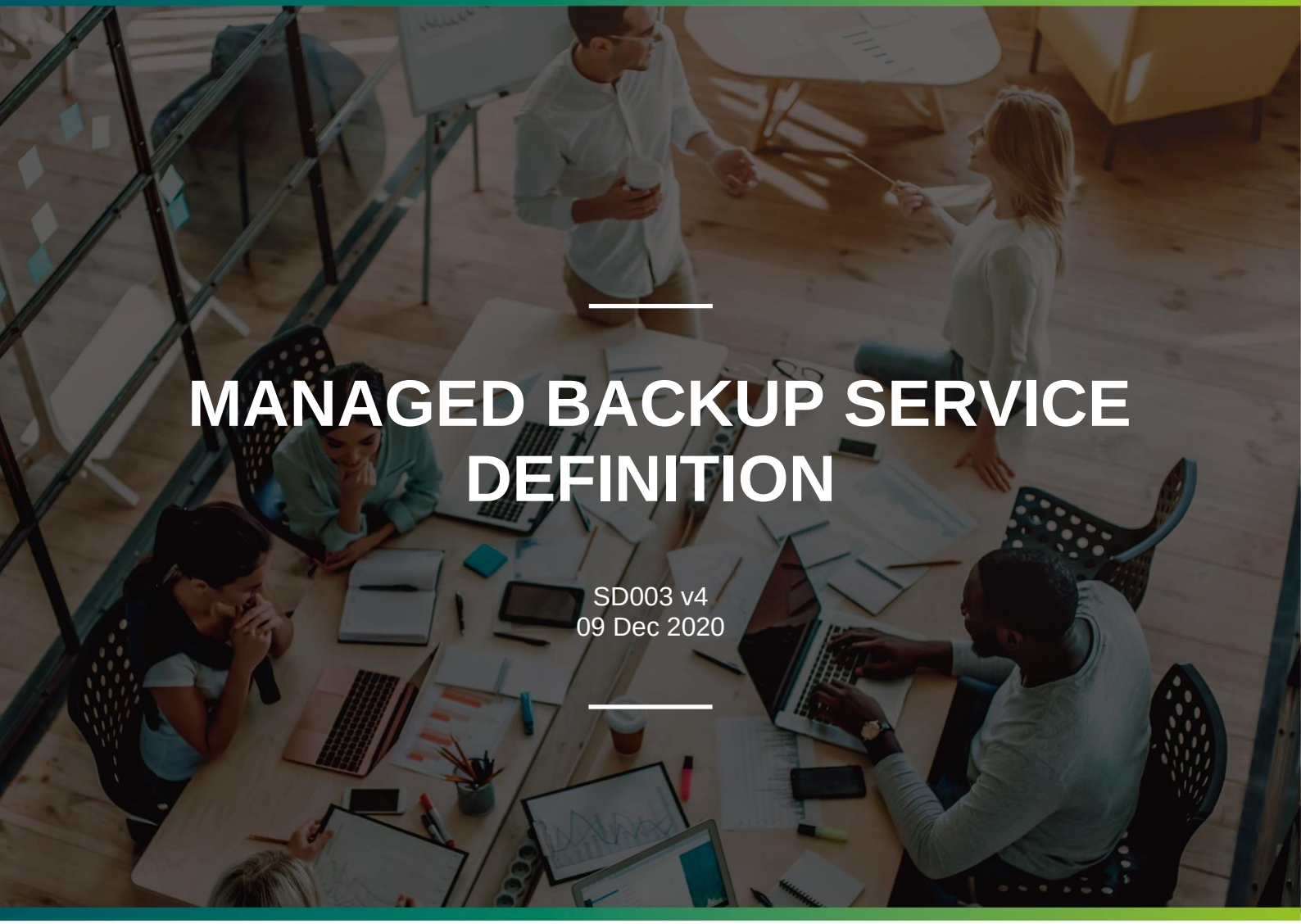

MANAGED BACKUP SERVICE DEFINITION

SD003 v4
09 Dec 2020

redcentric

AGILE • AVAILABLE • ASSURED

1. Service Overview

The Managed Backup Service (MBS) is a streamlined 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 servers and application / databases 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

Companies requiring data protection and rapid recovery want simplified management through one vendor, cost-effectiveness, more operational control, reliability, 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 back up their data to a remote storage device over common telecommunication connections. MBS allows for online restores of backup data transmitted over the same or alternate telecommunication connections.

2. Service Description

MBS centralises the backup and recovery of data on servers distributed across your organisation by utilising locally installed agents, giving you the ability to granularly protect a wide range of servers and applications.

2.1. Service Architecture

An MBS agent locally encrypts and compresses your data. The data is then sent to a vault held in one of the Redcentric datacentres over either a Wide Area Network (WAN) or Virtual Private Network (VPN). The vault, managed by Redcentric 24/7 staff stores the data in a SIDF standard format accessible only to the account provided to the Customer.

