

FIM Disaster Recovery Planning

<CUSTOMER NAME>

Thursday, 29 October 2015

Version 0.1 Draft

Prepared by

Peter Geelen

Premier Field Engineer - Security & Identity

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change reference |
| 05/05/2015 | Peter Geelen | 0.1 | Initial Document |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 General 1](#_Toc418605636)

[1.1 DRP 1](#_Toc418605637)

[1.2 SQL 1](#_Toc418605638)

[2 Backup 2](#_Toc418605639)

[2.1 VM System Snapshot/Backup 2](#_Toc418605640)

[2.1.1 Advantage 2](#_Toc418605641)

[2.1.2 Disadvantage 2](#_Toc418605642)

[2.1.3 Known issues with Snapshots 2](#_Toc418605643)

[1. Known issues with Snapshots 2](#_Toc418605644)

[2.2 Windows Backup 2](#_Toc418605645)

[2.2.1 Advantage 2](#_Toc418605646)

[2. Entire machine backup 2](#_Toc418605647)

[2.2.2 Disadvantage 3](#_Toc418605648)

[2.3 Backup FIM Synchronization server 3](#_Toc418605649)

[2.3.1 FIM Sync Database 3](#_Toc418605650)

[2.3.2 FIM Sync encryption key 4](#_Toc418605651)

[2.3.3 FIM Sync registry 4](#_Toc418605652)

[2.3.4 Source Code 4](#_Toc418605653)

[2.3.5 Log files 4](#_Toc418605654)

[2.3.6 Configuration files 4](#_Toc418605655)

[2.3.7 Scripts 5](#_Toc418605656)

[2.3.8 Folder: MAData (Filebased MAs) 5](#_Toc418605657)

[2.3.9 Software setup files 5](#_Toc418605658)

[2.3.10 FIM Sync server configuration export 5](#_Toc418605659)

[2.3.11 Backup Task scheduler configuration 6](#_Toc418605660)

[2.3.12 Backup 3rd party clients & tools configuration 6](#_Toc418605661)

[2.3.13 PCNS 6](#_Toc418605662)

[2.3.14 Non-FIM components (OS, ...) 7](#_Toc418605663)

[2.4 Backup FIM Service 7](#_Toc418605664)

[2.4.1 FIM Service export 7](#_Toc418605665)

[2.4.2 FIM Service Database 8](#_Toc418605666)

[2.4.3 Backup FIM Service Config file 8](#_Toc418605667)

[2.4.4 Registry 8](#_Toc418605668)

[2.4.5 SQL Agent Jobs 9](#_Toc418605669)

[2.4.6 Tools 9](#_Toc418605670)

[2.5 Backup FIM Portal 9](#_Toc418605671)

[2.6 Tools 9](#_Toc418605672)

[2.7 Backup FIM Reporting 9](#_Toc418605673)

[2.7.1 Databases 9](#_Toc418605674)

[2.8 SCSM 10](#_Toc418605675)

[2.9 Backup BHOLD 10](#_Toc418605676)

[2.10 Backup FIM CM 10](#_Toc418605677)

[2.11 Backup Documentation 11](#_Toc418605678)

[2.12 Backup External Source & Target data 11](#_Toc418605679)

[2.13 Schedule Backup 12](#_Toc418605680)

[2.13.1 Configuration components 12](#_Toc418605681)

[2.13.2 Suggested backup schedule (Manual) 12](#_Toc418605682)

[2.14 Data components 12](#_Toc418605683)

[2.14.1 Suggested backup schedule (automated) 12](#_Toc418605684)

[3 Failover FIM Synchronization 13](#_Toc418605685)

[3.1 Failover - Warm-standby 13](#_Toc418605686)

[3.2 Failover - Cold standby 13](#_Toc418605687)

[4 Server recovery 14](#_Toc418605688)

[4.1 Full system recovery 14](#_Toc418605689)

[4.2 FIM Server reinstallation 14](#_Toc418605690)

[4.3 FIM Server Refresh (repair installation) 14](#_Toc418605691)

[4.4 Partial / component recovery 15](#_Toc418605692)

[4.4.1 FIM Sync Server 15](#_Toc418605693)

[4.4.2 External data source 17](#_Toc418605694)

[4.5 FIM Service Recovery 17](#_Toc418605695)

[4.5.1 Database restore 17](#_Toc418605696)

