Information Management & Technology

Document No:	AWP/ IT/LP/ITOPS-009
Title:	AWP IT Backup Strategy and Procedure
Version:	2.0
Date:	06/04/2009
Author:	IT Operations Manager
Distribution List:	IMT Operations
Number of Pages:	17 Double-click here to update number of pages
Approval:	Head of IT

Version	Date	Author	Version Description
1.0	8/12/2008	IT Operations Manager	Initial Draft
1.1	12/1/2009	Deputy IT Operations Manager	Modification after decommission of AX100 SAN (RVN00-FILEDR)
1.2	26/3/2009	Deputy IT Operations Manager	Implementation of additional storage to increase retention
2.0	06/04/2009	Approved by Head of IT	Approved version for procedures library

Central Offices
Bath NHS House
Newbridge Hill, Bath, BA1 3QE

Table of Contents

Double-click here to update TOC

1. Introduction

The purpose of this document is to give an overview of the Backup process for AWP's IT systems.

2. Scope

The Trust backup procedures cover the applications and data stored on servers located at the Trusts primary IT Suite at Bath NHS House and it's DR suite at Callington road.

2.1. Desktop Computers

Desktop computers are configured to use network storage and utilise Citrix or browser based technology access corporate and national application. As such there should not be any business critical data stored locally on desktops computers.

Based on this no additional backup processes are in place for desktop computers.

2.2. Laptops computers

Laptop computers are configured in one of three way:

- Stand alone, only applications that have no requirement for data backup and installed
- Network attachable, which can store data locally but synchronise any local data back to network storage when attached to the Trust network
- Mobile thin clients, which do not store data locally and just use mobile wireless technology to act as a thin client

Based on this no additional backup processes are in place for laptop computers.

3. Background Information

The Trust performs backups of it production servers located at Bath NHS house to it's DR facilities at Callington Road on a daily basis. The Trust uses a dedicated server (RVN00-Backup) running Symantec Backup Exec to archive the required data to a pair of Dell MD3000 iSCSI storage units which act as the primary storage for the Trusts backup. The MD3000's are configured using RAID 5 sets to reduce the risk of data loss from device failure and wherever possible the backup processes are split across both units to further increase redundancy. The server also has a Dell PowerVault PV132T tape library which is used to provide the option of archiving to tape if required. The configuration of the Backup server and MD3000's can be seen in appendix B.

Exchange, Enterprise Vault, print queues and Active Directory are backed up directly from the production servers at Bath to the backup archive

For the other systems the production systems are replicated on a daily basis to that systems disaster recovery server located at Callington Road. These disaster recovery servers are then backed up as required to the backup archive.

The following equipment to achieve this

Device	Role
RVN00-BACKUP	DR server for user and workgroups storage
RVN00-DR-EFIN-DB	DR server for Cedar eFinancials System
RVN00-MHISDR	DR server for MHIS System
RVN00-DR01	DR server for all other systems

RVN00-BACKUP	Server used for backup data to backup
2 x MD3000 iSCSI SAN	Storage for backup archive
PowerVault 132T	Tape library used for one off and long term archival

4. Key Dependencies

Key dependencies to the Backup System are :-

- Core Switches at Bath and Callington
- Telewest 1GB Link Bath - Callington
- Domain Controllers and DNS servers used for authentication on the AWP.NHS.UK domain and mapping addresses

5. Access Control

Physical access to the Servers is restricted currently unrestricted, recorded or monitored

6. Backup Process

6.1. The backup process for the File Servers

- Copy of data to RVN00-BACKUP

At 19:00 each day data from the user, workgroup and profile shares from RVN00-FILE01, RVN00-FILE02, RVN00-IMT01 and RVN00-INF01 are robocopied to \\RVN00-BACKUP\F$\ (scripts held on RVN00-BACKUP). These jobs are usually complete by 02:00.

- Backup to disk

RVN00-BACKUP takes a full weekly backup to disk that runs each Sunday at 05:00. The retention for this weekly backup is four weeks. A differential backup is then run Monday to Saturday at 05:00 each morning for the data held on RVN00-BACKUP\F$.

- Monthly Backup

There is also a monthly backup that runs at 05:00 on the 1st of each month. Retention of the backup is 6 months.

