****

**High Level Design Template**

**Active Directory Migration**

***<Customer Logo>***

*<Project Name>*

*<RFP Number>*

*MSI EUS Directory Services Team. Final Review by Deepak Agarwal*

*<Client Name>*

|  |  |
| --- | --- |
| **Copyright** | Copyright by HCL. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of HCL. |
| **Limitations** | HCL management reserves the right to make changes in specifications and other information contained in this publication without prior notice, and the reader should in all cases consult HCL management to determine whether any such changes have been made. |
| **Published By** | HCL Technologies - Infrastructure Services Division |
| **Document Owner** |  |
| **Document Approver** |  |
| **Date of Release** |  |
| **Version** | Initial Draft |
| **Distribution** |  |

Document Tracking Information

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Status |
| Initial Draft | Dec 11 2017 | Santanu Kumar S | Have submitted to Arun G and Sunil S for review the document. Also would request you to please validate and change wherever necessary in the document. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Acronyms

|  |  |
| --- | --- |
| **Acronyms** | **Descriptions** |
| AD  ADMT  Azure backup (online and offline)  CIFS  EMCOPY  MARS  NTFS  OS  QMM  SME  Tree size  VMOVER | Active Directory  Active Directory Management tool  Data backup from on premise to the cloud using azure backup agent protected with the vault key  Common Internet File Systems  Data and security permissions copy tool by EMC  Azure cloud data backup/restore agent installation  New Technology File System  Operating System  Quest Migration Manager  Subject Matter Expert  Extract NTFS and share permissions of the shares  Utility of Quest Migration tool for re-acling activity. |

Table of Contents

[Document Tracking Information 3](#_Toc500757409)

[Table of Acronyms 3](#_Toc500757410)

[1. Introduction 6](#_Toc500757411)

[2. Objective 6](#_Toc500757412)

[3. Target Audience 6](#_Toc500757413)

[4. Assumptions 6](#_Toc500757414)

[5. Risk 6](#_Toc500757415)

[6. Overview 7](#_Toc500757416)

[6.2 Roles & Responsibility 8](#_Toc500757417)

[7. Phase -I 9](#_Toc500757418)

[7.1 Assessment 9](#_Toc500757419)

[7.2 Data Gathering 9](#_Toc500757420)

[8. Phase –II 10](#_Toc500757421)

[8.1 Data Analysis and Planning 10](#_Toc500757422)

[8.1.1 Pre-migration activities and checklists 11](#_Toc500757423)

[8.1.2 Areas need to be considered during migration 11](#_Toc500757424)

[8.2 Design 13](#_Toc500757425)

[9. Phase III 16](#_Toc500757426)

[9.1 Build Target Domain 16](#_Toc500757427)

[9.2 Build migration environment 16](#_Toc500757428)

[10. Phase IV 18](#_Toc500757429)

[10.1 Migration Testing on Test LAB 19](#_Toc500757430)

[10.1.1 Using ADMT 19](#_Toc500757431)

[10.1.2. Using Migration Manager for AD 20](#_Toc500757432)

[10.2 Pilot Testing on Production 20](#_Toc500757433)

[10.2.1 Using ADMT 20](#_Toc500757434)

[10.2.2 Using Migration Manager for AD 21](#_Toc500757435)

[11. Phase V 21](#_Toc500757436)

[11.1 Production Rollout 22](#_Toc500757437)

[11.1.1 Using ADMT 22](#_Toc500757438)

[11.1.2 Using Migration manager for AD 22](#_Toc500757439)

[11.2 Cutover 23](#_Toc500757440)

[11.4 Post Migration cleanup and Sign off 23](#_Toc500757441)

[12. Conclusion 23](#_Toc500757442)

# Introduction

A "pattern" has been defined as: "an idea that has been useful in one practical context and will probably be useful in others" [The Open Group].

This is an attempt to document industry best practices in order to define “preferred” method of executing certain task, in this case Microsoft Active Directory migration projects.

Generally, Active Directory (AD) is a critical cornerstone of any enterprise IT infrastructure. Therefore, any effort to migrate the AD environment has to be planned carefully for reducing risk and complexity.

# Objective

The objective of this document is to equip the team with information drawn from various Vendor repositories, Industry best practices & Individual experiences, so the execution of the project becomes a repeatable and consistent activity with predictable outcome.

In this document, the Active Directory migration activity has been viewed holistically and steps are ordered for the implementation team to logically progress thru the project’s lifecycle. This document also discusses other relevant entities within an enterprise which could potentially be affected by this activity and possible approaches to contain the impacts.

# Target Audience

This document is intended for the Technical Team responsible for executing the Active Directory migration projects.

# Assumptions

The followings is a list of assumptions taken while preparing this document:

1. There are no Legacy Domain Controllers (i.e. Windows NT DC) present in the environment.
2. A formal agreement has been secured from the relevant stakeholders to move ahead with the project.
3. The source and target environment has been discussed and in principle agreed however the actual design of target environment may or may not be in scope for the migration activity.

# Risk

1. Non availability of Migration team during production roll out.

* All resources should be given adequate advance notice for planning. In addition to this, alternate resources should be earmarked to fill-in if needed.