[4.5.2 Repair install with existing database 18](#_Toc418605697)

[5 Planning 19](#_Toc418605698)

[5.1 Review 19](#_Toc418605699)

[6 Crisis communication 20](#_Toc418605700)

[7 See also 21](#_Toc418605701)

[8 References 22](#_Toc418605702)

[8.1 FIM 22](#_Toc418605703)

[8.2 SQL 22](#_Toc418605704)

[9 Downloads 23](#_Toc418605705)

[10 Additional Resources 24](#_Toc418605706)

[11 Glossary, abbreviations & acronyms 25](#_Toc418605707)

1. General
   1. DRP

* A DRP plan must provide methods to recover different situations and scenarios
  + its required to include multiple backup methods, as each method is to be used in different situations
  + Do not rely on a single method, eg. 'system wide' backups only, as these have important disadvantages
* Whatever (combination of) method(s) you choose to backup your configuration, the value of your backup is only guaranteed if you are able to restore it.
* DRP (Disaster Recovery Planning) is only valid if you have tested it thoroughly, this includes
  + testing backup
  + restoring backups
  + executing bare metal restoration
* In case of disaster, you don't want to spend time on considering which option is the best
  + Make sure the DRP planning and execution is documented in detail
  + Describe which methods to use in which case
* DRP should not depend on the skills of the FIM admins only
  + Make sure you can execute the recovery blindly
  + Make sure that server admins with limited FIM skills can execute the DR
* DRP planning must be reviewed on a regular basis (yearly)
  1. SQL
* Carefully verify the SQL backups, as the the backups in SQL have double functionality
  + Backup data
  + Optimize logs, truncate logs to minimize use of space
* Make sure to have the proper maintenance plans for your FIM databases
  + Keep fragmentation under control (eg the FIM Sync database has the tendency to fragment...)

|  |
| --- |
| http://social.technet.microsoft.com/wiki/resized-image.ashx/__size/550x0/__key/CommunityServer-Wikis-Components-Files/00-00-00-00-05/1731.Note.gifNote |
| The core reference for database maintenance is <https://ola.hallengren.com/> |

1. Backup

This applies to any server on which FIM components are installed.

* 1. VM System Snapshot/Backup

Lots of environments run their servers on a virtualized machines, most of these VM systems allow to snapshot the guest system.

* + 1. Advantage
* Entire machine backup
* Fast method to take a snapshot of a working machine
* Quick method to safe the system state just before or just after configuration changes
  + 1. Disadvantage
* Snapshots cannot be used for long term storage (as you will run into issues with AD thumbstone when you restore an old machine account)
* If the snapshot contains corruption of configuration issues, it's very hard to recover the system
* It's mostly an all-in-one recovery (no single component recovery)
  + 1. Known issues with Snapshots
* <http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1007576>
* <http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2006849>
* <https://communities.vmware.com/message/1753988>
  1. Windows Backup
     1. Advantage

1. Entire machine backup
2. Allows for bare metal restore
3. Quick method to safe the system state just before or just after configuration changes
   * 1. Disadvantage

* This method usually takes some time to restore
* Snapshots cannot be used for long term storage (as you will run into issues with AD thumbstone when you restore an old machine account)
* If the snapshot contains corruption of configuration issues, it's very hard to recover the system
* It's mostly an all-in-one recovery (no single component recovery) 
  1. Backup FIM Synchronization server

More details at: [MIIS/ILM/FIM: How to Backup the Synchronization Engine](http://social.technet.microsoft.com/wiki/contents/articles/1764.miisilmfim-how-to-backup-the-synchronization-engine.aspx)

* + 1. FIM Sync Database

The FIMSynchronisationService database is hosted on SQL.

Make sure you have a regular backup of your database using the SQL Management tools.

It seems obvious, but also perform a restore once in a while. (Doing is the best practice!)

#### Advantage

* Contains all identity data and configuration items you configure in the GUI
* Contains most configuration data (eg files in Extensions directory), but not all files (like service config files, 3rd party client setup & config, source code ...)

#### Disadvantage

* Does NOT contain all configuration items
* Not able to restore partial configuration or single components
* If database is corrupt, this method is not valid
* Requires Encryption key to reinstall FIM on same DB, move DB, failover to standby...

#### Recommendation

* Do NOT rely on DB backup only, you must combine it with other backup methods (like configuration export)
  + 1. FIM Sync encryption key

When you install FIM, a tool MIISkmu.exe is installed with it, and available in the Programs > Microsoft Identity Integration Server menu.

