Identity Synchronization Techniques in SharePoint

[1]Rajan Prakash Todankar
[1]SharePoint Administrator,
[1]SharePoint Department, [1]Datavail Infotech Pvt. Ltd, Mumbai, India.

***Abstract* - Identity Synchronization in SharePoint has evolved from Forefront Identity Management (FIM), Active Directory (AD) import to Microsoft Identity Management (MIM). It is important to study the changes that have been introduced in each phase of evolution. The analysis revolves more around SharePoint wherein these Identity Synchronization Techniques are utilized and the pros and cons are detailed to determine the technique suitable according to the requirement. The technical paper also provides recommendation regarding the best approach based on the observations conducted during the analysis.**

***Index Terms* - Identity Synchronization, SharePoint, User Profile Synchronization Service, UPA, FIM, MIM**

I. INTRODUCTION

SharePoint is widely used Enterprise application across the globe mainly for collaboration and sharing information over web based platform. When we talk about sharing and collaboration of confidential information over a web, which is open to everyone in case of internet, then there should be a strong governance over the access of the information. SharePoint integrates with Active Directory directly or indirectly to fetch the user and group identity information and stores it in its own database. Over the period of time, there have been various techniques implemented to access information within SharePoint and import the profile information from the directory source, details of which are discussed in this research paper to determine the best possible recommended technique.

II. IDENTITY SYNCHRONIZATION ENTITIES

The below entities are common to all the Identity Synchronization Techniques. The detailed techniques are discussed later in this article.

a. User Profile Service Application

An IIS Application which is located in the SharePoint Web Services IIS Web Site. The IIS Web Site is on each Front End Server in the farm. When we boot the Service Machine Instance, the IIS Application will be created. It will be named with a GUID and is hosted by an Application Pool it is named with a GUID. It hosts a couple of WCF services viz. profileproperty and profiledbcache. This is known as a Service Application Endpoint.

The Service Application Endpoint has three associated back end databases and other configuration. Pages for managing the Service Application are hosted in Central Administration and are called using a GUID in the query string. The WCFs don't actually do any work here but provide an interface to calling clients and calls other elements of the system.

There also exist a Service Connection known as Service Connection Proxy. Service Connection Proxy lives within the SharePoint Foundation Web Application Service and allows the Service Consumers (Web Applications) to call the Service Application. [1]

b. User Profile Service

A "SharePoint Service" which can be seen in Services on Server. This is not a Windows Service, but .NET assemblies that work in the background with profiles and other elements. There are no configuration options for this service. This should run on the machine in the farm which will host the User Profiles "Role". The Machine running this service is called as the Service Machine Instance.

III. IDENTITY SYNCHRONIZATION TECHNIQUES IN SHAREPOINT

There are 3 types of Identity Synchronization Techniques used in SharePoint.

a. Forefront Identity Management (FIM) Synchronization Technique:

FIM is offered as a part of pre-requisite in SharePoint. It has several components such as FIM Service, FIM Synchronization Service, FIM Portal, etc. These can be installed on different servers based on the specific requirement of a business however installing it on the same server as SharePoint does not impact any metrics of Architecture hence generally it is found that FIM Service and FIM Synchronization Service are installed on the SharePoint server. [2]

The FIM Synchronization Service consists of the meta-directory, provisioning engine, and management agents (MA) for various connected data sources. It supports synchronization of data between the FIM Synchronization Service database and other identity stores in the enterprise AD, Novel, LDAP, etc.
Installing the **FIM Service** installs the Web services parts of FIM 2010 and also configures the FIM Service database on the server.
MIISClient.exe is the built in application installed on the Synchronization Server (SharePoint Server in our case) which can be used to identify success and failure factor of the synchronization.

Integration of FIM with SharePoint

User Profile Service Application in SharePoint integrates with FIM windows service through User Profile Synchronization Service of SharePoint. Fig.1 shown below provides the structure and relationship between User Profile Service Application and FIM. The FIM configuration starts as soon as the User Profile Synchronization is service is started manually by the Administrator. SharePoint configures FIM by setting up certificates, windows services and installing FIM database schema.

Working:

Before discussing the working of User Profile Synchronization using FIM Technique, let's understand the storage areas and types of synchronization involved in the process.

i. **Connector Space (CS)** is a storage area in which object deletion, addition and modification is stored before they are synchronized with connected data source. A part of Connector Space is dedicated for each management agent.
ii. **Metaverse (MV)** is a group of tables in SQL Server that contains collective Identity Information of a resource. Objects in Metaverse must resemble with one of the object type defined in FIM Metaverse Schema.
iii. **Full Synchronization** is a type of synchronization wherein all the source objects are synchronized irrespective of their presence in the target.
iv. **Incremental Synchronization** is a type of Synchronization wherein only the changed or modified source objects are synchronized with the target. [3]

FIM based Synchronization involves 8 step process to synchronize the data from the directory source to SharePoint. Below are the steps listed considering Active Directory as the data source.

Step1: Import data from Active Directory to Active Directory Connector Space (AD CS)
Step2: Import data from User Profile Store (Database) to SharePoint Connector Space (SP CS). This step is skipped for first FULL Import as no data exist in the User Profile Store.
Step3: Synchronization of data with the Metaverse (MV).
Step4: Export of data to the User Profile Store (Database)
Step5: Import and Acknowledge that the data is received in the User Profile Store.
Step6: Synchronization of data with Metaverse (MV). Data from User Profile Store is sent back to MV including the data that needs to be written back to Active Directory.
Step7: Export to Active Directory. The data is carried back to Active Directory by the AD CS.
Step8: Import and Acknowledge that the data is received in the Active Directory.

Observations:

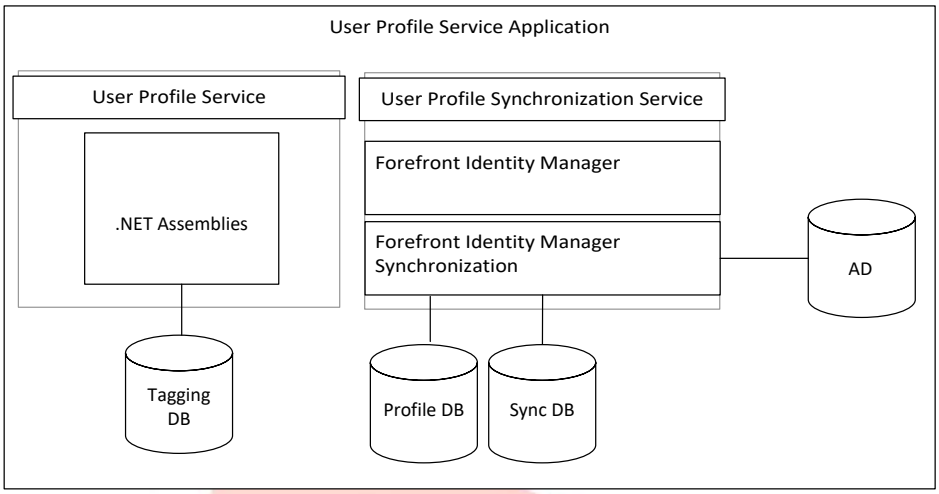
Below observations were observed while performing Identity Synchronization with FIM Technique:

Environment – SharePoint Server – 8GB RAM, Intel Xeon CPU E5 1 Core 2.6 GHz, 10 Gbps Ethernet connection
Network Latency – 1 millisecond with Active Directory for ping packets
Number of Users – 27
Number of groups – 23

1. It takes around 1 minute 38 second 35 Deci second for provisioning of User Profile Synchronization Service.
2. It takes around 15-17 second for the job to trigger after manual initiation for the first Full import and around 2-4 seconds on later Full imports.
3. It takes around 28 second 50 Deci second for a SharePoint Server to complete the Full User Profile Synchronization for the first time.
4. It takes around 32 second 11 Deci second for a SharePoint Server to complete the Full User Profile Synchronization for later synchronizations.
5. It takes around 33 second 13 Deci second for a SharePoint Server to complete the Full User Profile Synchronization after change in a property of an account.

Drawbacks of FIM Technique for Identity Synchronization

1. If the pre-requisites of FIM and SharePoint are not met, then User Profile Synchronization Service tries 15 times to configure the FIM service and establish the integration before failing. This process consumes a lot of time and eventually delete and recreating the User Profile service application resolves the issue. Pre-requisites of FIM and SharePoint integration are permissions to the service accounts, use of farm account to configure the User Profile Synchronization and requirement of farm account in the local administrator group.
2. FIM technique is a Windows service based technique wherein points of failure increases due to cross platform services involved viz. SharePoint and Windows.
3. Use of MIISclient.exe is not supported. It can be used to monitor the synchronization however making any changes during or after synchronization using this application is not supported. [4]



b. Active Directory Profiles Import Technique:

Considering the drawbacks of the FIM Technique, it was decided to directly "write back" to active directory using SharePoint services to remove the dependencies on windows services and the FIM mechanism, Active Directory Import (ADI) Technique was introduced. ADI runs as part of the **User Profile Service instance,** not the User Profile Synchronization Service Instance. [5]

Working:

As the Active Directory Import Technique uses only SharePoint Services there is no tool which can be used to monitor the working of the import or intervene the flow of the synchronization. We have to completely rely on the Unified Logging Service (ULS) logs to gather the synchronization information. Similar to FIM Technique, ADI also has synchronization types viz. Full and Incremental Synchronization. Considering a standard Full Import, below are the stages which ADI Techniques goes through to attain the successful Full Synchronization in SharePoint.

Step1: Import is kicked off, either on schedule time if one is set or manually.
Step:2 The type of profile import is verified (FULL IMPORT in our case).
Step3: Timer service starts the actual work with '*UserProfileADImportJob'*, it begins executing.
Step4: Discovers the NETBIOS name of the domain entered for sunchronization
Step5: Verifies if the synchronization account has '*Replicating Directory Changes*' permission on Active Directory.
Step6: '*InitializeProfileImportExportProcess*' method for end point is called to initialize the import.
Step7: '*UpdateWithProfileChangeData*' Method is called with an entry for number of updates in the batch.
Step8: Profile DB is updated with the new information.
Step9: '*UserProfileADImportJob*' completes post import operations
Step10: '*UserProfileADImportJob*' ends execution. [6]

Observations:

Below observations were observed while performing Identity Synchronization with FIM Technique:

Environment – SharePoint Server – 8GB RAM, Intel Xeon CPU E5 1 Core 2.6 GHz, 10 Gbps Ethernet connection
Network Latency – 1 millisecond with Active Directory for ping packets
Number of Users – 27
Number of groups – 23

1. It takes 17 second 89 Deci second for a SharePoint Server to complete the Full Active Directory Import.
2. Incremental Synchronization runs automatically after every 5 minute.

Drawbacks of Active Directory Import (ADI) Technique:

1. The most important drawback of using this technique is that we cannot right back the data to Active Directory unlike the FIM Technique hence the word 'Import' is used in the name as the data flows only unidirectional from Active Directory to SharePoint.
2. The AD import option does not filter the users when "Filter out disabled users" option is selected.
3. Using AD import option only a single, farm-wide property mapping can be configured.
4. The AD import option does not synchronize the profile photos from Active Directory to SharePoint automatically, some more custom configuration using PowerShell is required.
5. ADI does not support non-AD viz. LDAP sources.
6. ADI does not support the synchronization of Contact AD Objects.
7. ADI does not support custom AD Objects besides Users and Groups.
8. ADI does not support Business Connectivity Services Import.

c. Microsoft Identity Management (MIM) Technique:

Earlier versions of SharePoint Server had an out of the box copy of Forefront Identity Manager (FIM) that ran inside SharePoint Server. Those versions of FIM powered the User Profile Synchronization Service for products like SharePoint Server 2010 and 2013. But in SharePoint Server 2016, FIM has been advanced in favor of Microsoft Identity Manager, which is the advanced version to the FIM technology. MIM is a separate server technology (not built-in to SharePoint Server). That means, if you have MIM running on a different server machine, then more than one SharePoint Server 2016 farm can rely upon it for synchronization.

The MIM provides us with the flexibility to customize the import. It also has all the capabilities of FIM. The difference here is that MIM acts a separate entity independent of SharePoint to synchronize the profile information between Active Directory and SharePoint. It acts as an External Identity Manager. [7]

Working:

The way MIM works is almost similar to FIM, it is obvious for a successor to work in a similar fashion as the predecessor. However, MIM is installed outside SharePoint on a separate server. Below are the configuration items involved in MIM Technique:

i. **MIM Server:** The server which hosts the MIM application which governs the synchronization for SharePoint with other Identity Providers. MIM Server can be downloaded from MSDN website using the volume licensing subscription.
ii. **SharePoint Management Agent (SPMA):** It acts as a connector between the MIM Server and SharePoint User Profile Service Application to synchronize the data.

MIM based Synchronization involves the following steps to synchronize the data from the directory source to SharePoint. Below are the steps listed considering Active Directory as the data source.

Step1: Import data from Active Directory to Active Directory Connector Space (AD CS)
Step2: Import data from User Profile Store (Database) to SharePoint Management Agent (SPMA). This step is skipped for first FULL Import as no data exist in the User Profile Store.
Step3: Synchronization of data with the Metaverse (MV).
Step4: Export of data to the User Profile Store (Database)
Step5: Import and Acknowledge that the data is received in the User Profile Store.
Step6: Synchronization of data with Metaverse (MV). Data from User Profile Store is sent back to MV including the data that needs to be written back to Active Directory.
Step7: Export to Active Directory. The data is carried back to Active Directory by the AD CS.
Step8: Import and Acknowledge that the data is received in the Active Directory.