1. Invocation of DR during migration.

* In case of unavoidable circumstances of invoking DR, the migration plan should be either suspended or rolled-back as appropriate.

1. Progress of the project may be hindered in the event of unavailability of sufficient network bandwidth or other resources.

* Thorough capacity planning exercise should be carried-out prior to commence of the project to accurately estimate the resource requirement.

1. Progress of project may be hindered in the event of severity ticket raised in the client IT network.

* Change freeze can be placed during Active directory migration in the production environment.

1. Post migration, applications turning unstable.

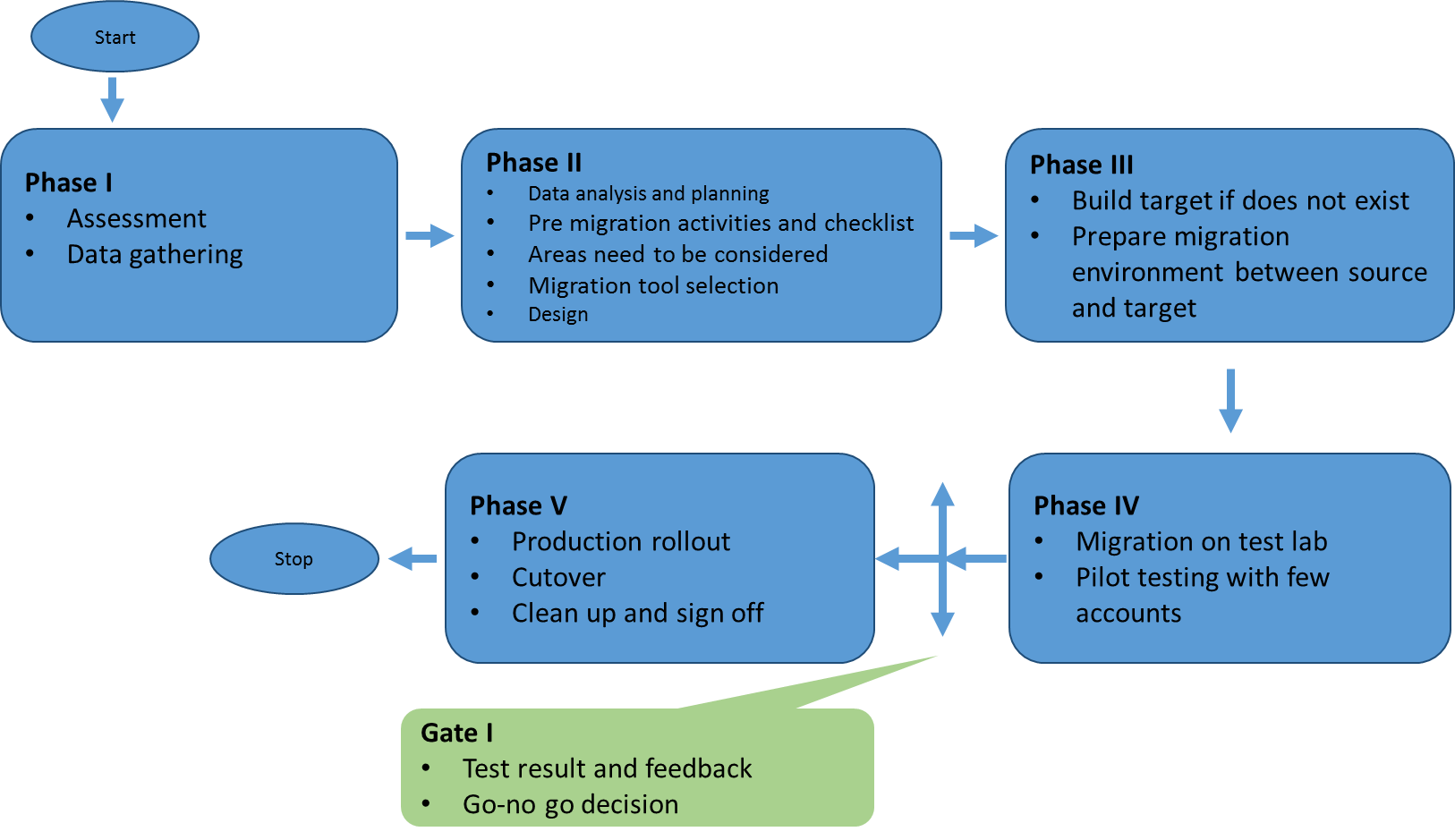
* Test environment should be established as a replica of Production environment. Through testing is recommended before migration is taken place in the production environment.

1. Roll back of migration due to business/operational requirement.

* Thorough planning is recommended before migration. Roll back plan should be tested in the test environment and handy to implement in the production as and when required.

# Overview

Following is a diagrammatic representation of stages involved for this activity.



# Roles & Responsibility

Followings are the RACI matrix.