#### Recommendation

* Take a backup (export) of the key regularly (eg before/after an hotfix, upgrade,...)
  + 1. FIM Sync registry

The following registry keys under the path

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\FIMSynchronizationService]:

* Logging
* ManagementAgents
* Parameters
* Performance
  + 1. Source Code

Safeguard the source files of the extensions you created and compiled.

This allows you to recompile the extensions if needed.

Before you start editing and recompiling the extensions, make a backup of the source.

* + 1. Log files

In some opinions maybe less critical, but certainly useful.

* + 1. Configuration files

Some extensions (like logging, GAL,…) use config files to read data.

Also the task scheduler or MASequencer configuration files, if applicable…

FYI: The FIM Sync Extensions directory is backed up into a Microsoft SQL Server table in the FIM Sync database, and the XML files are restored during the FIM Syncactivate process…

* + 1. Scripts

The scripts, commands and batch file you use to automate FIM Sync operations.

* + 1. Folder: MAData (Filebased MAs)

(Cfr. [FIM Sync Design and Planning collection](http://www.microsoft.com/downloads/details.aspx?FamilyId=DADC5021-222B-4AF7-8C58-2227C358756F&displaylang=en))

File-based management agent import and export files that are located in FIM Sync installation path\MAData

* + 1. Software setup files

And it’s always handy to make sure you have the software available you used to prepare your FIM Sync server.

Not only the FIM install files, but also the FIM Sync Resource Took Kit files, Visual Studio, SQL server and other tools you used for configuration, troubleshooting and other operations…

In general, make sure your backups are stored safely (and better at safe distance).

* + 1. FIM Sync server configuration export

Using the FIM Sync GUI (Identity Manager) you can export

* The entire [FIM Sync server](http://technet.microsoft.com/en-us/library/jj590321(v=ws.10).aspx) configuration (Menu File > Export Server Configuration)
* The MA configuration (export management agent, one by one)
* the MV configuration (Metaverse Designer > Export metaverse)

Important notice:

When exporting the FIM Sync configuration,the export does NOT export the content of the connector spaces, nor the metaverse. Also the exensions associated with the MA and MV are not exported.

* + 1. Backup Task scheduler configuration

Independent the tool used to schedule you FIM Sync run profiles, make sure you have a backup of

* the Run scheduler scripts, configuration files, ...
* the schedule used (via backup or via proper documentation)
  + 1. Backup 3rd party clients & tools configuration

The configuration of the "non-FIM Sync"tools and clients

For some MA’s you need to configure a client or specific files, or specific network settings. You better make sure you’ve documented these settings or make a backup of this configuration part.

Let me explain: for example the configuration of the hosts file, the services file, system files that are customized to support clients like the Oracle or SAP client.

Other client specific configuration (names.orafile, ID files for Notes, …)

* + 1. PCNS

Although it might be difficult to "backup" the PCNS config. Documenting the setup and the procedures used is of important value.

* + 1. Non-FIM components (OS, ...)

Another part of non-FIM Sync backup is the OS, but I’ll suppose it’s sufficiently known how to backup Windows Server…

One way of backing up the system is a full system backup of your server.On server system level, virtualisation also offers a way of taking a snapshot of the server image.

But still this doesn’t cover the list if the FIM Sync data is distributed over more than one system (eg FIM Sync server with remote SQL).

Remark: be aware of the Microsoft support policy for systems in a virtualized environment ([here](http://support.microsoft.com/kb/897615/) and [here](http://support.microsoft.com/kb/897614))

* 1. Backup FIM Service

Partially taken from: [FIM Service Backup and Restore](http://technet.microsoft.com/en-us/library/fim-service-backup-and-restore-fim-2010-backup-and-restore-guide(v=ws.10).aspx)

* + 1. FIM Service export
* <http://blogs.msdn.com/b/bikwan/archive/2010/02/05/what-can-export-fimconfig-do-for-me.aspx>
* Configuration Migration Deployment Steps: <http://technet.microsoft.com/en-us/library/ff400277(v=ws.10).aspx>
* Export-FIMConfig: <http://technet.microsoft.com/en-us/library/ff394182.aspx>