2.1.1. Vault

The vault, which is managed by Redcentric, provides backup and restore functionality to any number of remote agents. In addition to online transaction processing with clients, the vault's key function is to manage the storage and migration of backup data. Based on the parameters defined by the agent each backup has a life span and may be migrated from online storage to archive or deleted depending on policy.

2.1.2. Agent

The MBS agent is a lightweight application running on the host system. Depending on the host operating system an agent can take many forms. On Novell the agent runs as an NLM module, whilst a Microsoft Windows server would see the host running as a service.

1) Plugins and supported platforms

MBS supports the following operating systems and applications, in line with vender support and end of life cycles. Redcentric will endeavour to support future versions of the operating systems below:

- Windows
- Solaris
- Linux
- Novell NetWare
- MS Exchange
- MS SQL Server
- VMware
- SharePoint

The following operating systems and databases are not supported by Redcentric; however the MBS agent can be used and supported by the Customer to complete backups of these systems and databases:

- IBM AIX
- HP UX
- Oracle

A full list of supported versions and service levels can be found here: www.Redcentric.co.uk/downloads

2.2. 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 attached storage devices where there is no possibility of installing the backup agent.
- Microsoft Exchange Server (database) – this allows you to back up the entire Exchange database for disaster recovery purposes
- Microsoft Exchange Server (mailboxes and public folders) – this allows you to back up any combination of mailboxes and folders
- Microsoft SharePoint Server
- Microsoft 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

2.3. Backup parameters

2.3.1 Agent Management

MBS can be managed in two ways: either via a locally installed management console or via a web accessible centrally hosted console. The MBS agent console can reside on any network machine with visibility of the servers you wish to protect, providing a full graphical user interface to provide control over task configuration, backup and restore activities, retention configuration and account details amongst many other features.

The remote agent console (RAC) allows any agent you have installed to securely communicate with a centrally managed support tool, giving you all the features a standard agent console would provide, with the added benefit of being able to manage backups remotely from your server network. Further to this the RAC provides a management summary of the current state of backups in your environment.

2.3.2. 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 vault 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 vault.

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.

2.3.3. Encryption

MBS encrypts data at source, over the wire and at rest by default. A further layer of encryption can be applied at source using one of the 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 Customer. If they lose the password for whatever reason, the entirety of their encrypted backup data is no longer readable and neither the Customer nor Redcentric can recover the data.

2.3.4. Agent Plugins

A standard MBS agent will backup flat file and UNC path backups. Any further application level backups will require a plugin, these include:

- SQL
- Exchange
- Oracle
- Clustering
- SharePoint
- VM

A plugin is a customisation to the standard MBS install.

2.4. Satellite Vault

The satellite vault is onsite software installed on the Customer's servers to provide two significant benefits: 1) high-speed backups and restores and 2) disaster recovery protection. It works by allowing the Customer to have satellite vaults at each of the company's locations, and automatically replicating the backup data to the main Managed Backup Service vault in the Redcentric data centre. It requires one of the following satellite vault licences and can be used in a number of ways.

- 250 GB satellite vault
- 500 GB satellite vault
- 2000 GB satellite vault

2.4.1. Onsite Vault

Redcentric can provide a fully licensed unmanaged on site vault allowing local area network backup and restore speeds, on a Customer maintained device. The vault licence can be procured for use on Customer equipment; alternatively Redcentric can provide both the software and hardware for this service at an additional cost. In addition to this Redcentric can also provide remote support for the vault configuration and internal maintenance tasks. This vault would be stand alone on a Customer site with no offsite replication.

2.4.2. Many-to-One Vault

An MBS many to one vault emulates the same features as an onsite vault, as well as allowing unlimited storage on the local device (defined by the hardware itself) and also integrates replication to a Redcentric data centre. Redcentric can also support the base vaults at an additional charge. This feature would require an additional licence i.e. to enable the replication of data to the Redcentric MBS vault.

2.5. Backup and Restore

2.5.1. 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.

2.5.2. 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.

2.5.3. 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.

2.5.4. 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 Redcentric's data centre. However, in situations where the initial backup volume is such that a network transfer is impractical, Redcentric 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 Redcentric 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.

2.5.5. 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 Redcentric 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 Redcentric 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 Redcentric, the Customer support team will be able to advise more accurate data availability times.

2.5.5.1. **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 Redcentric 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.

2.5.5.2. **Category 2 - Portable Disk Restore** (carried out by Redcentric 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 Redcentric 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. Online backup and restore can continue whilst an onsite portable disk restore is taking place.