<<SAMPLE>>

|  |  |  |
| --- | --- | --- |
| **Pre-Migration Activities** | **Customer** | **HCL** |
| Prepare Migration Checklist for Pre, Execution and Post phase | C,I | R,A |
| Data analysis and Planning phase | C,I | R,A |
| Migration plan design, project plan design, HLD, LLD, BOM preparation and other technical documents etc. | C,I | R,A |
| Domain/Forest specific User, Groups and Object list for Merge using migration tool | C,I | R,A |
| Domain specific Server hardware assessment & compatibility list for Migration | C,I | R,A |
| User notification/communication | R | R,A |
| Domain specific assessment report for Migration | I | R,A |
| Sign-off from the application owner/vendor for the compatibility of the application to avoid and issues in the application functionalities with respect to applications compatibility with Windows server 2016, schema extension and raising domain/forest functional level etc. | R,A (Application owner) | R,A (Application Owner) |
| Windows server hardware, server 2016 OS and license procurement | C,I | R,A |
| Migration Tool and license procurement | R,A | I |
| **Migration Tool Readiness** | **Customer** | **HCL** |
| Install and configure the migration tool Servers | C,I | R,A |
| Installation and configuration of Migration tool | C,I | R,A |
| Requirement of open ports for migration tool | R | R,A |
| Service account Administrator rights on all Servers | R,A | R,A |
| Agent installation and Re-acling of devices etc. | C,I | R,A |
| **Migration PoC and Pilot** | **Customer** | **HCL** |
| Conduct migration test in the test environment | C,I | R,A |
| Record result, resolve any issues identified and documented | I | R,A |
| Review PoC document | R,A | I |
| Pilot migration, usability and finalized testing | C,I | R,A |
| Resolve any issues identified in pilot migration and documented | C,I | R,A |
| Prepare Migration SOPs on basis of executed test scenarios | I | R,A |
| Review pilot result | R,A | I |
| **Production Migration** | **Customer** | **HCL** |
| Communication/notification for migration to all stake holders | R | R,A |
| Configure OU structure, import group policy, scripts etc. in ENT domain | C,I | R,A |
| Migrate users/groups from child domain to ENT domain | C,I | R,A |
| Remove AD and DNS roles from child domain controllers | C,I | R,A |
| Adjusted domain controllers in ENT domain as per requirement | C,I | R,A |
| Security translation of workstations | C,I | R,A |
| Migrate work stations and troubleshooting of end users | C,I | R,A |
| Re-acling of all Servers | C,I | R,A |
| Migrate Servers and associated Service Accounts | C,I | R,A |
| Troubleshoot and fix HCL managed applications by the application team during AD migration project | C,I | R,A |
| Troubleshoot and fix HCL unmanaged applications by the application team during AD migration project | R,A | C,I |
| Migration of additional roles (DHCP, WINS) from child domain to ENT domain | C,I | R,A |
| Server decommission | C,I | R,A |
| Decommission of child domains | C,I | R,A |
| Stability of ENT domain after decommission of child domains (Hyper care period) | C,I | R,A |

# Phase -I

This phase comprises of Assessment and data gathering of source and target domain.

## 7.1 Assessment

The objectives of this engagement are to deliver solution recommendations with consideration for the following items of scope and drivers to the business:

* + 1. Identify business requirement and technical goals for the migration, including but not limited to costing, training, security, manageability and availability.
    2. Identify and developing a standard naming convention to better manage the infrastructure. The changes to the naming conventions may be because of many factors including, but not limited to acquisitions, divestitures, mergers, policy changes, new regulations etc. This is an optional task and should be considered only if applicable.
    3. Identify the Migration team for the design and execution of the migration plan
    4. Assess the current infrastructure regarding domains, users, servers, remote users, subnets and network links. The AD Discovery tool can automate some of this data collection process.
    5. Identify and Review the access issues and requirements related to migration process such as SID History, well-known groups, built-in groups etc.
    6. In the checklist, the status of the above tasks will be set to either Completed or In-Progress based on their status of completion.

## 7.2 Data Gathering

In this section, necessary data is gathered from source as well as target environment for analysis and planning. Following is a set of data that should be captured during this process.