Sample script

|  |
| --- |
| cls  If(@(get-pssnapin where-object {$\_.Name  "FIMAutomation"} ).count 0) {add-pssnapin FIMAutomation}  $targetdir = "C:\Backup\FIM Service Config\"  $URI = "http://localhost:5725/ResourceManagementService"    #export schema configuration  $export = Export-FIMConfig -uri $URI -schemaConfig  $targetfile = $targetdir + "schema.xml"  $export | ConvertFrom-FIMResource -file $targetfile    #export policy configuration  $export = Export-FIMConfig -uri $URI -policyConfig  $targetfile = $targetdir + "policy.xml"  $export | ConvertFrom-FIMResource -file $targetfile    #export portal configuration  $export = Export-FIMConfig -uri $URI -portalConfig  $targetfile = $targetdir + "portal.xml"  $export | ConvertFrom-FIMResource -file $targetfile |

* + 1. FIM Service Database

1. By default this database is called FIMService.
2. You do not have to stop the FIM Service when you create this backup.
3. If you added configuration data that was not included in the Setup process, you can also back up those items.
4. The FIM Service database is deployed in full recovery model by default. Using the full recovery model makes it possible to back up the log to provide incremental recovery points. See [Backup Under the Full Recovery Model](http://go.microsoft.com/fwlink/?LinkId=184025) (for more information.

See also: How to back up and restore the relevant SQL databases. For more information, see [Backup Overview (SQL Server)](http://go.microsoft.com/fwlink/?LinkId=184023) (<http://go.microsoft.com/fwlink/?LinkId=184023>).

* + 1. Backup FIM Service Config file

The FIM Service Configuration File, which is located at %programfiles%\Forefront Identity Manager\2010\Service\Microsoft.ResourceManagement.Service.exe.config.

* + 1. Registry

The following registry keys under the path:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\FIMService:

* DatabaseServer
* DatabaseName
* CertificateThumbpoint
* DefaultKeySize
* DefaultTokenLifetimeInMinutes
* ServiceAccountSid
* PollExchangeEnabled
  + 1. SQL Agent Jobs

SQL Server Agent Jobs:

* FIM\_DeleteExpiredSystemObjectsJob
* FIM\_MaintainGroupsjob
* FIM\_MaintainSetsJob
* FIM\_TemporalEventsJob

For detailed guidance, check TechNet [*FIM Service Backup and Restore*](http://technet.microsoft.com/en-us/library/fim-service-backup-and-restore-fim-2010-backup-and-restore-guide(v=ws.10).aspx)

* + 1. Tools
* [FIM 2010 R2 Service and Portal Configuration Backup Tool](http://technet.microsoft.com/en-us/library/jj134311(v=ws.10).aspx)
  1. Backup FIM Portal

See: [FIM Portal Backup and Restore](http://download.microsoft.com/download/E/1/6/E16D8C0D-0C51-45D1-8B60-27D48D54579E/FIM_Backup.doc)

* 1. Tools
* [FIM 2010 R2 Service and Portal Configuration Backup Tool](http://technet.microsoft.com/en-us/library/jj134311(v=ws.10).aspx)
  1. Backup FIM Reporting
     1. Databases

See: FIM 2010 R2 Reporting Disaster Recovery: <http://technet.microsoft.com/en-us/library/jj133846(v=ws.10).aspx>

* 1. SCSM

See: <http://technet.microsoft.com/en-us/library/jj133846(v=ws.10).aspx>

Best Practices for backing up the SCSM Management Server and Data Warehouse Server Databases

It is highly recommended that you follow the procedures outlined in the [System Center Service Manager 2010 SP1 Disaster Recovery Guide](http://technet.microsoft.com/en-us/library/ff625768.aspx). These procedures describe backing up the databases and the encryption key that is created when System Center is deployed. It also provides useful SQL scripts for capturing and preserving SQL Server logon and object level permissions information.

* 1. Backup Documentation

Document your setup in detail and keep it up to date.

Documentation should include:

* Project documentation (business requirement, business analysis & design)
* Technical architecture/design
* Technical implementation
* DTAP migration procedures
* FIM hotfix & upgrade procedures
* Disaster recovery planning
* Operational management procedures of FIM (maintenance tasks, task scheduling, ...)
* ...
  1. Backup External Source & Target data

An important piece of data that FIM Sync is managing, is the data residing in the external data sources.

If for some reason FIM Sync exported wrong of faulty data, it can be quite hard to roll-back the export.