.

6.2. The backup process for the RVN00-MHISNEW

- Real time Oracle replication to RVN00-MHISDR

- Backup to disk

RVN00-BACKUP takes a full weekly backup to disk that runs each Sunday at 02:00. The retention for this weekly backup is four weeks. A differential backup is then run Monday to Saturday at 02:00 from the data held on RVN00-MHIS (using Backup Exec Agents)

- Monthly Backup

There is also a monthly backup that runs at 02:00 on the 1st of each month. Retention of the backup is 6 months.

6.3. The backup process for the eFin

- Copy of data to RVN00-DR-EFIN-DB

eFinance Exports
At 20:30 a scheduled task runs on rvn-efin-db which backs up the database
This takes 9 minutes

At 23:00 a scheduled task runs on rvn-efin-db-dr which copies the backup files offsite
source=\\rvn-efin-db\e$\exports
dest=\\rvn-efin-db-dr\e$\exports
This takes 20 minutes

eFinance RMAN
At 22:30 a scheduled task runs on rvn-efin-db which backs up the database
This takes 2 minutes

At 23:00 a scheduled task runs on rvn-efin-db-dr which copies the backup files offsite
source=\\rvn-efin-db\e$\backup
dest=\\rvn-efin-db-dr\e$\backup
This takes 5 minutes

- Backup to disk

RVN00-BACKUP takes a full weekly backup to disk that runs each Sunday at 3:00. The retention for this weekly backup is two weeks. A differential backup is then run Monday to Saturday at 12:00 from the data held on RVN00-DR-EFIN-DB.

- Monthly Backup

There is also a monthly backup that runs at 03:00 on the 1st of each month. Retention of the backup is 6 months.

6.4. The backup process for the Exchange

- Backup to disk

RVN00-BACKUP takes a full weekly backup to disk that runs each Saturday at 23:00. The retention for this weekly backup is two weeks. No differential backups are taken of this system

- Monthly Backup

No monthly backups are taken of this system

6.5. The backup process for the Enterprise Vault

- Backup to disk

RVN00-BACKUP takes a full weekly backup to disk that runs each Sunday at 23:00. The retention for this weekly backup is two weeks.
No differential backups are taken of this system

- Monthly Backup

No monthly backups are taken of this system

6.6. The backup process for the other application servers

- Copy of data to RVN00-DR01

Starting at 23:00 each day data from each application server is robocopied to \\RVN00-DR01 (scripts held on RVN00-DR01).

- Backup to disk

RVN00-BACKUP takes a full weekly backup to disk that runs each Sunday at 06:00 in the morning. The retention for this weekly backup is two weeks. A differential backup is then run Monday to Saturday at 06:00 each morning for the data held on RVN00-BACKUP.

- Monthly Backup

There is also a monthly backup that runs at 06:00 on the 1st of each month. Retention of the backup is 6 months.

The full list of servers and details can be found in Appendix A with associated process diagrams in appendix C

7. Restore Process

The Trust offers an ad hoc recovery services to it's users for files located on RVN00-FILE01 and RVN00-FILE02 on request via the IT Helpdesk.

All other data restores are solely for system failure, system migration or disaster recovery purposes and are managed by the IT operation team. The exact restore process for the all servers are provided in each systems IT documentation.

8. Install Process

The installation process described in the system documentation for the appropriate DR servers and RVN00-BACKUP

9. Business Continuity Process

In the event of a disaster with the backup server or archive SAN the plan is to purchase and rebuild the effected equipment. As such the backup system would not be available or would operate at an impaired level until that would could be completed

10. Regular Work

At present the regular work that takes place relating to the backup process is :-

- Checking Robocopy jobs have completed for all backup jobs – manual daily task
- Checking Timestamps on oracle RMAN backups (MHIS & eFIN) – manual daily task
- Checking backup exec jobs have completed for all backup jobs – emailed daily report
- Monitoring capacity usage – weekly

11. Interfaces

None except for the interaction with the data sources

Systems management and alerting is provided buy Microsoft Operations Manager on RVN00-BACKUP and email alerts from the MD3000s.

12. Risk Assessment Plan

12.1. Threats

The following threats have been identified and are applicable to the Backup process

Threat Type	Threat
Environmental	Either CER unavailable Either CER power failure Network link failure Theft of backup hardware
Equipment	UPS failure PSU failure Hardware failure Disk failure Software failure Network failure
System Security	Configuration error Unauthorised access to files Operating system vulnerability Application vulnerability Data Corruption

12.2. Risk Assessment Results

The table below details the results of the risk assessment. Using the following ratings the threat impact is assessed along with the probability and any control measures currently in place to determine the risk rating. The impact rating ranges from 1 – 5 with 1 having the least impact and 5 being catastrophic. The probability rating is the probability that the threat occurring again ranging from levels 1 – 5. Once the threats have been assessed then any controls currently in place are evaluated before determining the level of risk that remains.

Impact Rating
1 = None 2 = Minor 3 = Serious 4 = Major 5 = Catastrophic

Probability
1 = Rare 2 = Unlikely 3 = Moderate 4 = Likely 5 = Almost Certain

12.3. Risk Rating

Ref	Threat	Impact Analysis	Impact	Probability	Controls In Place	Risk
1.1	Callington Road CER unavailable due to environmental event.	Loss of system availability for an extended period of time (>48 hours).	Major	Rare	Move or re-provide DR & Backup systems at Blackberry Hill	4
1.2	Callington Road CER power failure.	Temporary loss of system availability (<24 hours).	Minor	Unlikely	UPS + generator.	4
1.3	Network link Failure	Temporary loss of system availability (<24 hours).	Moderate	Rare	Repair of link covered under the contract with link supplier. Ability to reconfigure backups to ensure MHIS, files and Efin backups are maintained using the backup link to Callington road	3
1.3	Theft of backup hardware	Loss of system availability for an extended period of time (>48 hours).	Moderate	Rare	Backups facilities located in secure area of Callington road with 24hr security on site	3
2.1	System hardware failure.	Temporary loss of system availability (<24 hours).	Minor	Unlikely	Replacement hardware available under support contract.	4
2.2	Disk failure.	Temporary loss of system availability (<24 hours).	Minor	Possible	Redundant disk in RAID 5 configuration.	6
2.3	PSU failure.	Temporary loss of system availability (<24 hours).	Minor	Unlikely	Redundant power supplies.	4
2.4	Network switch failure	Network monitoring information unavailable.	Minor	Unlikely	Spare network switch available.	4
2.5	Software failure	Temporary loss of system availability (<24 hours).	Minor	Possible	Daily backup of application configuration.	6
3.1	System configuration error.	Disruption to File Servers. Loss of File Servers at Bath.	Major	Likely	User access restrictions in place.	16

3.2	Unauthorised access to files.	Data confidentiality risk / malicious deletions of files.	Moderate	Unlikely	OS permissions.	6
3.3	Operating system vulnerability.	AWP network integrity affected could lead to compromise of File Servers.	Major	Almost Certain	No external access from AWP network limits attack potential.	20
3.4	Application vulnerability.	AWP network integrity affected could lead to compromise of File Servers..	Major	Likely	No external access from AWP network limits attack potential.	16
3.4	Data Corruption.	Problems with the hardware, software or backup media could result in the backups not being an accurate copy of the source data	Moderate	Rare	Error checking hardware and verification of backups	3

13. Data Protection / Confidentiality Assessment

Data Protection for the File Servers is controlled via the NTFS permissions in place, along with the use of a product named Safend which controls the use USB/CD writing. No data is allowed to be written to USB devices unless they are Trust approved memory sticks (which are all encrypted).

All Servers are in Central Equipment Room at Callington Road Hospital. The CER is located in a restricted access area and which is covered by 24hr manned security.

DR & Backups copies between Bath NHS House and Callignton Road are perform over AWP controlled kit and dedicated point to point fibre optic links thus limiting access from third parties while in transit.

14. Support and Remote Access

Support for the Servers and SAN are on Dell Gold Support – which is a four hour fix time. During the investigation stage Dell use the 'gotoassist' application – a web based system which allows them to control your desktop and as such view remote desktop connections on Servers.

Access to AWP systems is by invitation only and is monitored while in use

15. Capacity Planning

The backup archive was originally specified to provide 21TB (~16TB usable) of storage and can be grown by adding additional disks to 90TB (~50TB usable).

As of December 2008 usage was approaching 8.5TB (53%) which based on current usage and growth of

66% of total at 22% per year for File01, File02, IMT01 and INF01
23% of total at 45% per year for Email
6% of total at 100% per year for MHIS
4% of total at 50% per year for Other servers

gives 26 months until we need to expand the storage capacity of the unit and 62 months until we reach maximum capacity.

The MHIS and Exchange account for about 27% of current usage so migration to RiO and NHSmail within a 18 month period will offset this growth rate and extend the usage life to 55 months until we need to expand the storage capacity.

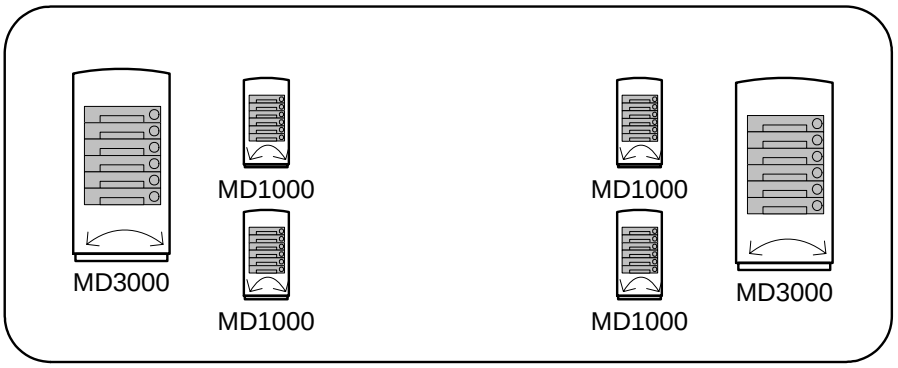
These figures are based on current usage and the growth rates show. Additional systems, changes in utilisation patterns or new storage requirements will required these figures to be adjusted accordingly.

APPENDIX A – Backup Schedule

\\rvn00-imt01\Workgroups\IMT Technology\Operations\Servers\Backups\backups.xls

APPENDIX B – MD3000 Configuration

Storage



Backup Array 1

Backup01 – 7.2Tb

5 x Full Monthly Backups File Server (6TB)

Backup02 – 7.2Tb

4 x Weekly File Servers (5TB)
MHIS Differentials (700Gb)
EFIN Differentials (100Gb)
Other Differentials (300Gb)

Backup Array 2

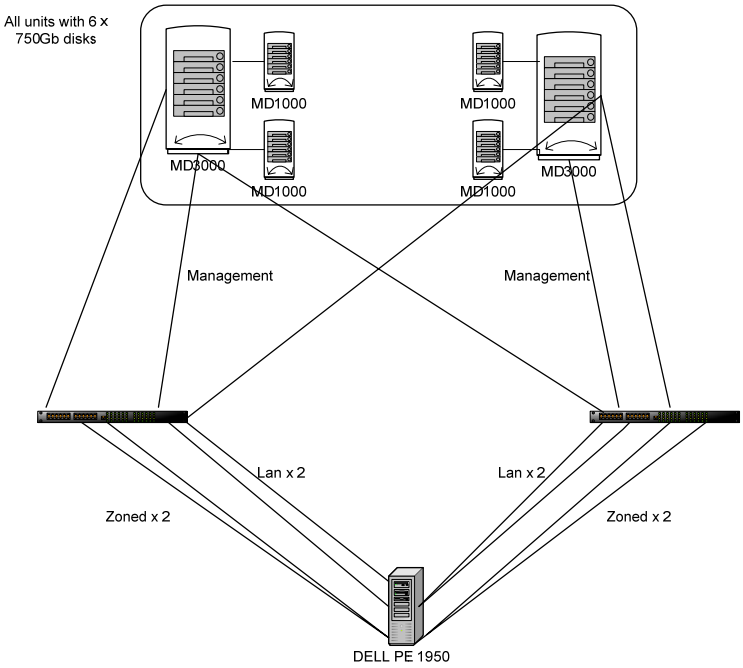
Backup03 – 7.2Tb

File Server Differentials (250Gb)
Exchange Full x 2 (3Tb)
4 x Weekly MHIS Full (1Tb)
5 x Full Monthly Backups EFIN (200Gb)
5 x Other Monthly Backups (1.5Gb)

Backup04 – 7.2Tb

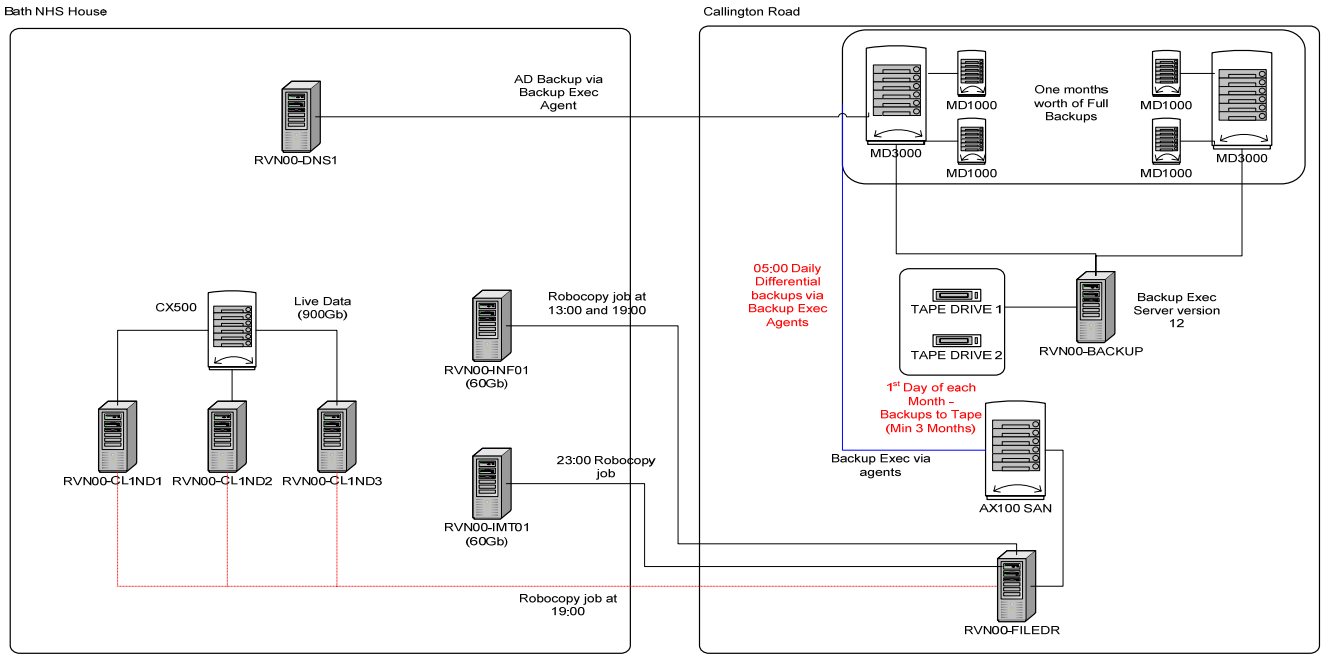
5 x Full Monthly MHIS (2TB)
4 x Weekly Efin (160Gb)
4 x Other Weekly Backups (1.2Tb)
2 x Enterprise Vault Backup (200Gb)

Switch Config

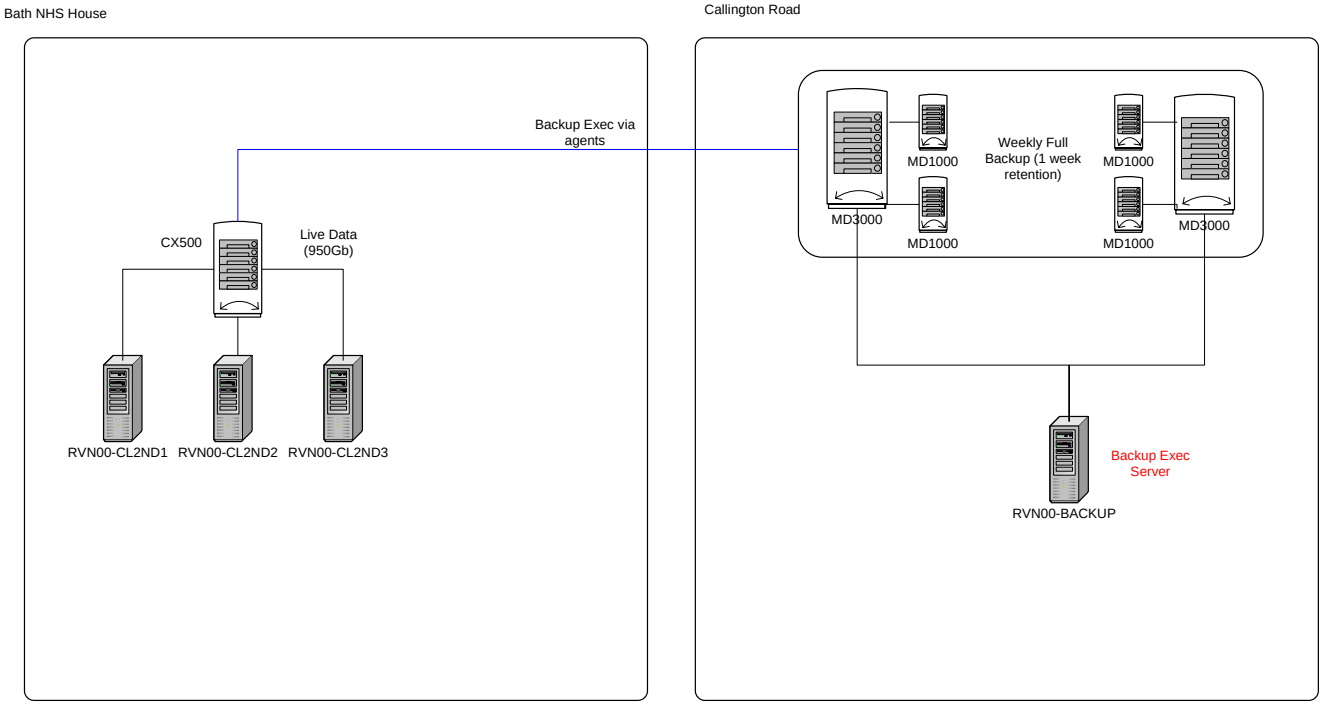


APPENDIX B – Backup Processes

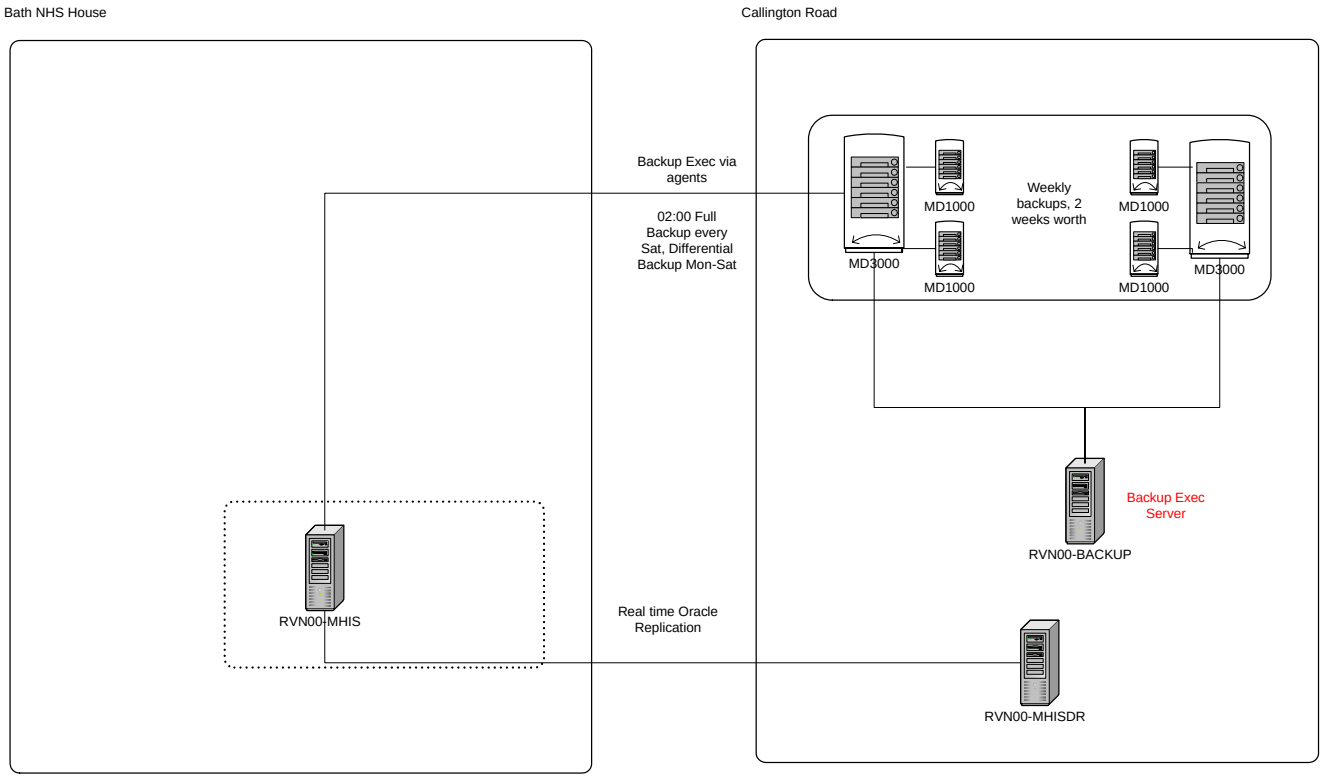
File Servers Backup



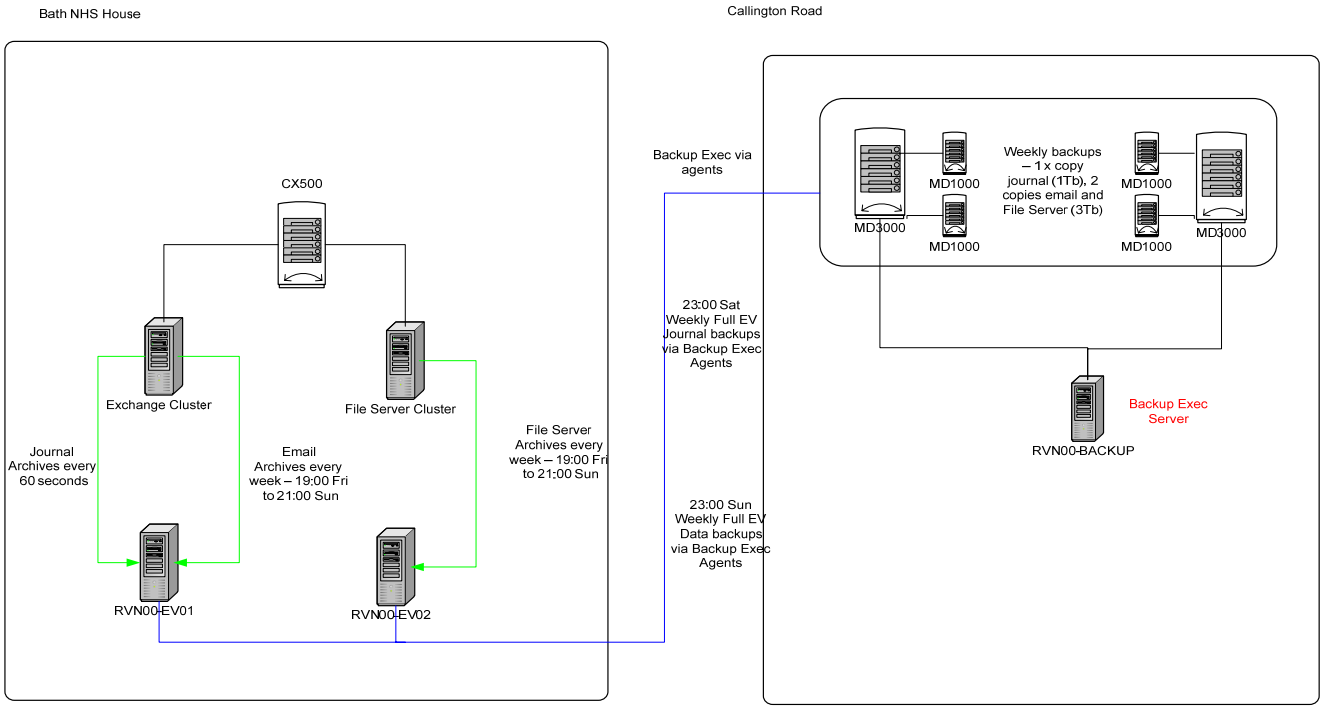
Exchange Backup



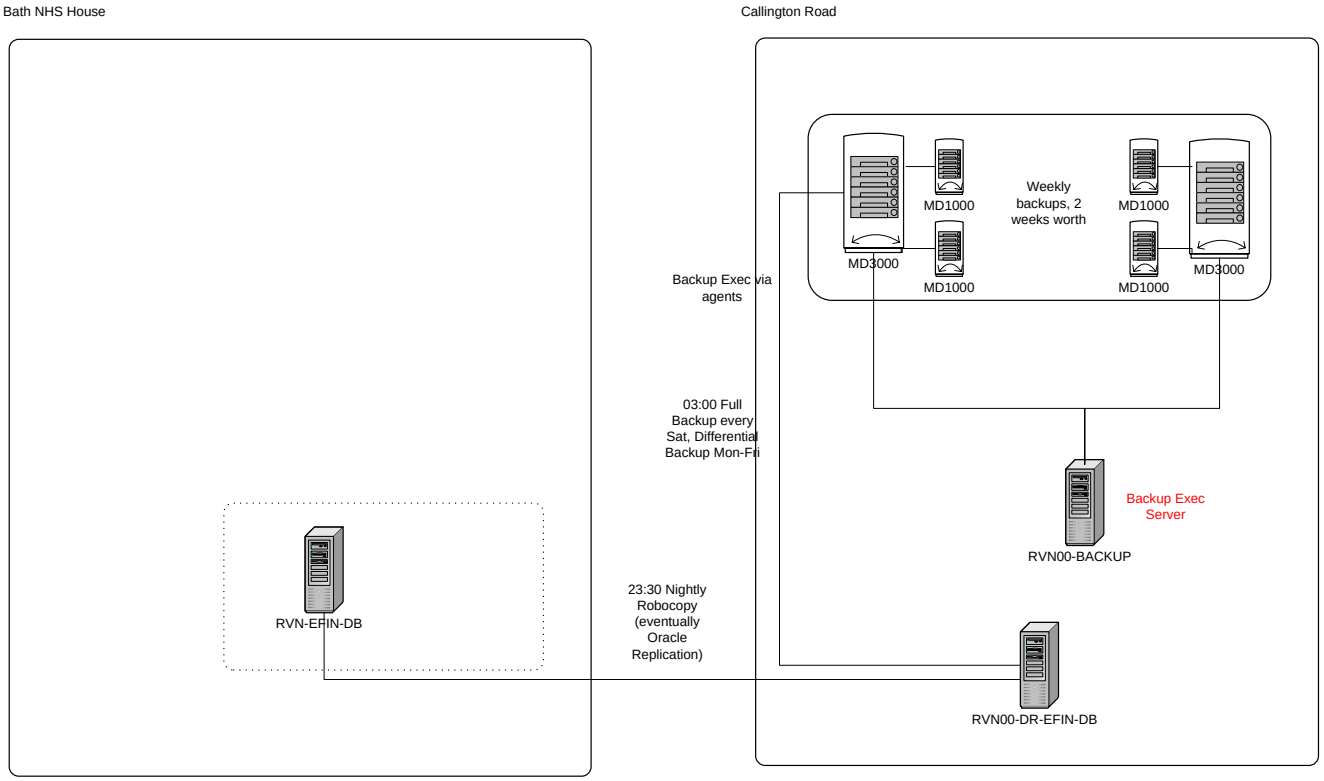
MHIS Backup



Enterprise Vault



Efin Backup



Other Servers Backup