored to a remote system; for example, the administrator could use their desktop machine to restore data to a remote server. Multiple restore operations to separate servers can be performed from a Customer Remote Agent Console making this particularly suitable for a help desk role.

There are four methods in which data can be restored:

1. Online restore, where data is restored across the internet or service connection.

2. Restore of data is made available at the InTechnology data centre via a portable disk drive

3. Major disaster recovery, involving a portable MBS Vault being delivered to the Customer's site or alternative disaster recovery location

4. Recovery of data directly to a Customer server hosted in the InTechnology data centre.

The following table maps examples of restore categories to the four methods of data restoration.

Restore category	Volume of Customer data	Data available to restore (hours)
1 - Online Restore	1MB +	Immediately
2 - Portable Disk Restore	10 GB- 250 GB	4 - 12*
3 - Portable Vault (DR) Restore	250 GB +	12*
4 – Server Recovery	0-2,000GB	0-24h

* Excludes travelling time. These figures are guidelines, the accurate time to provide data for restore at the Customer's site depends on the data volume and number of files. At the time the restore request is issued to InTechnology, the customer support team will be able to advise more accurate data availability times.

Category 1 - Online Restore (Carried out by the Customer)

The primary method of data restoration is online. The Customer's Remote Agent Console provides a restore functionality that guides the Customer's administrator through the process of selecting and restoring data. This functionality allows the administrator to search and select files for restore, select the version of the files and choose the target destination for delivery.

Having selected the data to be restored, the MBS Agent then delivers the data from the InTechnology data centre to the specified system on the Customer's network. As part of the operation all associated security permissions for the data are also restored.

Category 2 - Portable MBS Disk Restore (Carried out by InTechnology in conjunction with the Customer)

During a restore situation, which cannot be accommodated via the service connection, and which does not require a full DR restore, the Customer would contact the InTechnology Support Team to invoke a portable disk recovery service. The only data that can be restored from the portable MBS disk is that which was specified when initially requested. If additional backup data is required then this can be restored either online or by a new request for a portable disk being initiated. Times vary according to the requirement when creating and completing a portable disk restore. Critical instances may involve a necessary upgrade to a portable system restore level. Please note that online backup and restore can continue whilst an onsite PDR is taking place.

Note

- The PDR has to be generated first (data copied onto disk) and then restored using the Agent on the Customer's site

- The backup-set is locked whilst the PDR is being generated, therefore no other backup or restore activity can occur

Category 3 - Portable MBS Vault (DR) Restore (Carried out by InTechnology in conjunction with the Customer)

The third restore option is to request a portable MBS Vault. This could be used as an alternative to the portable MBS disk or in a major disaster situation where complete backup data is required.

InTechnology will deliver the portable MBS Vault to either the Customer's site or an alternate disaster recovery location within the UK or at a mutually agreed location. The portable MBS Vault is then connected to the Customer's LAN. Data can then be restored in the same way as for an online restore.

For any investigative work carried out by InTechnology regarding a fault that is found not to be the responsibility of InTechnology, the Customer may incur charges. Details will be passed onto the InTechnology Sales Representative.

Customer online backups and restores will be suspended whilst this exercise is taking place and will not be able to re-commence until the system is returned, and set-up, in the InTechnology data centre.

Category 4 – Server Recovery (Carried out by InTechnology in conjunction with the Customer if the recovery server is manage and provided by InTechnology)

- The standby DR server is powered up by the Customer
- InTechnology provide copy of the backup data to DR server
- The Customer recovers the data

Installation and Configuration

The following details what will happen upon signing of the Service Agreement and the sequence in which the Managed Backup Service will be installed.

Pre-Installation - The InTechnology service delivery team will call the Customer nominated technical contact and verify all the technical details prior to proceeding with Phase 1 of the MBS installation.

Phase 1 - Installation of MBS Agents on target machines.

Phase 2 - Transfer of the Customer's data offsite, testing and sign off.

Phase 3 - One month after the installation an InTechnology customer implementation engineer will contact the Customer to arrange a post installation review. The purpose of the review will be to address any issues the Customer may have and to ensure that the Service is providing the protection to the Customer's data

Training

InTechnology will ensure the Customer is trained on how to use the service. This will ensure that the Customer achieves the maximum benefit of the service provided. In most case this training is going to be delivered onsite, as part of the service installation. Alternatively InTechnology may decide to provide this training at one of InTechnology's offices.