Better make sure the data source administrators got their data backed up.

Now you should have secured the most important pieces of the configuration.

Let’s hope we haven’t forgotten anything (otherwise send feedback).

Having a backup is one thing, restoring is another.

Depending on how bad your server got damaged, you have some options for recovery.

It depends on the type of disaster which options to choose or to combine.

* 1. Schedule Backup
     1. Configuration components

Configuration components don't change frequently (or should not). Configuration items only need to backupped before and after the change to allow recovery.

* + 1. Suggested backup schedule (Manual)

It's a best practice for the administrators to take a backup of the configuraton before and after they change configuration.

* 1. Data components

Component that change base on the FIM processes require frequent backup to allow recovery of the entire FIM content.

* + 1. Suggested backup schedule (automated)

It's higly suggested to take regular (automated) backup of the data components. But it's not required to take full backups on a high frequency

Suggestion

* regular low frequency (weekly, biweekly, monthly) full database backup
* regular high frequency (daily) incremental or differential database backups.

1. Failover FIM Synchronization
   1. Failover - Warm-standby

A warm standby server is a 2nd FIM Sync up and running along your production system.

But an active server means you need a FIM Sync license for that system…

"FIM Sync Help : Activating a standby server Running ILM 2007 FP1" explains this procedure in detail (using FIM Syncactivate.exe to fail over).

When you run the FIM Syncactivate utility, you’ll need the current FIM Sync encryption key.

* 1. Failover - Cold standby

This is the same procedure, but with the secondary server NOT up and running simultaneously.

For this reason there is no need for an additional FIM Sync license.

The procedure for recovery is the same, except for a bit more delay to boot up the standby server.

1. Server recovery
   1. Full system recovery

Snapshot restore, bare metal restore, system restore… Get the existing system up and running in one step from scratch.

Easy! ;)

But usually a pretty lengthy job, that requires additional tasks...

* 1. FIM Server reinstallation

The most time consuming way to recover is completely reinstall your FIM Sync server from scratch.

A well documented server setup you created before, will be your guide in that case…

Reinstall OS, restore FIM Sync DB, reinstall FIM Sync with existing encryption key, restore config and log files, restore MA data, … the full path.

* 1. FIM Server Refresh (repair installation)

Recovering the FIM Sync application and service with a fresh FIM Sync install (database intact, encryption key OK, file backup OK…)

One of the interesting features of FIM Sync is the fact that you can rerun the FIM Sync setup on top of an existing installation without loosing the configuration.

In the case that FIM Sync gets corrupted as application, just rerun the setup and reconnect to the existing database when the wizard asks for the database location.

A fresh install of FIM/ ILM also serves other purposes:

* upgrading IIFP to ILM, ILM to FIM, FIM 2010 to FIM 2010 R2,
* FIM Sync update/upgrade
* eval version to licensed version
* relocating the FIM Sync database (documented [here](http://technet.microsoft.com/en-us/library/cc708637.aspx))
* …

Luckily, in some situations you don’t need a complete recovery or a complete reinstallation.

FIM Sync allows for exporting and importing the server configuration , the management agents and the metaverse, via the MIS GUI.

* 1. Partial / component recovery
     1. FIM Sync Server

#### FIM Sync server configuration

This FIM Sync server configuration export only contains configuration data only, not the live data of objects in the CS or metaverse. The actual compiled extensions are not included in the FIM Sync config export.

You can recover the FIM Syncconfiguration quickly for example if you wish to recover with a clean FIM Sync database (and then run the full import and sync run cycles..)

This method also allows for initially uploading an existing (test)configuration in to a blank FIM Sync production server.

But also an existing setup can be restored, for example in case of a misconfiguration.

If you need more detailed info on this method, check the ILM 2007 FP1 Help: Importing and Exporting a Server.

#### MV recovery

The metaverse can be exported and imported separately from the server config.

This is a useful for a emergency recovery of the MV.

More info: FIM 2010 Help: Export Metaverse Schema to File

#### MA Recovery

The MA export can be used for multiple purposes

* fresh creation of a new MA by importing the MA (without existing MA available)
* duplication of an existing MA (import MA function)
* updating the schema of an existing MA (update MA function)

Keep in mind that adding or creating a new MA, also impacts the MV attribute flow precedence…

#### Database recovery

In some situations it is faster to to restore the complete SQL DB with the actual data (configuration AND object data).