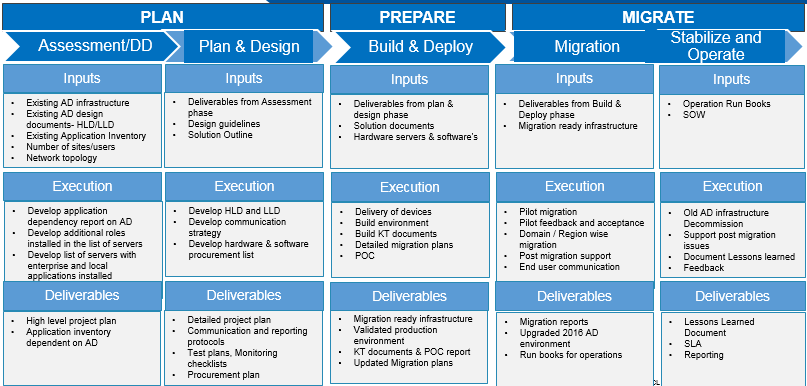
|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| |  |  |  |  | | --- | --- | --- | --- | | **Source** | | | | | Forest hierarchy | Domain hierarchy | Forest Functional level | Domain Functional level | | User type (normal /VIP) | User Profile(Roaming/Mandatory/local) | List of resources need to be migrated | Password policy | | Expired accounts | Duplicate accounts | obsolete computer accounts and type of service accounts | Trust relationship | | Hierarchy level of OU | Sites and subnets | site link and bridge | Applications running with AD | | Type of AD groups | Naming convention of AD object | Accounts never logged on | Number of AD objects | | Size of NTDS and sysvol | Backup tool used in AD | Recovery tool used in AD | External and internal DNS | | Any Third party template used in Group policy? | group policies | RODC used in the environment |  | |  |  |  |  | | **Target** | | | | | Forest hierarchy | Domain hierarchy | Forest Functional level | Domain Functional level | | User type (normal /VIP) | User Profile(Roaming/Mandatory/local) | List of resources need to be migrated | Password policy | | Expired accounts | Duplicate accounts | obsolete computer accounts/type of service accounts | Trust relationship | | Hierarchy level of OU | Sites and subnets | site link and bridge | Applications running with AD | | Type of AD groups | Naming convention of AD object | Accounts never logged on | Number of AD objects | | Size of NTDS and sysvol | Backup tool used in AD | Recovery tool used in AD | External and internal DNS | | Any Third party template used in Group policy? | group policies | RODC used in the environment |  | |  |  |  |
| In addition to the above, for 2008 and prior AD environment, use Active Directory Topology Diagrammer (ADTD) tool to generate a pictorial representation of the complete environment, Also, gather any available diagram/Visio etc. of the existing environment for reference. |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Phase –II

This phase comprises of data analysis, planning, areas need to be covered and design with respect to migration.

## 8.1 Data Analysis and Planning

Following steps will be adhered in the AD migration project.



Following is a list of decisions to be taken post analysis of the data captured in previous step

1. Decision on handling the AD objects for migration.
2. Planning of batch migration for AD objects.
3. List of resources need to be migrated.
4. Migration complexity.
5. Decision on checklist.
6. Migration of group policy, sites/subnets and links.
7. Creation of target forest/domain if does not exist.

## 8.1.1 Pre-migration activities and checklists

This section contains pre-migration checklists and other checklists necessary for a successful migration.

1. Distribution of migration schedule to the relevant stakeholders in advance.
2. Established two way Trust relationship between Source and target domain.
3. Successful hostname resolution between source and target.
4. Basic replication heath check of source and target domain.
5. Configuration of Windows local firewall for computer account migration by opening required ports/disable temporarily.
6. Migration/service account should be added in the local administrators group of all computers to perform successful computer migration. Migration/service account should have sufficient permission level for object migration between source and target. Example, migration account can be added in administrator/Domain admin groups of source and target.
7. Check the required access right of the migration/service account for the migration project.
8. Make sure of good backup of AD.
9. Inventory of shared drives and printers for each workstation and servers, for manual process in the event of an unsuccessful computer account migration.
10. Backup of user profiles using native backup tools (i.e. USMT etc.) to be used in the event of a data corruption during computer account migration (optional: extra caution).
11. Handling of duplicate accounts between source and target domain.
12. Handling of NULL groups.
13. Handling Password migration.
14. Handling of SID history.
15. Identify and list out all service accounts and their dependent applications.
16. Identify few accounts for pilot testing.
17. No active user during computer migration.
18. Define AD object batches for migration.
19. Export Group policy and login scripts from source into target domain.
20. Export Site/Subnet/Site Link information to be imported in target.
21. Creation of target domain if does not exist.
22. Prepare Fallback plan.

## 8.1.2 Areas need to be considered during migration

1. **Ongoing Projects (like Virtualization and Exchange Migration)**

Each separate project should have its own ‘freeze’ period by which no other changes are being made while the current project is ongoing.

1. **Microsoft SQL Server Deployments**

Databases rights on SQL servers that are assigned via domain accounts will need to be updated during migration of the SQL servers when they are joined to the target domain.

1. **Microsoft SharePoint Deployments**

SharePoint is a web-based application and as such does not benefit from the use of Sid History for granting access to a particular workspace. New account access will need to be granted prior to a user’s migration or the user will be prompted for its username/password from the source domain until the SharePoint deployment has been ‘moved’ into the target domain. So, user experience can be affected during co-existence period.

1. **Microsoft System Center Configuration Manager Deployments**

Workstations that have joined the target domain will lose some functionality during co-existence. Because the same is still being managed by a SCCM deployment in the source domain.

1. **Microsoft Windows Server Update Service (WSUS)**

An update on the workstation to point to the new WSUS server will be required, when the migrated workstations are joined to the target domain, Can be done through Group Policy Object.

1. **Certificate Services**

If Certificate Authority has been deployed in a source domain, coordination in the project plan will need to be tracked to ensure a smooth transition to a deployed CA in the target domain as well as any application utilizing certificates from the source CA.

1. **Centralized Backups**

Coordination of the workstation backup agent will need to occur to ensure no interruption of the migration process. Additional testing need to be taken place for the newly joined workstation to the target domain.

1. **RADIUS** – Authentication Proxy Policy

If source domain accounts are being used to authenticate users via a RADIUS deployment, steps need to be in place on the RADIUS server to ensure target domain accounts are also searchable for authentication. If universal accounts are being used no further steps should be required.

8.1.3 Migration tool selection

Based on the analysis of data and assessment of the environment/business requirement, appropriate tool should be selected. Following is a feature comparison of the tools for reference.

* + 1. Quest Migration Manager
    2. ADMT with scripting

Feature Comparison of Migration Tools for reference:

**ADMT vs QMM ADMT QMM**

Users x x

Groups x x

Computers x x

OU - x

Sites - x

Trusts - x

Undo Migration - x

Directory Synchronization x (Script) x

Supports Object Rename x x

Supports SID History migration x x

Supports SID History Cleanup - x

Supports more Source domains x x

Delegation of Tasks - x

Distributed Installation - x

IntraOrg Migration Copy Account - x

Windows Agent Updates x x

Agentless Updates - x

IIS Permissions - x

SQl Permissions - x

Exchange & permissions - x

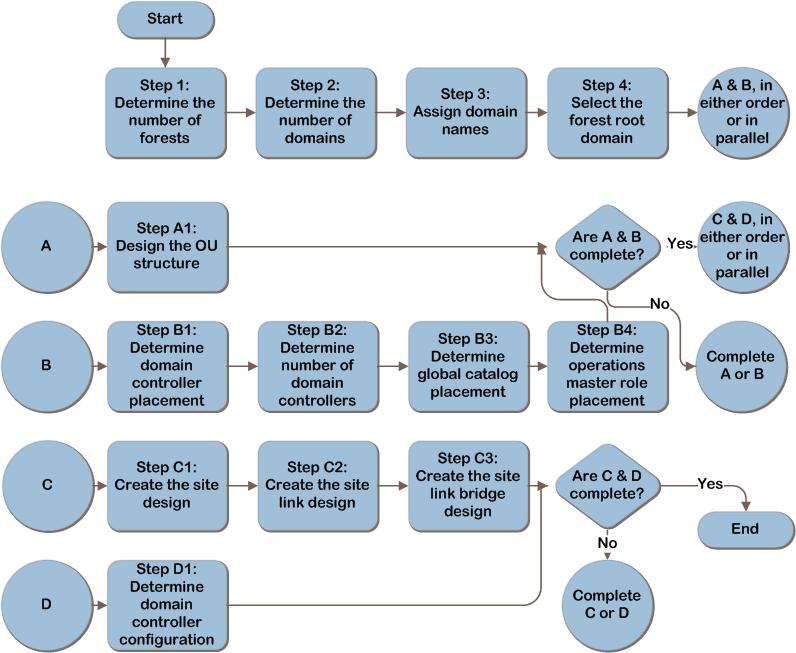
SCCM permissions x x

Licensing Cost - x

## 8.2 Design

If target infrastructure is not present then design the AD as per following steps.

* **Steps for building a new Active Directory target environment**



**Figure 1: Process flow chart: Creating a target domain (source: Microsoft)**

**Considerations:**

* **OU structure**

The OU structure should be designed to meet the business/operational requirement as determined in the below step.

* + - 1. To enable delegation of administration.
      2. To scope the application of GPOs
* **Domain Controller placement**

Domain Controller can be placed by considering the following steps.

1. Place forest root domain controllers in hub locations and at locations that host datacenters.
2. Forest root domain controllers are needed to create trust paths for clients that need to access resources in domains other than their own.
3. Add writable regional domain controllers only to locations in which physical security can be guaranteed.
4. Link availability and bandwidth.
5. Additional domain controllers to be factored for AD enabled application like SharePoint, exchange etc.

* **Global catalog placement**

Global catalog can be placed by considering the following steps.

1. In a single-domain forest, configure all domain controllers as global catalog servers
2. In multiple-domain forests,
3. Check if any application needs GC?
4. Check the number of users?
5. Check the availability of WAN link
6. Number of roaming users

* **Operation master role placement**

Flexible single master operations role can be placed by considering the following steps.

1. Rule1: The PDC Emulator and RID Master roles should be on the same machine because the PDC Emulator is a large consumer of RIDs. Since the PDC Emulator is the role that does the most work by far of any FSMO role, if the machine holding the PDC Emulator role is heavily utilized then move this role and the RID Master role to a different DC, preferable not a global catalog server (GC) since those are often heavily used also.
2. Rule 2: The Infrastructure Master should not be placed on a GC.

Make sure the Infrastructure Master has a GC in the same site as a direct replication partner.

Exception 1: It's OK to put the Infrastructure Master on a GC if your forest has only one domain.

Exception 2: It's OK to put the Infrastructure Master on a GC if every DC in your forest has the GC.

1. Rule 3: For simpler management, the Schema Master and Domain Naming Master can be on the same machine, which should also be a GC.

Exception: If you've raised your forest functional level to Windows Server 2003, the Domain Naming Master doesn't need to be on a GC, but it should at least be a direct replication partner with a GC in the same site.

1. Rule 4: Proactively check from time to time to confirm that all FSMO roles are available or write a script to do this automatically

* **Site creation**

Active directory sites can be created by considering the following steps. Ensure that clients authenticate against domain controllers nearest to them, reducing authentication latency and keeping traffic off WAN connections.

1. Authentication.
2. Replication.
3. Active Directory-enabled services.

* **Hardware Consideration for Domain Controller**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Component** | **Estimates** | | Storage/Database Size | 40KB to 60KB for each user, Operating System storage requirement and 120% for database defragmentation. | | RAM | Database Size (sysvol and ntds.dit) | | Base operating system recommendations | | Third-party applications | | Network | 1 Gigabyte(GB) | | CPU | 1000 concurrent users for each core | |  |
| * **Domain Controller planning**  |  |  |  | | --- | --- | --- | | **User per domain in a site** | **Minimum number of domain controllers required per domain in a site** | **GC** | | 1–499 | One – Single Processor | Yes | | 500–999 | One – Dual Processors/Cores | Yes | | 1,000–2,999 | Two – Dual Processors/Cores | Both DC’s GC | | 3,000–10,000 | Two – Quad Processors/Cores | Both DC’s GC | |  |

**Note:** Above is standard recommendation however peak and average utilization of existing infrastructure should also be taken into consideration while designing the target infrastructure.

* **Design output:**

1. Site Topology.
2. BOM (Hardware and Software requirement including CAL).

Use this section to identify the design documents that have been developed and summarizes the overall solution design in a succinct statement. Also, define why each of these design documents is necessary for the project.

Justification: This information provides the reader with strategic context for the follow on reading. It explains the differences between the design documents and explains how each provides a unique picture of the solution.

# 9. Phase III

This step comprises of build the target domain and prepare the migration environment for successful migration.

## 9.1 Build Target Domain

1. Build the target domain per above mentioned design (Refer 8).
2. Install and configure Active Directory onto target domain by considering the below factors.
   * Environment preparation
   * AD installation
   * FSMO configuration
   * Site Configuration
   * group policy creation
   * OU structure creation
   * Admin delegation configuration
   * Login scripts
   * DNS configuration
   * Backup configuration
3. Create trusts between source and target.

## 9.2 Build migration environment

* **Using Migration Manager for AD**

Install/Configure Active directory LDS instance.

Install .Net framework 3.5.

Install exchange MAPI CDP.

Install/Configure Database SQL 2008 above.

Open ports 135,137,138,139 and 389 on Firewall, Source and target servers and routers.

Install Directory synchronization setup.

Install Migration Manager Console and create migration account.

Create migration account with access rights as per below table for Migration Manager for AD.

| **Accounts Involved** | **Requirements** | **How To Grant** |
| --- | --- | --- |
| Source and target Active Directory accounts | Administrative access to each source and target domain involved in Active Directory migration | We recommend that you to create a **new user account** for the migration activities in each source and target domain instead of using an existing one. Add these accounts to the domain’s local **Administrators** group in the corresponding domains. For details, see Migration and dedicated Exchange environment preparation documents..  **Note**: If you have established two-way trusts between each source and target domain or forest trust, you can grant this single account administrative access to each source and target domain.  **Important**: This powerful account must be maintained closely and should be deleted after the project is complete. It is recommended that this account be owned by one individual and one backup individual (or as few individuals as possible). |

Distributed resource update

|  |  |
| --- | --- |
| **Accounts Involved** | **Requirements** |
| The account used to update a computer | Member of the computer’s local Administrators group |
| Migration Manager RUM Controller Service account | * Member of the local **Administrators** group on the computer running the Resource Updating Manager * **Full Admin** access rights on the ADAM/AD LDS database access rights on the ADAM/AD LDS database |

* **Using ADMT**

Install ADMT on Target domain controller.

Install Password Export server on source domain controller by importing the password export key from the target domain.

Create migration account with access rights as per below table.

|  |  |  |  |
| --- | --- | --- | --- |
| **Migration Object** |  | **Credentials Necessary in Source Domain** | **Credentials Necessary in Target Domain** |
| User/Group without SID history |  | Delegated **Read all user information** permission on the user OU or group OU. | Delegated **Create user objects** permission on the user OU or group OU and local administrator on the computer on which ADMT is installed. |
| User/Group with SID history |  | Local administrator or domain administrator | Delegated permission on the user OU or the group OU, extended permission to migrate SID history, and local administrator on the computer on which ADMT is installed. |
| Computer |  | Domain administrator or administrator in the source domain and on each computer | Delegated permission on the computer OU and local administrator on the computer on which ADMT is installed. |
| Profile |  | Local administrator or domain administrator | Delegated permission on the user OU and local administrator on the computer on which ADMT is installed. |
|  |  |  |  |

1. Export group policy from source and save the data in a common place.
2. Prepare list of site/subnet/site link/bridge using script.
3. Prepare input file (source SAM, Target SAM and Target name/UPN) for confliction rule. With respect to source SAM, Name and UPN, what would be the target SAM, name and UPN?