Acceptance Criteria

The following acceptance criteria will be demonstrated during the service delivery process and the Customer's signed approval will signify that the service as described in this service definition is ready for use:

- Verify the Customer has copy of account details
- Demonstrate installations of agent(s), agent console and registration with the MBS vault
- Demonstrate backup task creation
- Demonstrate backup schedule creation
- Run sample backup task (file system data)
- Restore sample backup task to alternate location

Note: the Customer will nominate (Pre-Installation) and make available (Phase 1) an appropriately qualified representative to work with the InTechnology representative during the installation of the Service Connection.

The nominated Customer representative will confirm the completion of Phase 1 and will accept delivery of the MBS Service as a fully commissioned service (Phase 2). Upon completion of Phase 2 and notification by the InTechnology Customer Support Team the nominated Customer representative will sign the Service Sign-off Document and return this to InTechnology. Installation will be carried out between 09:00 - 17:30, Monday - Friday.

Service Management & Reporting

E-mail Report

The daily e-mail report forms part of the MBS Management Layer. It provides an overview of the backup and recovery processes across the Customer's entire estate, be that one site or a multi-site environment. The daily e-mail report is described below.

Aims

The MBS system currently emails Customers daily usage reports to users to give a view on activity and storage usage. This document aims to provide an overview of the Customer report and to give an understanding on the data contained within the report.

Report Overview

A report is sent to the Customer on a daily basis, this Customer report aims to give the Customer an overall picture of the status of the backup sets, the storage used by the backup sets, and the number of activities recently completed. The report is generated and sent to the Customer at 08:00 each day.

Report Breakdown

The report is broken down into two main sections, 1) Customer Summary and 2) Location Summary. The first section provides a summary of the storage and activities for the Customer; the location section is repeated for each location and provides a more detailed view of activities and possible faults. The sections are explained in more detail below:

Customer Summary

The summary contains high level summary data regarding the current state of backup sets. It is a count of backups in each category from the "Last Successful Backup Report" given for each location later in the report. The deferred backup sets entry will only appear if the Customer has agent reporting configured, and can only show defers which happened on backup tasks which specifically have agent reporting configured.

<u>Activity Summary</u>

The activity summary section shows the Customer's locations, with a single line for each of the backup and other tasks that have run since midnight the day before this report was generated. For each location and task type the following items are detailed:

- The number of jobs that have run (not all of these may have been successful), both the current period, and the period 7 days ago for comparison
- The amount of data transferred during the process, in Gigabytes
- If the number of tasks run 7 days ago is different to that run with the last day, or the amount of data transferred is significantly different, then the cells are highlighted in a yellow colour. Activities that can be detailed are backups, imports, exports, restores and archives.

<u>Storage Usage</u>

The storage usage graph shows the total billable storage used by the Customer, along with the top 10 locations (in terms of current storage, so a previously large location that is currently small will not show on the graph). The graph covers the last 60 days. The graph data uses floating point data based on the byte count converted to Gigabytes.

Storage Summary

The storage summary provides a breakdown per location of the restorable amount and the stored size. This indicates how efficient the service is and how much Customer data is being protected. The stored size is the space taken up on the vault; it does not include space overhead in the pool files, or any overhead used by InTechnology. During each day vault activities will change this figure. The stored size figure used in the Customer report is the lowest figure for the previous calendar day.

The total restorable figure is the total amount of storage that has been backed up by the Customer across all save sets. If a drive contains 10GB of files and has been backed up 10 times the protected storage figure will be 100GB. During the day backup, and migration tasks will change this figure, The total restorable figure used in the Customer report is the maximum figure for the previous calendar day.

Location Summary

The location section contains 3 reports and is repeated for each Customer location.

Last Successful Backup Report

This report details each backup set defined within the location, and when the backup last successfully ran. Failed backup are ignored in this report. A successful backup is defined as one that contacted the vault, transferred data and completed without a pool system or communication error - however it is not a guarantee that the backup covered everything that it should have done (for example if the agent was unable to talk to a SQL server then this could still count as a successful backup to MBS).

Backup sets that have completed within the last 24 hours are marked in blue, ones that completed within the last three days are marked yellow, and backups that have not completed within the last 3 days (or have never run) are marked in pink.

Backup Storage Usage Report

The backup storage usage report is a detailed report showing each backup set currently defined within the location, and the current storage used. If the Customer has more than one location a thumbnail graph of the location's storage usage over the past 60 days is also shown (this is suppressed for single location sites since it would just be a low resolution duplicate of the main graph). During the day we run many internal storage reports on the vault. These internal storage reports provide InTechnology with two following basic figures on the vault:

a) Stored Size

The Stored size is the space taken up on the vault; it does not include space wasted in the pool files, or any overhead used by InTechnology. During the day vault activities will change this figure; the stored size figure used in the Customer report is the lowest figure for the previous calendar day.

b) Total Restorable

The total restorable figure is the total amount of storage that has been backed up by the Customer across all save sets. If a drive contains 10GB of files and has been backed up 10 times the protected storage figure will be 100GB. During the day backup, and migration tasks will change this figure, the Total Restorable figure used in the Customer report is the maximum figure for the previous calendar day.

Agent Reports

In order to offer this functionality the agent must be configured by the Customer to send success / failure reports to InTechnology. Agent reporting allows InTechnology to collect the agent reports locally, transfer them to the MBS backend vault, from where InTechnology can extract information on successful backup, backups with errors and failed backups per location and agent and append it to the daily e-mail report.

The agent reporting section gives a summary of the Agent reports emailed to the MBS backend. Successful backups are shown with a green tick, failed ones with a red cross. For details of the reasons for failure or errors the user must look at the backup logs using MBS central console. Agent reports entries are only shown if they failed, or if there are some errors, or if there is deferred backup data. Completely successful entries are not displayed unless the same backup set had an earlier error. The columns and meanings are as follows:

- Time: the time the backup started
- Computer: the computer that ran the backup
- Task: the backup task Name
- Status: Failure or Success as reported from the agent
- Function: Backup or Restore
- Errors: the number of client side errors reported by the Agent
- Warnings: the number of client side warnings reported by the Agent
- Deferred: if the Agent reaches the optional time limit this is the number of bytes left to backup; it could indicate the backup task is not fully protected
- Transfer Size: the size of the data transferred over the wire between the agent and the vault, measured in GB

Restarting Backups

If a backup fails to complete InTechnology will log a service call and endeavour to restart the backup within 2 hours of the backup failing and email the Customer to let them know that a backup has failed and has been restarted. It is the responsibility of the Customer to either stop this manual process or leave it running.

InTechnology will use the Remote Agent Console as the mechanism to access the Customer's backup agents to restart a failed backup. This requires for the Customer to have configured the agents to point to the Remote Agent Console.

Managed Backup Service - Service Level Agreement

This Service Level Agreement ("SLA") details the agreed target levels of performance of the MBS Service provided by InTechnology to the Customer:

a) the level of services to be provided by InTechnology for the MBS Service in terms of availability and response time
b) specific responsibilities for both InTechnology and the Customer to ensure that the Managed Backup Service is properly commissioned
c) the mechanism for reviewing InTechnology's performance in providing the Managed Backup Service
d) what will happen in the event that a problem occurs

InTechnology Responsibilities and Obligations

InTechnology will provide an automated mechanism whereby the Customer will be able to backup data from all designated servers and network connected desktop computers as defined in this Service Definition. The Managed Backup Service downtime will not exceed the stated availability below.

Subject to the conditions outlined in this SLA, InTechnology will undertake that the Managed Backup Service delivered to the Customer will function as specified.

Restarting Backups

This support functionality is only available to Customers who have access to the Enhanced Management Layer.

If a backup fails to complete, InTechnology will log a service call and endeavour to restart the backup within 2 hours of the backup failing and email the Customer to let them know that a backup has failed and has been restarted. It is the responsibility of the Customer to either stop this manual process or leave it running. If Agents are not visible in the remote agent console, InTechnology will not be able to restart backups and thus these agents will not be covered by this SLA clause.

Replicated backup sets

If the Customer has opted for backup data to be replicated, the replicated copy will be failed over to within 4 hours of the primary backup copy being unavailable for backup and restore purposes.

Customer Responsibilities and Obligations

Although the Managed Backup Service is a managed service and InTechnology will be responsible for the availability and support of the service components, the day-to-day operation of the Managed Backup Service will, in part, depend on certain key processes and related equipment which are wholly under the Customer's control. The Customer will also be responsible for the provision, installation, management and support of any internal network connectivity at the Customer's site required to deliver this service.

Support Process

The nominated Customer representative will be responsible for promptly reporting any problems directly to the InTechnology Customer Support Organisation in accordance with the escalation procedures outlined in the support process section (*Customer Service Plan*).