Supposing the encryption key is OK, stop the FIM Sync service, restore the database and restart the FIM Sync service.

BBTW, as the re-installation of FIM Sync only takes a short time, it still might be a good idea to reinstall on top of the existing FIM Sync.

##### Advantage

* Database backup contains major part of configuration and data
* Depending the data volume database restore is quicker than reloading the FIM Sync data via run profiles

##### Disadvantage

* Aggressive procedure (high impact)
* When the database is corrupt, configuration must be recovered from the FIM Sync Server configuration. Data must be reloaded via the run profiles.
* Provisiong must be disabled during initial load and initial sync. A second cycle with provisioning must be executed to get back in operational state.

#### Source code - Extensions recovery

If the source files of the compiled FIM Sync .NET extension have been deleted of corrupted, restore (or copy) a backup of the project files to original location. Eventually you might need to recompile (rebuild) the .NET projects.

#### MA Data

Some MA’s need external configuration (like the ERPMA config tool for SAP).

Other MA’s (file based MA’s) need their data in the MA subfolder…

Restore the configuration and/or data files from backup to their initial location.

* + 1. External data source

Restore the data on the external data source and rerun your FIM Sync operations using preview, logging… before performing the export again.

|  |
| --- |
| Important |
| When recovering your FIM Sync server, it might be wise to temporarily turn off the provisioning in the first phase.  Then run the imports and synchronization cycles.  If that runs fine, re-enable provisioning and run the cycles again. |

* 1. FIM Service Recovery
     1. Database restore

1. Install the FIM Service on a computer in the same Active Directory domain as the FIM Service was previously installed. When installing the FIM Service to a new database the SQL Server Agent Jobs are automatically restored.
2. Ensure that the FIM Service and SQL Server Agent are not running. If it is not possible to stop the SQL Server Agent, ensure that the FIM stored procedures are not running and disabled. Use the appropriate method for restoring the database, depending on your backup type and the data that you want to recover. See [Restore and Recovery Overview (SQL Server)](http://go.microsoft.com/fwlink/?LinkId=184026) (http://go.microsoft.com/fwlink/?LinkId=184026) for more information.
3. Restore the SQL Server database. It may be necessary to close open connections on the SQL Server database. For more information, see [sp\_who (Transact-SQL)](http://go.microsoft.com/fwlink/?linkid=181177) (http://go.microsoft.com/fwlink/?linkid=181177).
4. Restore and validate the .NET Application Configuration file.
5. Restore the registry key values.
6. Restore the SQL Server Agent jobs.
7. Start the FIM Service and SQL Server Agent.
   * 1. Repair install with existing database
8. Install the FIM Service on a computer in the same Active Directory domain as the FIM Service was previously installed. When installing the FIM Service, connect to the existing database.
9. Restore and validate the .NET Application Configuration file.
10. Validate the registry key values. Restore if required.
11. Validate the SQL Server Agent jobs. Restore if required.
12. Restart the FIM Service and SQL Server Agent.
13. Planning
    1. Review

Review your disaster recovery planning from time to time.

Keep in mind that a good preparation and the necessary technical precautions are not the only part of disaster recovery.

1. Crisis communication

Plan for crisis communication: who is impacted if the FIM Sync server fails, who should you warn or inform if disaster happens, what information do they need,…

When disaster strikes, keep cool and think!

* Immediately shut down/block/disable automated operations and scripts to avoid more trouble
* Check how bad it got
* Choose a recovery plan
* If possible, test the recovery.
* Perform the recovery
* Communicate !

1. See also

* [MIIS/ILM/FIM: How to Backup the Synchronization Engine](http://social.technet.microsoft.com/wiki/contents/articles/1764.miisilmfim-how-to-backup-the-synchronization-engine.aspx)
* [How to Use PowerShell to Backup all Resource Control Display Configuration (RCDC) Objects](http://social.technet.microsoft.com/wiki/contents/articles/11265.how-to-use-powershell-to-backup-all-resource-control-display-configuration-rcdc-objects.aspx)
* [How to migrate FIM backend database to new SQL Server](http://social.technet.microsoft.com/wiki/contents/articles/3876.how-to-migrate-fim-backend-database-to-new-sql-server.aspx)

1. References
   1. Original source

Short URL: <http://aka.ms/FIMDRP>

Full link: <http://social.technet.microsoft.com/wiki/contents/articles/24363.fim-2010-planning-disaster-recovery.aspx>