# 10. Phase IV

This phase comprises of Lab testing and pilot testing steps.

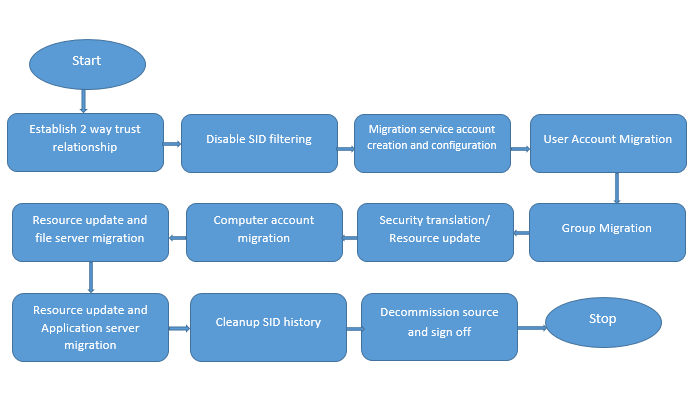
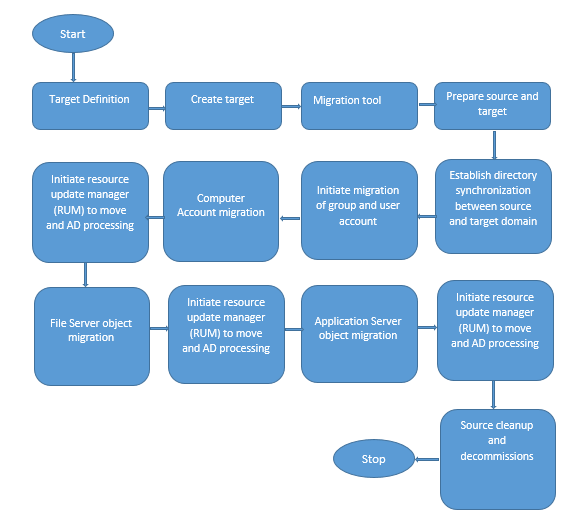


Figure 2: Process flow chart: AD migration using ADMT

  
Figure 3: Process flow chart: AD migration using quest migration manager

## 10.1 Migration Testing on Test LAB

## 10.1.1 Using ADMT

Below is the migration steps by ADMT migration tool.

1. Make sure we are already done with the pre migration checklist.
2. Make sure host name resolution between source and target domain.
3. Disable SID filter into source and target.
4. Enable SID history in source and target domain.
5. Migrate Sites/subnet/site link into target using scripting.
6. Confirm account password complexity during migration as per plan.
7. Create/validate the OU structure into target.
8. Confirm migration service account creation and configuration.
9. Confirm confliction rule.
10. Perform Group account migration batch wise by adding SID history.
11. Create/Import group policy using migration table into target (As applicable).
12. Perform user account migration batch wise by adding SID history.
13. Perform service account (used in different applications) migration.
14. Resource Update-Re ACL and fix group membership.
15. Restart computer (no active logged on user).
16. Perform security translation for previous migrated objects (local profiles) with pre check agent installation.
17. Perform Computer account migration batch wise by adding SID history.
18. Restart computer.
19. Resource update, File and print server migration.
20. Resource update and Application server migration.
21. Link/validate the group policy onto target.
22. Validate the result and feedback.
23. Source SID cleanup.

## 10.1.2. Using Migration Manager for AD

Below is the migration steps by Quest migration manager for AD tool.

1. Make sure we are already done with the pre migration checklist.
2. Perform Trust Migration.
3. Make sure host name resolution between source and target domain.
4. Perform Site Migration.
5. Create new domain pair between source and destination.
6. Create migration session for group’s batch wise. Test and run.
7. Create/Import group policy using migration table into target (applicable to newly created target domain).
8. Create migration session for user’s batch wise. Test and run.
9. Create migration session for service accounts. Test and run.
10. Create Active Directory Sync. Run.
11. Restart computer and no active logged on user.
12. Create Migration session for computer account batch wise. Test and run.
13. Create Collection of computers. Enable resource update manager task by discovery and move. Finally AD process task.
14. Create migration session for File servers. Test and run.
15. Create Collection of computers. Enable resource update manager task by discovery and move. Finally AD process task.
16. Create migration session for application servers. Test and run.
17. Create Collection of computers. Enable resource update manager task by discovery and move. Finally AD process task.
18. Link/validate the group policy onto target.
19. Cleanup SID history and source ACL.
20. Validate the result and feedback.

## 10.2 Pilot Testing on Production

## 10.2.1 Using ADMT

Below is the migration steps by ADMT migration tool.