It is important to note that the portable disk restore 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 portable disk restore is being generated, therefore no other backup or restore activity can occur

2.5.5.3. **Category 3 - Portable Vault Restore** (carried out by Redcentric in conjunction with the Customer)

The third restore option is to request a portable vault. This could be used as an alternative to the portable disk or in a major disaster situation where complete backup data is required. Redcentric will deliver the portable vault to either the Customer's site or an alternate disaster recovery location within the UK or at a mutually agreed location. The portable 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 Redcentric regarding a fault that is not the responsibility of Redcentric, the Customer may incur charges.

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 Redcentric data centre.

2.5.5.4. **Category 4 – Server Recovery** (carried out by Redcentric in conjunction with the Customer if the recovery server is provided within one of Redcentric's data centre)

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

2.6. Reporting and Monitoring

2.6.1. E-mail Report

The daily e-mail report provides an overview of the backup and recovery processes across the Customer's entire environment. The report is sent to the Customer on a daily basis, and 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. The report provides a high level view of the current state of the backup environment allowing you to quickly pinpoint any issues that need investigating.

2.6.2. Remote Agent Console Monitoring

In addition to the standard e-mail report there is also the option to use the remote agent console as a reporting tool. A dashboard view is provided at first login to the remote agent console portal, giving you an overview of all failed tasks, tasks with warnings or tasks with errors.

2.6.3. Monitoring Backups

The Customer's remote agent console or local 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. Notification can be configured to alert Redcentric's support team of backup failures allowing them to investigate and if necessary restart backup failures

2.6.4. Restarting Backups

If a backup fails to complete Redcentric 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. Redcentric 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.

2.7. Data Deletion

The Customer can delete data from MBS via the agent in the portal. Portal users will need to be assigned the admin role to be able to submit deletion requests.

Once the deletion has been submitted it will be queued for seven days before being actioned on the back-end vault. Once the deletion has been actioned on the vault the data cannot be recovered by Redcentric.

3. Implementation and Acceptance

3.1. Service Delivery

The service delivery of MBS is determined by the option chosen by the Customer in the Order Form. Depending on the service option chosen, the following activities will either be performed by Redcentric or the Customer:

1. Installation of the agent and a local management console if being used. Alternately configuration of remote agent console communication if no local console is being used.
2. Configuration of backup tasks including the files and directories that require protection
3. Configuration of schedules, encryption methodology, vault passwords and type of backups for each machine.

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

The supported application agents only backup the selected application data. In addition to the application agent the appropriate file system backup client must also be installed and configured to back up 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.

3.1.1. 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 vault at Redcentric's data centre. However, in situations where the initial backup volume is such that a network transfer is impractical, Redcentric 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 Redcentric to manually transport the initial backup data, the process will involve installing a local drive / portable Vault on the Customer's premises. Initial backups are performed to this temporary vault until an agreed time when the vault is disconnected and transported back to the data centre. Once re-installed at the data centre the Vault is re-configured and connected via the service connection. The agents and the vault are then re-synchronised and normal service activity resumes.

3.2. 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 a copy of account details
- Demonstrate installations of agent(s), agent console and registration with the vault
- Demonstrate backup task creation
- Demonstrate backup schedule creation
- Run sample backup task (file system data)
- Restore sample backup task to alternate location
- Ability to backup and restore flat file data to a Windows Server
- Ability to backup and restore SQL via plugin/API (if SQL agent plug-ins have been ordered by the Customer)
- Ability to backup SharePoint and restore DR via SQL or item via granular restore tool (if SharePoint and SQL agent plug-ins have been ordered by the Customer)
- Access to remote agent console for agent configuration, task creation, scheduling, ad hoc backup/restore running, backup set data and logs or access to local agent console for DMZ / DR or unsupported remote agent console configurations for agent configuration, task creation, scheduling, ad hoc backup/restore running, backup set data and logs
- Delivery of daily email report showing point in time backup status as at 08:00 daily
- Access to download page for agent installation code
- Delivery of (or of link to) agent installation & configuration instructions

The Customer will need to nominate (pre-installation) and make available an appropriately qualified representative to work with the Redcentric representative during the installation of the service connection. The nominated Customer representative will accept delivery of the Managed Backup Service as a fully commissioned service and sign the service sign-off document and return this to Redcentric. The installation will be carried out between 09:00 - 17:30, Monday - Friday.

4. Service Levels and Service Credits

4.1. Service Levels

4.1.1. Reporting and Monitoring

4.1.1.1. 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 report is sent to the Customer on a daily basis, and 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. The report provides a high level view of the current state of the backup environment allowing you to quickly pinpoint any issues that need investigating.

4.1.1.2. Remote Agent Console Monitoring

In addition to the standard e-mail report there is also the option to use the RAC as a reporting tool. A dashboard view is provided at first login to the RAC portal, giving you an overview of all failed tasks, tasks with warnings or tasks with errors.