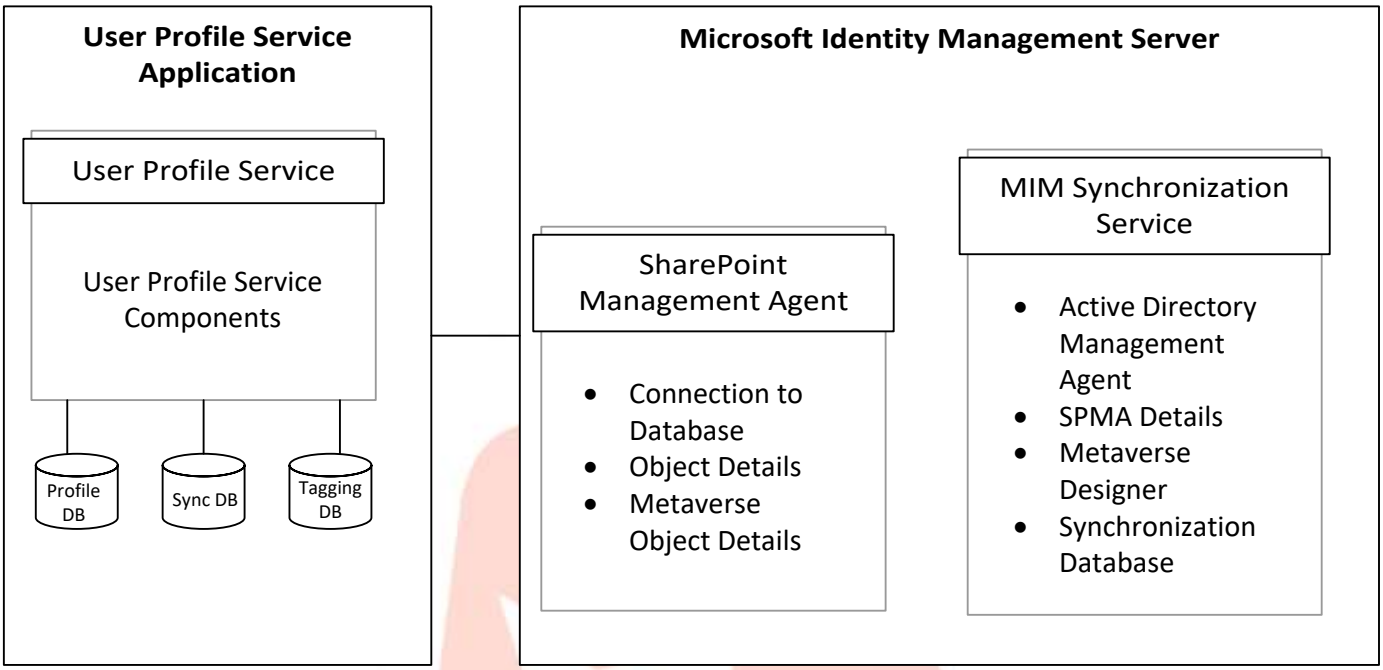
Drawbacks of MIM Technique for Identity Synchronization

1. A separate MIM server is required in the Architecture which involves a server cost and complexity in architecture.

Observations:

Below observations were observed while performing Identity Synchronization with MIM Technique:
Environment – SharePoint Server – 8GB RAM, Intel Xeon CPU E5 1 Core 2.6 GHz, 10 Gbps Ethernet connection
Network Latency – 1 millisecond with Active Directory for ping packets
Number of Users – 27
Number of groups – 23

1. It takes around 25 second 22 Deci second for a SharePoint Server to complete the Full User Profile Synchronization for the first time.
2. It takes around 27 second 53 Deci second for a SharePoint Server to complete the Full User Profile Synchronization for later synchronizations.
3. It takes around 27 second 73 Deci second for a SharePoint Server to complete the Full User Profile Synchronization after change in a property of an account.



IV. Conclusion

Based on the above 3 techniques discussed in the article and the observations derived from the practical application of the techniques in the Lab environment, it is determined that the "Active Directory Import Technique" is about 60% faster than the other two however there exist an ample of limitations by the data is synchronized using ADI Technique it can be concluded that "Microsoft Identity Management Technique" to be the best suited synchronization technique among the three. MIM Technique provides the flexibility of multi forest infrastructure along with almost all properties covered for synchronization which is important for day to day operations in SharePoint.

References

[1] Explore SharePoint 2013 – Microsoft Corporation, Published October 2014, Author Microsoft Office System and Servers Team, Page No. 158-162

[2] "Stuck on Starting": Common Issues with SharePoint Server 2010 User Profile Synchronization by Spencer Harbar

[3] Rational Guide to implementing SharePoint Server 2010 User Profile Synchronization – Spencer Harbar

[4] Profile synchronization guide for Microsoft SharePoint Server 2010 – Microsoft Corporation, Published August 2011

[5] Configure profile synchronization by using SharePoint Active Directory Import in SharePoint Server 2013 by Technet, Microsoft

[6] First Look: SharePoint Server 2013 Active Directory Import – Spencer Harbar

[7] SharePoint 2016 Step by Step Installation of Microsoft Identity Manager (MIM) by Waqas Sarwar.