Reports

The Customer will be responsible for reviewing and acting upon the reports provided by the Managed Backup Service, such as reviewing the detailed logs generated by the Service.

Managed Backup Service Availability

Managed Backup Service Availability	**Equivalent downtime per month (24 x 7 x 365)**
99.0 %	7 hour 18 minutes

The SLA for MBS Vault availability will be 99.0% availability in any one month. The MBS availability measures the proportion of time in any given month that the MBS Vault in the InTechnology data centre is available for backup and restore of the Customer's data. The availability measurement will be the total amount of time in any one month that the MBS Vault is available to backup and restore data to and from the Customer's associated server(s) as percentage of the total number of hours in that month.

This means that if the MBS Vault exceeds a total cumulative downtime of more than 7 hours and 18 minutes in any one calendar month it will be considered to be outside of the SLA. Downtime (i.e. periods when the MBS Service is unavailable) will be measured from when the fault is logged by the Customer or identified by InTechnology support to the time when the MBS Vault becomes available for operational use.

Each percentage point or part of a percentage point that the MBS Service availability for the month in question is less than 99.0% availability, shall be considered as one instance and InTechnology shall pay service credits to the Customer in accordance with the Service Credits section below.

Planned Maintenance - Reserved Windows

The window for planned maintenance is Mondays from 11:00-15:00 and Thursdays from 11:00-15:00. In exceptional circumstances, there may be an emergency requirement to instigate work outside of these maintenance windows. However, every effort will be made to avoid disruption during core service hours and prior notification will be issued at the earliest possible opportunity.

Total Service Outage

When a platform or system upgrade is planned that will result in a total system outage affecting all Customers, InTechnology will endeavour to give 7 days prior notice to allow Customers time to limit any impact on their own operations.

Exclusions:

- Downtime due to InTechnology network outages – the Service Connection between the Customer network and the InTechnology data centre(s)
- Downtime due to problems on the Customer’s network, either within a the Customer’s site or between sites
- Planned downtime for maintenance of equipment where adequate written notice has been given to the Customer
- Problems that have occurred due to actions or failure to perform necessary actions by the Customer

Service Credits

The following service credits will apply based on the criteria detailed in the MBS Availability section above. In the event that the MBS Vault falls outside of the SLA, i.e. the downtime on the MBS Vault exceeds a cumulative total of 7 hours and 18 minutes (99.0% availability) in any one month, then a service credit shall apply based upon a percentage of the maximum service credit per instance (i.e. where a specific MBS Vault falls outside of the SLA in any one month) as calculated below. The Maximum Service Credit per instance = Total monthly Managed Backup Service charge.

The table below details the sliding scale of service credits that will be applied based on the number of MBS Vault instances outside of the SLA in any one month.

Total number of instances of the MBS Vault falling outside of SLA in any one month	**Percentage of maximum service credit paid per MBS Vault instance.**
1	5%
2	10%
3	20%
4	30%
5	40%
6	50%
7	60%
8	70%
9	80%
10	90%
11+	100% (Maximum)
Where any one instance exceeds the SLA and the MBS Vault is unavailable for operation (i.e. the Customer is unable to perform a backup or restore) for longer than 72 hours	100% (Maximum)
Important: Regardless of the total number of client instances the total service credit paid in any one month will not exceed the total monthly service charges for the month.	

Managed Backup Service Charges

Installation Charges

The following table details the chargeable elements associated with the installation of the Managed Backup Service. Please note an increase in data volumes may require some or all of the components of MBS to be upgraded at some point in the future, thereby incurring additional charges.

Service Element	Details
Service activation	InTechnology will install the Agent software and Plug-ins on all source servers, provide training for customer admin staff and enable the offsiting of backup data
Agent Plug-ins MS Exchange Agent Plug-ins MS SQL Cluster Agent Plug-ins	The additional application agent software required to backup specified application data
Data Capture	Initial data capture for one site (typically carried out over the service connection)

Monthly Charges

Service Element	Details
Data Storage Charge (DSC) for Primary Backup Data	The variable charge based on the peak amount of MBS data stored at the InTechnology data centre
Data Storage Charge (DSC) for Secondary Backup Data	The variable charge based on the peak amount of MBS data stored at the InTechnology data centre

Notes on Charging

- The Monthly Data Storage Charge (DSC) is a variable charge based on the actual peak volume of data stored on the MBS Vault in each month. If data volumes increase or decrease the Data Storage Charge (DSC) will increase or decrease. InTechnology will charge for the compressed data stored within the secure data centre and not the transferred data volume.