4.1.1.3. Monitoring Backups

The Customer's remote agent console or local 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. Notification can be configured to alert Redcentric's 24/7 team to backup failures allowing them to retroactively investigate and if necessary restart backup failures

4.1.1.4. Restarting Backups

If a backup fails to complete Redcentric 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.

Redcentric 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.

The Service Level applicable to the Managed Backup Service is as follows:

Service Level: Availability **Measurement Period: Month**	
Measured element	**Availability**
The MBS vault	Availability: Not less than 99.0%

4.2. Floor Service Level

The Floor Service Level applicable to the Managed Backup Service in respect of Availability of the MBS vault shall be 85% in any given Month.

4.3. Service Credits

The Service Credits applicable to the Managed Backup Service shall be calculated as follows:

The formula for calculating the Service Credits shall be:

Service Credit = (C x S) / MS

Where:

S = the number of seconds by which Redcentric fails to meet the Service Level for Availability in the relevant Month

C = total Charges payable in respect of the Service for the same Month

MS = total number of seconds in the same month

5. DATA PROCESSING

5.1. Data Processing Scope

- MBS backs up data from Customer servers and stores it in shared storage servers (vaults) in the Redcentric datacentre.
- The back-up jobs are configured and managed by the Customer. Redcentric does not in the normal course of business have any operational involvement in the management of the individual backup jobs.
- Although this service is called Managed Backup Service, the management is done by the Customer.
- In the course of normal operations Redcentric does not and is not able to access, alter or use the data (because it is usually encrypted by the Customer and only the Customer has access to the encryption keys).

5.2. Data Storage and Unencrypted Data

- MBS provides two levels of data encryption.
- The data is automatically encrypted during transmission from the Customer's servers to the MBS storage vault. Prior to transmission the data is de-duplicated, compressed and encrypted. Only the Customer knows the encryption key for the transmission encryption algorithm.
- Customers have the option to encrypt their data and have it stored in an encrypted state. This encryption uses an encryption key that only the Customer knows. Redcentric cannot access the encrypted data as Redcentric has no way of obtaining the encryption key.
- Data is stored in storage vaults dedicated to the MBS service in the Redcentric datacentres.
- In the event that Customers have not encrypted data Redcentric has the capability to access the unencrypted data held in storage. However, during the course of normal business operations Redcentric does not access Customer data and would only do so in the course of providing support services, and at the request of and in conjunction with the Customer.
- Because Redcentric does not know or have access to the Customer's encryption key for transmission or storage encryption, if the Customer loses that key there is no way Redcentric can recover the data.

5.3. Data Processing Decisions

- In the normal course of business Redcentric does not make any data processing decisions in relation to the Service.
- The MBS service is configured by the Customer using the Remote Access Console (RAC). Using the RAC Customers can decide what data to backup, how frequently, whether to encrypt it, how long to keep it etc.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer. Even during such interventions, if the data is encrypted Redcentric cannot access it.

5.4. Service Configuration with Respect to Data

- The service configuration parameters (back up frequency, duration of storage, use of encryption etc.) are controlled by the Customer.
- When the initial download of data to set up the initial backup is done using a portable storage vault, that backup uses encryption for transmission and storage of data, again with only the Customer having access to the key.

5.5. Sub-Processors

- No other parties are involved in delivering this service, and there are no sub-processors.

5.6. Customer Access to Data

- Through their login to the Remote Access Console the Customer has access to restore their backed-up data and change the backup configurations.

5.7. Security arrangements and options

- The data is automatically encrypted during transmission.
- Customers have the option to encrypt their data and have it stored in an encrypted state using an encryption key that only they know.
- The stored data is held at Redcentric's datacentres with physical data centre security and cyber security measures (e.g. Firewall) in place.

5.8. Service Options

- The only options available to the Customer are in the way they configure their backups.

5.9. Compliance with Specific GDPR Requirements

The statements below are taken from the Carbonite (the company that provide the software that 'powers' the MBS service) GDPR compliance statement available on their website.

Right to Rectification

- Backups capture any and all changes made to source data.
- So when source/production data is corrected/verified those changes will be reflected in the next backup.

Right to Erasure

- Data retention periods are configurable to wipe old datasets after a predetermined period.
- If the retention period is 30 days any old backups would be deleted after 30 days, effectively erasing the data.

Right to Privacy

- The solution separates the administrative portal from the encryption keys, ensuring that if the admin credentials are compromised, customer data isn't at risk.
- Encryption keys are held by the customer, not the service provider, which further protects data.

- Encryption is to AES-256 with one key per customer, so unauthorised access to one key will not compromise all the data.

Records of Processing

- To assist with data processing record keeping requirements, system logs can be used to show what has been both backed up and purged.

HEAD OFFICE

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522
E sayhello@redcentricplc.com
W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED