iMedConsent
by Dialog Medical

Disaster Recovery Plan

Technical Guide

Version: 2007.11.15

Support ID: I38-4xx-000

Table of Contents

Introduction

This document serves as a guide for setting up the proper backup procedures, testing a recovery plan, and migrating iMedConsent™ to a new server. This document refers to server in generic terms as a system that can run iMedConsent™. The system can be shared and is not recommended. A dedicated or virtual server is recommended instead.

Server Requirements

The following are requirements for the iMedConsent™ server. This is not the same as requirements for Terminal Servers that run iMedConsent™ for application sharing.

- Windows Server 2003 or 2003 R2 with latest service pack
  - Standard, Enterprise, or Data Center Editions
  - as of this writing, SP2 has been tested
  - x86 fully tested and support; x64 not tested
- Modern P4/Xeon or later processor
- 2 GB RAM or more
- 120 GB HD or more, preferably with redundancy (RAID)
- 2 partitions formatted NTFS as C: and D:
- Microsoft SQL Server 2000 or 2005 with latest service pack
  - Any Edition will work
  - MSSQL 2000 SP4 tested
  - MSSQL 2005 SP2 tested
  - Clustering is a supported configuration however Dialog Medical support cannot assist in maintaining or configuring the cluster itself, only the data within working instances.

Backup Resources and Frequencies

The following resources must be properly backed up for a complete system restore. Recommended frequencies are also listed. For a general guidance on how to perform backups with the standard installed tools, see Appendix A.

- File System
  - C:\dataSummaryService\
  - C:\documentService\
    - If you **do not** have an Open File agent, skip the following files:
      - C:\documentService\trace.log
      - C:\documentService\emrRun\X
      - C:\documentService\DocToImg\X
  - C:\iMedInstall\
  - D:\DocumentStore\
    - If you **do not** have an Open File agent for your backup software, please skip this directory but be sure to regularly fix documents in error or those documents will be lost on a disk failure.
  - D:\iMedConsent\
  - SKIP D:\SQL Data\ and D:\SQLData as the database is actively using those folders. Use SQL Server Tools or a backup agent specifically designed for backing up Microsoft SQL Server databases.
- Database
  - iMed37
    - Main iMedConsent™ database
    - Transaction Log backup daily, Full backup weekly
  - iMedAudit
    - Contains auditing information for document tracking
    - Transaction Log backup daily, Full backup weekly
  - UpdateHistory
    - Patch system and required for upkeep
    - Transaction Log backup daily, Full backup weekly

Backup Recommendations

These are helpful notes from other IT Administrators:

1. Make sure to backup files to a different system as a hardware failure may wipe out your system and your backups.
2. Test your Backup and Recovery steps each year. For non-production restores, use a Virtual PC in a segmented or local-only network environment. A second Virtual PC can be used as a client to connect to your recovered system for testing. Microsoft Virtual PC is free at: http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx (click here for a direct download to VPC 2007)

Restore or Migration Setup Prerequisites

The following steps must be completed for a server restore.

1. Verify that you have the latest iMedInstall files for use by this process. During the rollout of iMedConsent™ servers, we had three revisions in the Server Installer files. To verify that you have the latest, look for the file D:\iMedConsent\iMed37\Install\DocumentServer\install.bat. If the file exists, continue to step 2.
    a. To update an older Server Install to the latest revision, download the files:
        i. http://www.dialogmedical.com/downloads/support/va/drp/DataSummary_3_80_2007_04_18.zip
        ii. http://www.dialogmedical.com/downloads/support/va/drp/DocumentServer_3_80_2005_01_05.zip
    b. Rename the existing DataSummary and DocumentServer folders to something else if they already exist. We recommend adding ".old" to the end of the folder name or moving them to a completely different root folder.
    c. Unzip the contents of these files to D:\iMedConsent\iMed37\Install\
    d. Verify that your folder structure looks like this:

        - D:\iMedConsent\iMed37\Install\
            - DataSummary\
                - Backup\
                - SDClean\
            - DocumentService\
                - files\

2. If you need or have pre-scheduled assistance with Dialog Medical Support, please make sure the server is accessible via the VA's VPN and that the proper Dialog Medical AD accounts are added to the local Administrator's group.

Restore Guide for Full Recovery

The following steps are for recovery to a server from backup files. The process is separated into three phases: files, database, and services.

1. Files
    a. Restore the same directory structures you originally backed up:
        i. C:\dataSummaryService\
        ii. C:\documentService\
        iii. C:\iMedInstall\
        iv. D:\DocumentStore\
        v. D:\iMedConsent\
    b. Don't worry about file shares just yet, that'll be done in step 3.
2. Database
    a. Using your database recovery tools, restore the following databases:
        i. iMed37
        ii. iMedAudit
        iii. UpdateHistory
    b. Depending on the configuration and environment, you may need to reset security rights.
        i. Remove the Domain Users "user" from underneath Security at the server instance level.
        ii. Add back in the Domain Users "user".
        iii. Add that user to each database and check the "public" role.
3. Services
    a. Run D:\iMedConsent\iMed37\Install\DocumentServer\install.bat
        i. Install.bat will:
            1. Create shares
            2. Install the iMedConsent™ Document Service
            3. Install the printer for converting documents to images
            4. Create the encryption hash for decrypting documents sent from clients to the server's dropBox for processing.
    b. Run D:\iMedConsent\iMed37\Install\DataSummary\installServerX.bat where X is 1, 2 and then 3.
    c. Set Images$ share permissions (D:\DocumentStare\imagingShare\) to VHAxxxIA, VHAxxxIU, and local SYSTEM, all = Full Control (where 'xxx' = three-letter site designation)
        i. The users VHAxxxIA and VHAxxxIU allow the VistA Imaging Background Processor to access the images remotely.

ii. The user SYSTEM is used by the service to check that the files are accessible via the share before sending the request to the VI Background Processor.

d. Run D:\iMedConsent\iMed37\Install\DocumentServer\setup.exe

Restore Guide for Server Migration

The following steps are for migrating from an old server to a new server while both systems are up and running (hot). Some of these steps will send you to other sections where needed.

For the purposes of this documentation, the existing iMedConsent™ server will be called SERVER_OLD and the new server is, you guessed it, SERVER_NEW.

1. From SERVER_NEW, map to \\SERVER_OLD\c$ and \\SERVER_OLD\d$ using IP addresses instead of computer names.
2. Copy \\SERVER_OLD\d$\iMedInstall to SERVER_NEW's D: drive.
3. Instead of pulling files and databases from backup, you can copy the proper folders and their contents from SERVER_OLD to SERVER_NEW.
    a. Since we're transferring files and data from one system to another, you'll want to have everyone exit iMedConsent™. To stop processing jobs in the background, stop the service "iMedConsent Document Service".
    b. Following the steps in the section Restore Guide for Full Recovery, you'll want to copy the files, backup/restore the database, and reinstall the services.
        i. If using detach/attach to move the SQL Server databases, stop the SQL Server services before copying the database MDF/LDF files to the new server.
        ii. We still recommend using backup/restore to test the migration in advance while the main production server can continue to run.
    c. You may want to clear out old log files from the following folders to speed along the file copy process.
        i. C:\documentService
        ii. C:\dataSummaryService
    d. You may also want to move the contents of the following folders to another local directory to speed along the file copy process. You can move these files over later or leave them off to the side for 30 days or until needed.
        i. D:\DocumentStore\clientLogs
        ii. D:\DocumentStore\imagingShare
        iii. D:\DocumentStore\storeToPurge
4. Continue to execute the batch files in step 3 of the section Restore Guide for Full Recovery.
5. After SERVER_NEW has been restored, we will transfer the old server's computer name to the new server.

a. Remove SERVER_OLD from the domain
b. Rename SERVER_OLD to SERVER_SOMETHING_ELSE (not SERVER_NEW)
c. Rename SERVER_NEW to SERVER_OLD, leaving the IPs the same so that our two servers don't have an IP conflict.
d. If SERVER_NEW (now named SERVER_OLD) isn't already on the domain, add it now.
e. You can optionally add SERVER_OLD (now named SERVER_SOMETHING_ELSE) back to the domain if needed.

Restore Guide for Live Server Migration

If time is of the essence, following these changes to the section Restore Guide for Server Migration. These steps will allow you to copy a bulk of the files, install all the services, and practice the database restore steps in advance of the real switch.

1. Complete steps 1-4 from the section Restore Guide for Server Migration.
2. Stop and wait for the real migration. Continue with this section if there's a small gap of time between this step and the next. An iMedConsent™ patch must **not** have run between these two steps or have any configuration changes made to the system itself by Dialog Medical Support.
3. Copy changed files:
    a. D:\iMedConsent\iMed37\Content\UserDocs
    b. D:\DocumentStore\
        i. This assumes jobs have been processed that are in error or still pending.
4. Backup and restore the databases.
5. Continue with step 5 in the section Restore Guide for Server Migration to give SERVER_NEW the old computer name.

Appendix A: Performing Backups

1. File backup:
    a. How To Use the Backup Wizard for Backup Jobs in Windows 2000 (which is still valid in Windows Server 2003) at http://support.microsoft.com/kb/300135
2. Database backup in SQL Server 2000:
    a. Explanation of the Database Maintenance Plan Wizard: http://technet.microsoft.com/en-us/library/aa933075(SQL.80).aspx
    b. Unfortunately, the documentation for SQL Server 2000 is lacking in direct guidance on using the Database Maintenance Plan Wizard to create a proper backup schedule.
        i. Fortunately, the Microsoft® Identity Integration Server 2003 also uses a SQL Server 2000 database and they have guidance here: Scheduling Full Database Backups by Using the Database Maintenance Plan Wizard
        ii. Note, documentation for MIIS notes transaction log backups at every 4 hours. That frequency is not required for iMedConsent™ and you can do daily transaction log backups instead.
        iii. Note, documentation for MIIS on step 5 asks you to select the database MicrosoftIdentityIntegrationServer which works well if you have MIIS installed. Since this is for iMedConsent™, select the databases listed in the section Backup Resources and Frequencies.
    c. In-depth Backup and Restore documentation: SQL Server 2000 Backup and Restore
3. Database backup in SQL Server 2005:
    a. One-time and straight forward backup: How to: Back Up a Database (SQL Server Management Studio)
    b. Creating a maintenance plan for scheduled backups: How to: Create a Maintenance Plan
    c. In-depth Backup and Restore documentation: Introduction to Backup and Restore Strategies in SQL Server

Appendix B: Server name locations

In the event that your server computer name changes, you'll need to make changes in two phases.

1. Once the server roles have transferred to a new server, change the SERVERNAME in the following locations:
    a. C:\documentService\bin\documentservice.exe.config
    b. C:\documentService\bin\jobMonitor\jobmonitor.exe.config
    c. D:\iMedConsent\iMed37\Install\jobMonitor\jobmonitor.exe.config
    d. D:\iMedConsent\iMed37\Install\Workstation\ccow_install.bat
    e. D:\iMedConsent\iMed37\Install\Workstation\epad_install.bat
    f. D:\iMedConsent\iMed37\Install\Workstation\iMedConsent\program files\Dialog Medical\iMedConsent VA\updater.ini
    g. D:\iMedConsent\iMed37\Admin\acleditor.ini
    h. D:\iMedConsent\iMed37\Admin\dialog.ini
    i. D:\iMedConsent\iMed37\Content\dialogsql.udl
    j. D:\iMedConsent\iMed37\Program\dialog.ini
    k. D:\iMedConsent\iMed37\Program\updater.ini
2. All client workstations will have their dialog.ini and updater.ini still pointing to the old server. You will need to configure the old server's D:\iMedConsent\iMed37\Program\dialog.ini and updater.ini to the new server's name so that clients will update themselves on startup. The process is:
    a. Existing client has a dialog.ini and updater.ini pointed to SERVER_OLD.
    b. Client starts Updater2.exe which opens up the current updater.ini (still pointing to SERVER_OLD).
    c. Updater2.exe downloads any changed files from SERVER_OLD including the new dialog.ini and updater.ini. These files point to the new server.
    d. Updater2.exe launches dialog.exe which loads the newly refreshed dialog.ini that now points to SERVER_NEW.
    e. On the next execution of Updater2.exe, it loads the newly refreshed updater.ini and will check for file changes from SERVER_NEW.