1. Take feedback from the LAB testing and implement accordingly.
2. Make sure we are already done with the pre migration checklist.
3. Make sure host name resolution between source and target domain.
4. Go/No-Go meeting.
5. Disable SID filter into source and target.
6. Enable SID history in source and target domain.
7. Migrate Sites/subnet/site link into target using scripting.
8. Confirm account password complexity during migration as per plan.
9. Create/validate the OU structure into target.
10. Confirm migration service account creation and configuration.
11. Confirm confliction rule.
12. Perform Group account migration batch wise by adding SID history.
13. Create/Import group policy using migration table into target (applicable to newly created target domain).
14. Perform user account migration batch wise by adding SID history.
15. Perform service account (used in different applications) migration.
16. Resource Update-Re ACL and fix group membership.
17. Go/No-Go meeting.
18. Restart computer (no active logged on user).
19. Perform security translation for previous migrated objects (local profiles) with pre check agent installation.
20. Perform Computer account migration batch wise by adding SID history.
21. Restart computer.
22. Resource update, File and print server migration.
23. Resource update and Application server migration.
24. Link/validate the group policy onto target.
25. Validate the result and feedback.

## 10.2.2 Using Migration Manager for AD

Below is the migration steps by Quest migration manager for AD tool.

1. Take feedback from the LAB testing and implement accordingly.
2. Make sure we are already done with the pre migration checklist.
3. Perform Trust Migration.
4. Make sure host name resolution between source and target domain.
5. Go/No-Go meeting.
6. Perform Site Migration.
7. Create new domain pair between source and destination.
8. Create migration session for group’s batch wise. Test and run.
9. Create/Import group policy using migration table into target (applicable to newly created target domain).
10. Create migration session for user’s batch wise. Test and run.
11. Create migration session for service accounts. Test and run.
12. Create Active Directory Sync. Run.
13. Go/No-Go meeting.
14. Restart computer and no active logged on user.
15. Create Migration session for computer account batch wise. Test and run.
16. Create Collection of computers. Enable resource update manager task by discovery and move. Finally AD process task.
17. Create migration session for File servers. Test and run.
18. Create Collection of computers. Enable resource update manager task by discovery and move. Finally AD process task.
19. Create migration session for application servers. Test and run.
20. Create Collection of computers. Enable resource update manager task by discovery and move. Finally AD process task.
21. Link/validate the group policy onto target.
22. Validate the result and feedback.

# 11. Phase V

This phase comprises of production roll out, cut over and post production cleanup.

## 11.1 Production Rollout

## 11.1.1 Using ADMT

Below is the migration steps by ADMT migration tool.

1. Take the feedback from Pilot test result and adapt accordingly.
2. Go/No-Go meeting
3. Create/validate the OU structure into target.
4. Confirm account password complexity during migration as per plan.
5. Migrate Sites/subnet/site link and bridge into target using scripting.
6. Confirm Service account migration and creation.
7. Confirm confliction rule.
8. Go/No-Go meeting.
9. Perform Group account migration batch wise by adding SID history.
10. Create/Import Group policy onto target domain using policy migration table (applicable to newly created target domain).
11. Perform user account migration batch wise by adding SID history.
12. Perform service account (used in different applications) migration.
13. Resource Update-Re ACL and Fix Group membership.
14. Go/No-Go meeting.
15. Restart computer (no active logged on user).
16. Perform security translation for previous migrated objects (local profiles) with Pre check with agent installation.
17. Perform Computer account migration batch wise by adding SID history.
18. Restart computer.
19. Go/No-Go meeting.
20. Resource update, File and print server migration.
21. Go/No-Go meeting.
22. Resource update and Application server migration
23. Go/No-Go meeting.
24. Link/validate the group policy onto target.
25. Update the login scripts in sysvol.
26. Validate result and feedback.

## 11.1.2 Using Migration manager for AD

Below is the migration steps by Quest migration manager for AD tool.

1. Take feedback from the pilot testing and adapt accordingly.
2. Go/No-Go meeting.
3. Perform Site Migration.
4. Create new domain pair between source and destination.
5. Go/No-Go meeting.
6. Create migration session for group’s batch wise. Test and run.
7. Create/Import Group policy onto target domain using policy migration table (applicable to newly created target domain).
8. Create migration session for user’s batch wise. Test and run.
9. Create migration session for service accounts. Test and run.
10. Create Active Directory Sync. Run.
11. Go/No-Go meeting.
12. Restart computer and no active logged on user.
13. Create Migration session for computer account batch wise. Test and run.
14. Create Collection of computers. Enable resource update manager task by discovery and move. Finally AD process task.
15. Go/No-Go meeting.
16. Create migration session for File servers. Test and run.
17. Create Collection of computers. Enable resource update manager task by discovery and move. Finally AD process task.
18. Go/No-Go meeting.
19. Create migration session for application servers. Test and run.
20. Create Collection of computers. Enable resource update manager task by discovery and move. Finally AD process task.
21. Link/validate the group policy onto target.
22. Validate the result and feedback.

## 11.2 Cutover

1. Go/No-Go meeting with the result.
2. Final Sync of users/group membership/ACLS of computers and share drives.
3. Observation: constant communication with IT help desk.

## 11.4 Post Migration cleanup and Sign off

1. Clean up of SID history.
2. Clean up of source ACL.
3. Uninstall tool.
4. Reverse KT.
5. Decommission.
6. BAU hand over.

# 12. Conclusion

The practices discussed in this paper reflect the smooth Active directory migration methodology by minimizing business and operational risk.