* 1. FIM
* [Backing up Forefront Identity Manager 2010 R2](http://technet.microsoft.com/en-us/library/jj590250(v=ws.10).aspx)
* [Restoring Forefront Identity Manager 2010 R2](http://technet.microsoft.com/en-us/library/jj590299(v=ws.10).aspx)
* [Forefront Identity Manager 2010 R2 Best Practices](http://technet.microsoft.com/en-us/library/jj590305(v=ws.10).aspx)
  + [Forefront Identity Manager 2010 R2 Best Practices General](http://technet.microsoft.com/en-us/library/jj590345(v=ws.10).aspx)
  + [Best Practices for Security](http://technet.microsoft.com/en-us/library/jj590274(v=ws.10).aspx)
* [FIM 2010 R2 Reporting Disaster Recovery](http://technet.microsoft.com/en-us/library/jj133846(v=ws.10).aspx)
* [FIM 2010 Backup and Restore Guide](http://technet.microsoft.com/en-us/library/fim-2010-backup-and-restore-guide(v=ws.10).aspx)
  + [Recommended FIM Backup Schedule](http://technet.microsoft.com/en-us/library/fim-2010-recommended-component-backup-schedule(v=ws.10).aspx)
  + [FIM Service Backup and Restore](http://technet.microsoft.com/en-us/library/fim-service-backup-and-restore-fim-2010-backup-and-restore-guide(v=ws.10).aspx)
  + [FIM Portal Backup and Restore](http://technet.microsoft.com/en-us/library/fim-portal-backup-and-restore-fim-2010-backup-and-restore-guide(v=ws.10).aspx)
  + [FIM Synchronization Service Backup and Restore](http://technet.microsoft.com/en-us/library/fim-synchronization-service-backup-and-restore-fim-2010-backup-and-restore-guide(v=ws.10).aspx)
  + [Testing FIM Backups](http://technet.microsoft.com/en-us/library/ff400285(v=ws.10).aspx)
  + [Case Study: How Microsoft Deploys Disaster Recovery for FIM 2010](http://technet.microsoft.com/en-us/library/gg508743(v=ws.10).aspx)
* [Configuration Migration Deployment Guide](http://technet.microsoft.com/en-us/library/ee534906(v=ws.10).aspx)
* [FIM 2010 R2 Service and Portal Configuration Backup Tool](http://technet.microsoft.com/en-us/library/jj134311(v=ws.10).aspx)
  1. SQL
* [Backing Up and Restoring Databases in SQL Server](http://msdn.microsoft.com/en-us/library/ms187048(v=sql.105).aspx)
  + [Backup Overview (SQL Server)](http://msdn.microsoft.com/en-us/library/ms175477(v=sql.105).aspx)
  + [Backup Under the Simple Recovery Model](http://msdn.microsoft.com/en-us/library/ms191164(v=sql.105).aspx)
  + [Backup Under the Full Recovery Model](http://msdn.microsoft.com/en-us/library/ms190217(v=sql.105).aspx)
  + [Backup Under the Bulk-Logged Recovery Model](http://msdn.microsoft.com/en-us/library/ms190692(v=sql.105).aspx)
  + [Introduction to Backup and Restore Strategies in SQL Server](http://msdn.microsoft.com/en-us/library/ms191239(v=sql.105).aspx)

1. Downloads

* [FIM 2010 Backup and Restore](http://go.microsoft.com/fwlink/?LinkId=200495) (http://go.microsoft.com/fwlink/?LinkId=200495)
* [FIM Portal Backup and Restore](http://download.microsoft.com/download/E/1/6/E16D8C0D-0C51-45D1-8B60-27D48D54579E/FIM_Backup.doc)

1. Additional Resources

* [FIM 2010 R2 Synchronization Service On-disk Help](http://technet.microsoft.com/en-us/library/jj572795(v=ws.10).aspx)

1. Glossary, abbreviations & acronyms

|  |  |  |
| --- | --- | --- |
| Acronym | Name | Description |
| DTAP | Development, Test, Acceptance & Production environments |  |
| FIM | Forefront Identity Manager 2010 |  |
| MV | Metaverse |  |
| CS | Connector space |  |
| Acc | Acceptance |  |
| tst | Test |  |
| dev | Development |  |
| Prod | Production |  |