- Where MBS is to be provided at multiple sites then the Charges for a particular sites will be chargeable from the date MBS becomes available at that site and will be invoiced monthly/quarterly in advance/arrears (as the case may be) from such date.

Optional Services

The following table illustrates the additional services / consultancy InTechnology can provide through its Technical Consultancy and 3rd line Customer Support Teams.

Service Element	Details
Agent and Agent Plug-in Installation	InTechnology's consultants will provide onsite assistance in installing agents and establishing backup tasks
Data Collection via a Portable Vault for additional sites	InTechnology's consultants will capture the data onsite via a Portable Vault and transfer it to the remote data centre
Additional Training Courses	Scheduled training courses on topical subjects at InTechnology premises
Second copy of all Customer data	Stored in an alternative InTechnology data centre
Portable Disk Restore (PDR) up to 250GB	Shipping Portable Disk to the Customer's site
Portable Disk Restore (PDR) up to 250GB with onsite support	Delivering Portable Disk to the Customer's site and initiate restore of data
Portable MBS Vault Restore - DR or Test DR	Delivering Portable Vault to the Customer's site to initiate restore for DR or Test DR purposes
Agent Plug-ins (for MS Exchange, MS SQL, MS SharePoint and Oracle)	The application agent software required to backup specified application data
Cluster Agent Plug-ins	The application agent software required to backup specified clustered application servers
VMware Agent Plug-in	The application agent software required to backup VMware servers
Satellite Vault	The Satellite Vault is an onsite software installed on customer servers to provide two significant benefits: high-speed backups and restores and disaster recovery protection. It works by allowing you to have satellite vaults at each of your company's locations, and automatically replicating their backup data to the main Managed Backup Service vault in the InTechnology Data Centre.
Bare Metal Restore	Bare Metal Restore (BMR) is a standalone software module that compliments the Managed Backup Service (MBS) but is not integrated with MBS as such . BMR is used to quickly recover an unusable system after catastrophic failure
Continuous Data Protection	Continuous Data Protection (CDP) is a standalone software module that compliments the Managed Backup Service (MBS) but is not integrated with MBS as such. CDP is a backup and recovery software product that provides up-tothe-minute protection of your mission critical systems.

Generic Notes on Charging

- Service activation charges cover the installation of Services during normal working hours (09:00-17:00, Monday – Friday). Installations required outside of these hours will be charged at a hourly rate. Installations requested by the Customer to be undertaken outside of normal working hours should be agreed in advance between InTechnology and the Customer and must be accompanied by a customer specific purchase order or an email of intent.

- Important: the initial monthly charge has been based on information provided by the Customer, in particular an estimate of the volume of data to be replicated, backed up and / or archived.

- It is recommended that the Customer maintains their existing backup solution until Phase 2 installation (as detailed within the MBS Service Definition) is complete and signed off.

- A day rate for consultancy services provides for the hours of 09:00-17:00. Expenses are included in the charge unless otherwise agreed.

- The sizing of the all service components has been based on information provided by your own employees. Any subsequent configuration changes required for any of the service components as a result of increased workload, data volumes or managed servers will result in an amended Monthly Charge.

- The initial software management charges (where appropriate) is based on information provided by your own employees. InTechnology will provide appropriate software licenses to meet this requirement. Addition or removal of customer servers and / or increasing the number of licenses required will result in an amended monthly license charge.

Service Exclusions

- Rebuild of Customer hardware or operating system environment

- Support for operating systems other than replication, backup and recovery and /or archiving issues related to the operating system.

- Support for Customer's network infrastructure

- Support for Customer's application software

InTechnology designs and supports the best IP solutions for business with a range of applications seamlessly integrating clients' communications needs through the delivery of secure voice, data and mobile solutions.

InTechnology employs 200 people and has data centres in Harrogate, London and Reading.

Head Office

Central House
Beckwith Knowle
Harrogate
HG3 1UG
Tel: 01423 850 000

London Office

17 St Helens Place
Bishopsgate
London
EC3A 6DG
Tel: 0203 040 5000

Reading Office

Commensus House
3 – 5 Worton Drive
Reading
RG2 0TG
Tel: 0870 777 7778

Enquiries: 0800 528 2522
www.intechnology.co.uk

inTechnology